



МОСКОВСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ
имени М. В. ЛОМОНОСОВА
МЕХАНИКО-МАТЕМАТИЧЕСКИЙ ФАКУЛЬТЕТ



ИНСТИТУТ ПРИКЛАДНОЙ МАТЕМАТИКИ
имени М. В. КЕЛДЫША РАН



ПЕНЗЕНСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ

МАТЕРИАЛЫ XVIII МЕЖДУНАРОДНОЙ ШКОЛЫ-СЕМИНАРА

«СИНТЕЗ И СЛОЖНОСТЬ УПРАВЛЯЮЩИХ СИСТЕМ» имени академика О. Б. Лупанова

(Пенза, 28 сентября – 3 октября 2009 г.)

Издательство механико-математического факультета МГУ

Москва 2009

УДК 519.7
М34



*Издание осуществлено
при поддержке Россий-
ского фонда фундамен-
тальных исследований по
проекту 09-01-06087*

М34 Материалы XVIII Международной школы-семинара «Синтез и сложность управляющих систем» имени академика О. Б. Лупанова (Пенза, 28 сентября – 3 октября 2009 г.) / под ред. О. М. Касим-Заде. — М.: Изд-во механико-математического факультета МГУ, 2009. — 136 с.

Сборник содержит материалы XVIII Международной школы-семинара «Синтез и сложность управляющих систем» имени академика О. Б. Лупанова, проходившей в Пензе с 28 сентября по 3 октября 2009 г. при поддержке Российского фонда фундаментальных исследований (проект 09-01-06087). Для студентов, аспирантов и научных работников в области дискретной математики и математической кибернетики.

Научное издание

МАТЕРИАЛЫ
XVIII МЕЖДУНАРОДНОЙ ШКОЛЫ-СЕМИНАРА
«СИНТЕЗ И СЛОЖНОСТЬ УПРАВЛЯЮЩИХ СИСТЕМ»
имени академика О. Б. Лупанова
(Пенза, 28 сентября – 3 октября 2009 г.)

Под общей редакцией О. М. Касим-Заде

Редакционная группа:
*М. А. Алехина, В. В. Кочергин,
А. В. Чашкин, В. В. Чугунова*

Ответственный за выпуск *В. В. Кочергин*

Н/К

ИД №04059 от 20.02.2001 Подписано к печати 30.10.2009. Формат 60 × 84¹/₁₆.
Бумага типогр. №1. Усл. печ. л. 8. Заказ № . Тираж 100 экз.

Издательство механико-математического факультета МГУ. 119992, Москва, Ленинские горы, МГУ.

Отпечатано с оригинал-макета в типографии издательства Пензенского государственного университета, Пенза

© Коллектив авторов, 2009

СОДЕРЖАНИЕ

Д. А. Алекберли Условия оптимизации частного случая расписания из 2-нагрузок	5
М. А. Алехина, С. М. Грабовская Об асимптотически оптимальных по надежности неветвящихся программах в полном конечном базисе с функциями $x_1 \oplus x_2, x_1 \& x_2$	6
М. А. Алехина, П. Г. Пичугина О надежности двойственных схем в произвольном полном конечном базисе	10
Л. Н. Бондаренко Многочлены Эйлера и их связь с перманентами и гафнианами	13
А. В. Васин Оценки ненадежности оптимальных схем в базисе $\{x_1 \& x_2, \bar{x}_1\}$ при инверсных неисправностях на выходах элементов ...	18
С. Ф. Винокуров, А. С. Францева Сложность булевых функций в некоторых классах обратимых схем	20
А. А. Вороненко О сложности распознавания свойств не всюду определенных дискретных функций	22
М. А. Герасимов О битовой длине разбиений входного потока алгоритма Хаффмана при реализации на машинах Тьюринга с почти линейным временем	24
А. А. Груздов Сравнительный анализ динамической информационной модели DIM и ORM систем	27
Д. А. Дагаев Об одном классе псевдолинейных функций	31
А. Б. Дайняк, Д. С. Романов, М. С. Шуплецов О сложности реализации булевых функций контактными схемами с ограничениями на структуру	33
О. С. Дудакова О конечной порожденности предполных классов монотонных функций девятизначной логики	38
Л. П. Жильцова, А. А. Рызаев О свойствах матрицы первых моментов и деревьев вывода для разложимой стохастической КС-грамматики в критическом случае	42
А. С. Казимиров Преобразования булевых функций, сохраняющие сложность полиномов	45
Р. М. Колпаков, М. Раффино, М. Рао О числе слов Дежан над алфавитом из 5, 6 и 7 букв	48
В. В. Кочергин О сложности вентильных схем с кратным числом путей	51
В. Б. Ларионов О надструктуре некоторых семейств замкнутых классов монотонных k -значных функций	56
А. М. Магомедов Применение теоремы о разбиении гиперграфа к задаче оптимизации расписания	61
Т. А. Магомедов Непрерывное 3-тестирование	62
П. П. Макарычев Модели многокомпонентных систем на основе маркированных графов	64

Р. Г. Мубаракзянов Определение конечности множества состояний функции цепи Маркова	68
В. И. Пантелеев О некоторых максимальных частичных гипер-и ультраклонах	73
О. А. Садовников О реализации некоторых функций схемами с подведением переменных, вложенными в единичный куб	75
А. Ю. Улесова О сложности реализации функций алгебры логики в одной модели клеточных схем	79
В. С. Федорова О сложности выполнимости системы функциональных булевых уравнений	84
А. В. Чашкин О приближенном вычислении монотонных булевых функции	88
И. Ф. Чебурахин О сложности реализации элементарных симметрических полиномов	93
Д. В. Чистиков Об одной характеристике деревьев, связанной с индивидуальным тестированием неповторных функций	94
В. В. Чугунова О сложности некоторых оптимальных по надежности схем	99
С. В. Шалагин Распределенное представление дискретных вероятностных автоматов, реализующих марковские процессы	104
С. В. Шалагин, А. Р. Нурутдинова Анализ признаков, идентифицирующих автоматные марковские модели по генерируемым ими последовательностям	109
Т. И. Шарапудинов Трехмерная визуализация на основе синтаксического анализа	114
В. И. Шевченко О сложности тестирования замыканий в формулах булевых функций	115
Л. А. Шоломов Прямое доказательство обобщенного правила сложения энтропий для частично определенных данных	118
М. С. Шуплецов О синтезе предикатных схем на основе разложений по обобщенным переменным	123
А. Д. Яшунский О предельных вероятностях значений случайных выражений в квазигруппах	128
Информация	133

УСЛОВИЯ ОПТИМИЗАЦИИ ЧАСТНОГО СЛУЧАЯ РАСПИСАНИЯ ИЗ 2-НАГРУЗОК

Д. М. Алекберли (Махачкала)

Условия существования для некоторых расписаний специального вида рассмотрены, в частности, в [1]. Как видно из замечания [2, с. 311], задача нетривиальна даже когда длительность расписания равна 3.

Пусть $N = \{1, \dots, n\}$, M — $(l \times 3)$ -матрица с элементами из множества $\{0, 1, \dots, n\}$; количество ненулевых элементов (необязательно различных) в каждой строке M равно двум, в каждом столбце положительные элементы (попарно) различны.

Определение. $(l \times 3)$ -матрицу M' будем называть *непрерывным представлением* матрицы M , если

- набор элементов в каждой строке M' — тот же, что и в соответствующей строке M , а в каждом столбце M' все ненулевые элементы попарно различны;
- в каждой строке M' ненулевые элементы размещены рядом;
- для каждого элемента $j \in N$ все элементы матрицы M' , равные j , размещены в соседних столбцах.

Задача. Существует ли непрерывное представление матрицы M ?
Построим сеть с множеством вершин

$$S \text{ (источник)}, x_1, \dots, x_n, y_1, \dots, y_l, T \text{ (сток)}$$

и дугами вида $(S, x_j) \forall j$, $(y_i, T) \forall i$ и (x_j, y_i) , где кратность каждой дуги вида (x_j, y_i) равна количеству вхождений элемента $j \in N$ в i -ю строку матрицы M ; пропускные способности всех дуг равны 1; нижние потоковые ограничения равны 1 для дуг вида (y_i, T) , а также для дуг вида (S, x_j) , где j встречается в матрице M не менее двух раз (для остальных дуг нижние потоковые ограничения равны 0).

В формулировке следующей теоремы термин “допустимый поток” понимается в соответствии с [3].

Теорема. *Непрерывное представление матрицы M существует тогда и только тогда, когда в сети существует допустимый поток.*

Работа выполнена при финансовой поддержке гранта 09–01–96504–р_юг_а.

Список литературы

1. Магомедов А. М. Уплотнение расписания с директивным сроком, кратным количеству занятий каждого преподавателя // Матем. заметки. — 2009. — Т. 85, вып. 1. — С. 65–72.
2. Гэри М., Джонсон Д. Вычислительные машины и труднорешаемые задачи. — М.: Мир, 1982.
3. Форд Л. Р., Фалкерсон Д. Р. Потоки в сетях. — М.: Мир, 1966.

ОБ АСИМПТОТИЧЕСКИ ОПТИМАЛЬНЫХ ПО НАДЕЖНОСТИ НЕВЕТВЯЩИХСЯ ПРОГРАММАХ В ПОЛНОМ КОНЕЧНОМ БАЗИСЕ С ФУНКЦИЯМИ $x_1 \oplus x_2, x_1 \& x_2$

М. А. Алехина, С. М. Грабовская (Пенза)

Рассматривается реализация булевых функций неветвящимися программами с условной остановкой [1] в полном конечном базисе B , содержащем функции $x_1 \& x_2, x_1 \oplus x_2$. Программы с условной остановкой характеризуются наличием управляющей команды — команды условной остановки, дающей возможность досрочного прекращения работы при выполнении определенного условия [1].

Будем предполагать, что все вычислительные операторы базиса B независимо друг от друга с вероятностью ε ($\varepsilon \in (0; 1/2)$) подвержены инверсным неисправностям на выходах. Эти неисправности характеризуются тем, что в исправном состоянии вычислительный оператор реализует приписанную ему булеву функцию φ , а в неисправном — функцию $\bar{\varphi}$.

Операторы условной остановки в разделе 2 считаются абсолютно надежными, а в разделе 3 предполагается, что эти операторы ненадежны, подвержены инверсным неисправностям на выходах и переходят в неисправные состояния с вероятностью ε независимо друг от друга и от вычислительных операторов. В неисправном состоянии оператор условной остановки вместо единицы выдает нуль.

Считаем, что программа реализует булеву функцию $f(x_1, \dots, x_n)$, если она реализует ее при отсутствии неисправностей.

Ненадежностью $N(Pr)$ программы Pr назовем максимальную вероятность ошибки на всех выходах программы Pr при всевозможных входных наборах.

1. Некоторые результаты для схем из функциональных элементов. Схемы из функциональных элементов отличаются от

неветвящихся программ отсутствием оператора условной остановки.

Ненадежностью $N(S)$ схемы S из функциональных элементов, подверженных инверсным неисправностям на выходах, назовем максимальную вероятность ошибки на выходе схемы S при всевозможных входных наборах. Обозначим $N_\varepsilon(f) = \inf N(S)$, где инфимум берется по всем схемам S из ненадежных элементов, реализующим булеву функцию $f(\tilde{x})$.

Теорема 1 [2]. При $\varepsilon \in (0, 1/240]$ любую булеву функцию f в базисе B можно реализовать схемой A с ненадежностью $P(A) \leq 2\varepsilon + 27\varepsilon^2$.

Пусть B' — один из базисов $\{x_1 \oplus x_2, x_1 \& x_2, 1\}$ или $\{x_1 \& x_2, x_1 \oplus x_2, x_1 \sim x_2\}$. Обозначим через $K(n)$ множество булевых функций, зависящих от переменных x_1, x_2, \dots, x_n и отличных от функций $0, 1, x_i, x_i \& x_j, x_i \oplus x_j, x_i \sim x_j$ ($i, j = 1, 2, \dots, n, i \neq j$).

Теорема 2 [2]. Пусть $\varepsilon \in (0, 1/4]$, функция $f(\tilde{x}) \in K(n)$, и пусть S — любая схема в базисе B' , реализующая функцию f . Тогда $P(S) \geq 2\varepsilon - 2\varepsilon^2$.

Таким образом, в базисах $\{x_1 \oplus x_2, x_1 \& x_2, 1\}$, $\{x_1 \& x_2, x_1 \oplus x_2, x_1 \sim x_2\}$ при инверсных неисправностях на выходах элементов для почти всех булевых функций асимптотически оптимальные по надежности схемы функционируют с ненадежностью, равной 2ε при $\varepsilon \rightarrow 0$.

2. Неветвящиеся программы с абсолютно надежным оператором условной остановки. Для неветвящихся программ с абсолютно надежным оператором условной остановки справедливы лемма 1, теоремы 3 и 4.

Лемма 1. При $\varepsilon \in (0, 1/240]$ программа Pr_g (рис. 1, 2) реализует функцию голосования $g(x_1, x_2, x_3) = x_1x_2 \vee x_1x_3 \vee x_2x_3$ с ненадежностью $N(Pr_g) \leq 2\varepsilon$, а вероятности появления нуля и единицы соответственно на каждом из трех выходов I, II и III приведены в табл. 1.

Pr_g :

- 1) $z_1 = x_1 \& x_2$
- 2) stop(z_1)
- 3) $y_1 = x_1 \oplus x_2$
- 4) $z_2 = x_3 \& y_1$
- 5) stop(z_2)
- 6) $z_3 = z_1 \oplus z_2$

Рис. 1

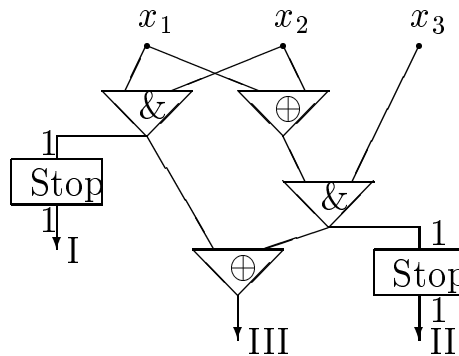


Рис. 2

Таблица 1

Наборы	Выход I		Выход II		Выход III	
	P_0^I	P_1^I	P_0^{II}	P_1^{II}	P_0^{III}	P_1^{III}
(000) (010) (100)	-	ε	-	$\varepsilon(1 - \varepsilon)$	$1 - 3\varepsilon + 3\varepsilon^2 - \varepsilon^3$	$\varepsilon - 2\varepsilon^2 + \varepsilon^3$
(001)	-	ε	-	$2\varepsilon(1 - \varepsilon)^2$	$1 - 4\varepsilon + 7\varepsilon^2 - 6\varepsilon^3 + 2\varepsilon^4$	$\varepsilon - 3\varepsilon^2 + 4\varepsilon^3 - 2\varepsilon^4$
(011) (101)	-	ε	-	$1 - 3\varepsilon + 4\varepsilon^2 - 6\varepsilon^3 + 2\varepsilon^4$	$2\varepsilon - 6\varepsilon^2 + 6\varepsilon^3 - 2\varepsilon^4$	$2\varepsilon^2 - 3\varepsilon^3 + 2\varepsilon^4$
(110)	-	$1 - \varepsilon$	-	ε^2	$\varepsilon - 2\varepsilon^2 + \varepsilon^3$	$\varepsilon^2 - \varepsilon^3$
(111)	-	$1 - \varepsilon$	-	$2\varepsilon^2(1 - \varepsilon)$	$\varepsilon - 3\varepsilon^2 + 4\varepsilon^3 - 2\varepsilon^4$	$\varepsilon^2 - 2\varepsilon^3 + 2\varepsilon^4$

Для доказательства леммы 1 необходимо вычислить и оценить вероятности $P_0^I, P_1^I, P_0^{II}, P_1^{II}, P_0^{III}, P_1^{III}$ программы Pr_g на всех входных наборах \tilde{a} .

Теорема 3. При $\varepsilon \in (0, 1/240]$ любую булеву функцию f можно реализовать такой программой Pr_f с абсолютно надежным оператором условной остановки (рис. 3, 4), что $N(Pr_f) \leq \varepsilon + 24\varepsilon^2$.

- Pr_f :
- 1) $y_1 = f(x_1, \dots, x_n)$ [S]
 - 2) $y_2 = f(x_1, \dots, x_n)$ [S]
 - 3) $y_3 = f(x_1, \dots, x_n)$ [S]
 - 4) $z_1 = y_1 \& y_2$
 - 5) stop(z_1)
 - 6) $y_4 = y_1 \oplus y_2$
 - 7) $z_2 = y_3 \& y_4$
 - 8) stop(z_2)
 - 9) $z_3 = z_1 \oplus z_2$

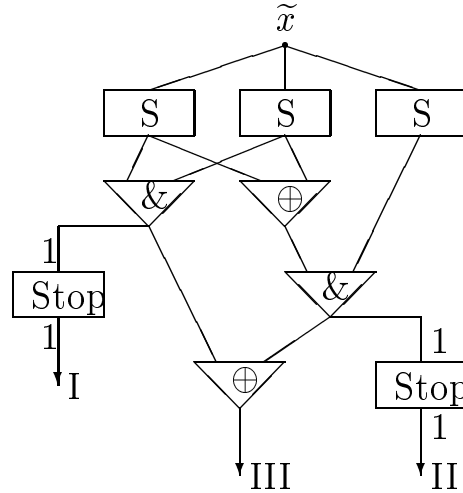


Рис. 3

Рис. 4

Доказательство теоремы 3 опирается на результаты теорем 1 и 2 и леммы 1. Оцениваются вероятности ошибки программы Pr_f для каждого из трех выходов I, II и III на наборах $\tilde{a} : f(\tilde{a}) = 0$ и $\tilde{a} : f(\tilde{a}) = 1$, а затем среди полученных вероятностей выбирается максимальная.

Теорема 4. При $\varepsilon \in (0, 1/2)$ для любой функции $f(x_1, x_2, \dots, x_n)$, не равной $x_i (i \in \{1, 2, \dots, n\})$, и любой программы Pr_f с надежным оператором условной остановки, реализующей функцию f , справедливо неравенство $N(Pr_f) \geq \varepsilon$.

Доказательство теоремы 4 проводится в два этапа. На первом

этапе предполагается, что в программе Pr_f вход ни одного оператора условной остановки не соединен с выходом никакого функционального оператора. Тогда хотя бы один из выходов программы является функциональным оператором. На втором этапе — вход хотя бы одного оператора условной остановки соединен с выходом функционального оператора. И в первом, и во втором случаях программа представляет собой функциональную схему, состоящую хотя бы из одного функционального оператора.

Из теорем 3 и 4 следует, что в любом полном конечном базисе B , содержащем функции $x_1 \oplus x_2, x_1 \& x_2$, для всех булевых функций $f(x_1, x_2, \dots, x_n)$, исключая функции $x_i (i \in \{1, 2, \dots, n\})$, асимптотически оптимальные по надежности программы с абсолютно надежным оператором условной остановки функционируют с ненадежностью, равной ε при $\varepsilon \rightarrow 0$.

3. Неветвящиеся программы с ненадежным оператором условной остановки. Далее будем считать все операторы условной остановки ненадежными, подверженными инверсным неисправностям на выходе. Справедливы лемма 2 и теоремы 5, 6, которые доказываются аналогично лемме 1 и теоремам 3 и 4 соответственно.

Лемма 2. При $\varepsilon \in (0, 1/240]$ программа Pr_g (рис. 1, 2) реализует функцию голосования $g(x_1, x_2, x_3) = x_1 x_2 \vee x_1 x_3 \vee x_2 x_3$ с ненадежностью $N(Pr_g) \leq 2\varepsilon$, а вероятности появления нуля и единицы соответственно на каждом из трех выходов I, II и III приведены в табл. 2.

Таблица 2

Наборы	Выход I		Выход II		Выход III	
	P_0^I	P_1^I	P_0^{II}	P_1^{II}	P_0^{III}	P_1^{III}
(000) (010) (100)	ε^2	$\varepsilon - \varepsilon^2$	$(1 - \varepsilon)\varepsilon^2$	$\varepsilon(1 - \varepsilon)^2$	$1 - 3\varepsilon + 3\varepsilon^2 - \varepsilon^3$	$\varepsilon - 2\varepsilon^2 + \varepsilon^3$
(001)	ε^2	$\varepsilon - \varepsilon^2$	$2\varepsilon^2(1 - \varepsilon)^2$	$2\varepsilon(1 - \varepsilon)^3$	$1 - 4\varepsilon + 7\varepsilon^2 - 6\varepsilon^3 + 2\varepsilon^4$	$\varepsilon - 3\varepsilon^2 + 4\varepsilon^3 - 2\varepsilon^4$
(011) (101)	ε^2	$\varepsilon - \varepsilon^2$	$\varepsilon - 3\varepsilon^2 + 4\varepsilon^3 - 2\varepsilon^4$	$1 - 3\varepsilon + 4\varepsilon^2 - 6\varepsilon^3 + 2\varepsilon^4$	$2\varepsilon - 6\varepsilon^2 + 6\varepsilon^3 - 2\varepsilon^4$	$2\varepsilon^2 - 3\varepsilon^3 + 2\varepsilon^4$
(110)	$\varepsilon - \varepsilon^2$	$(1 - \varepsilon)^2$	ε^3	$\varepsilon^2(1 - \varepsilon)$	$\varepsilon - 2\varepsilon^2 + \varepsilon^3$	$\varepsilon^2 - \varepsilon^3$
(111)	$\varepsilon - \varepsilon^2$	$(1 - \varepsilon)^2$	$2\varepsilon^3(1 - \varepsilon)$	$2\varepsilon^2(1 - \varepsilon)^2$	$\varepsilon - 3\varepsilon^2 + 4\varepsilon^3 - 2\varepsilon^4$	$\varepsilon^2 - 2\varepsilon^3 + 2\varepsilon^4$

Теорема 5. При $\varepsilon \in (0, 1/240]$ любую булеву функцию f можно реализовать такой программой Pr_f с ненадежным оператором условной остановки (рис. 3, 4), что $N(Pr_f) \leq \varepsilon + 24\varepsilon^2$.

Теорема 6. При $\varepsilon \in (0, 1/2)$ для любой функции $f(x_1, x_2, \dots, x_n)$, не равной x_i ($i \in \{1, 2, \dots, n\}$), и любой программы Pr_f с ненадежным оператором условной остановки, реализующей функцию f , справедливо неравенство $N(Pr_f) \geq \varepsilon(1 - \varepsilon)$.

Из теорем 5 и 6 следует, что в любом полном конечном базисе B , содержащем функции $x_1 \oplus x_2$, $x_1 \& x_2$, для всех булевых функций $f(x_1, x_2, \dots, x_n)$, исключая функции x_i ($i \in \{1, 2, \dots, n\}$), асимптотически оптимальные по надежности программы с ненадежным оператором условной остановки функционируют с ненадежностью, равной ε при $\varepsilon \rightarrow 0$.

Проведенные исследования показывают, что при $\varepsilon \in (0, 1/240]$ почти все булевы функции в базисах $\{x_1 \oplus x_2, x_1 \& x_2, 1\}$, $\{x_1 \& x_2, x_1 \oplus x_2, x_1 \sim x_2\}$ можно реализовать неветвящимися асимптотически оптимальными программами с оператором условной остановки, которые функционируют с ненадежностью, равной ε при $\varepsilon \rightarrow 0$, в то время, как ненадежность асимптотически оптимальных схем в этих базисах равна 2ε при $\varepsilon \rightarrow 0$, т. е. в 2 раза хуже.

Работа выполнена при финансовой поддержке РГНФ, номера проектов 08-06-00503а, 09-06-28615а/В.

Список литературы

1. Чашкин А. В. О среднем времени вычисления значений булевых функций // Дискретный анализ и исследование операций. — 1997. — Т. 4, № 1. — С. 60–78.
2. Алехина М. А., Васин А. В. Синтез асимптотически оптимальных по надежности схем // Известия вузов. Поволжский регион. Технические науки. — Пенза: Инфор.-издат. центр ПГУ, 2009. — № 2. — С. 36–45.

О НАДЕЖНОСТИ ДВОЙСТВЕННЫХ СХЕМ В ПОЛНОМ КОНЕЧНОМ БАЗИСЕ

М. А. Алехина, П. Г. Пичугина (Пенза)

Будем рассматривать реализацию булевых функций схемами из ненадежных функциональных элементов [1] в полном конечном базисе $B = \{e_1, e_2, \dots, e_q\}$ и предполагать, что все базисные функции e_j ($j = 1, 2, \dots, q$) зависят не более чем от m ($m \geq 2$) переменных. Схема

реализует функцию $f(x_1, x_2, \dots, x_n)$ ($\tilde{x} = (x_1, x_2, \dots, x_n)$), если она реализует ее при отсутствии неисправностей в схеме. Предполагается, что неисправности элементов статистически независимы, т. е. все элементы схемы независимо друг от друга переходят в неисправные состояния.

Ненадежность $P(S)$ схемы S определяется как максимальная вероятность ошибки $P_{f(\tilde{a})}(S, \tilde{a})$ при всевозможных входных наборах \tilde{a} схемы S , реализующей булеву функцию $f(\tilde{x})$. Надежность схемы равна $1 - P(S)$. Функционирование m -входного базисного элемента E с приписанной ему функцией $e_j(x_1, x_2, \dots, x_m)$ можно задать табл. 1, в которой p_0 и p_1 — вероятности появления 0 и 1 на выходе элемента E (числа $\alpha_0, \alpha_1, \dots, \alpha_{2^m-1} \geq 0$).

Таблица 1

x_1	x_2	...	x_m	$e_j(x_1, x_2, \dots, x_m)$	p_0	p_1
0	0	...	0	$e_j(0, 0, \dots, 0)$	α_0	$1 - \alpha_0$
0	0	...	1	$e_j(0, 0, \dots, 1)$	α_1	$1 - \alpha_1$
...
1	1	...	0	$e_j(1, 1, \dots, 0)$	α_{2^m-2}	$1 - \alpha_{2^m-2}$
1	1	...	1	$e_j(1, 1, \dots, 1)$	α_{2^m-1}	$1 - \alpha_{2^m-1}$

Элемент E^* с приписанной ему функцией e_j^* , двойственной функции e_j , назовем двойственным элементом E , если он функционирует согласно табл. 2.

Таблица 2

x_1	x_2	...	x_m	$e_j^*(x_1, x_2, \dots, x_m)$	p_0	p_1
0	0	...	0	$\bar{e}_j(1, 1, \dots, 1)$	$1 - \alpha_{2^m-1}$	α_{2^m-1}
0	0	...	1	$\bar{e}_j(1, 1, \dots, 0)$	$1 - \alpha_{2^m-2}$	α_{2^m-2}
...
1	1	...	0	$\bar{e}_j(0, 0, \dots, 1)$	$1 - \alpha_1$	α_1
1	1	...	1	$\bar{e}_j(0, 0, \dots, 0)$	$1 - \alpha_0$	α_0

Две схемы S и S^* назовем двойственными, если одна получается из другой заменой всех элементов на двойственные им элементы соответственно.

Теорема. Для любых двойственных схем S и S^* и любого входного набора \tilde{a} верно равенство

$$P_{f(\tilde{a})}(S, \tilde{a}) = P_{f^*(\tilde{a})}(S^*, \tilde{a}),$$

где $\tilde{a} = (\bar{a}_1, \dots, \bar{a}_n)$, а $f(x_1, \dots, x_n)$, $f^*(x_1, \dots, x_n)$ — функции, реализуемые схемами S и S^* соответственно.

Для схем из двухвходовых элементов (т. е. для случая $m = 2$) эта теорема была доказана М. А. Алехиной [2]. Докажем ее в случае, когда число входов элемента равно m , причем $m \geq 2$.

Доказательство теоремы проведем методом математической индукции по k — числу элементов в схеме S .

При $k = 1$ свойство вытекает из определения (см. табл. 1 и 2). Предположим, что для двойственных схем, число элементов в которых не более $k - 1$ утверждение верно. Рассмотрим произвольную схему S , реализующую f и состоящую из k элементов. Выделим в ней элемент E , содержащий выход схемы S . Обозначим через A схему, полученную из схемы S удалением элемента E . Для произвольного входного набора \tilde{a} вероятность появления 0 на выходе схемы S равна

$$P_0(S, \tilde{a}) = p_{0,0,\dots,0}\alpha_0 + p_{0,0,\dots,1}\alpha_1 + \dots + p_{1,1,\dots,0}\alpha_{2^m-2} + p_{1,1,\dots,1}\alpha_{2^m-1}, \quad (1)$$

где $p_{0,0,\dots,0}$, $p_{0,0,\dots,1}$, \dots , $p_{1,1,\dots,0}$, $p_{1,1,\dots,1}$ вероятности появления наборов $(0, 0, \dots, 0)$, $(0, 0, \dots, 1)$, $(1, 1, \dots, 0)$ и $(1, 1, \dots, 1)$ на выходах схемы A соответственно.

По схеме S построим двойственную схему S^* и выделим элемент E^* , содержащий выход схемы S^* . Обозначим через A^* схему, получаемую из схемы S^* удалением элемента E^* . Для входного набора \tilde{a} вероятность появления 1 на выходе схемы S^* равна

$$P_1(S^*, \tilde{a}) = p_{0,0,\dots,0}^*\alpha_{2^m-1} + p_{0,0,\dots,1}^*\alpha_{2^m-2} + \dots + p_{1,1,\dots,0}^*\alpha_1 + p_{1,1,\dots,1}^*\alpha_0, \quad (2)$$

где $p_{0,0,\dots,0}^*$, $p_{0,0,\dots,1}^*$, \dots , $p_{1,1,\dots,0}^*$, $p_{1,1,\dots,1}^*$ вероятности появления наборов $(0, 0, \dots, 0)$, $(0, 0, \dots, 1)$, $(1, 1, \dots, 0)$ и $(1, 1, \dots, 1)$ на выходах схемы A^* соответственно.

К каждому из выходов схем A и A^* применимо индуктивное предположение, согласно которому $P_0^i(S, \tilde{a}) = P_1^i(A^*, \tilde{a})$, т. е. на i -х выходах ($i = 1, 2, \dots, m$) равны вероятности противоположных значений при противоположных входных наборах. Тогда вероятность появления двоичного набора $\tilde{b} = (b_1, b_2, \dots, b_m)$ на выходах схемы A и вероятность появления противоположного ему набора $\tilde{\bar{b}} = (\bar{b}_1, \bar{b}_2, \dots, \bar{b}_m)$ на выходах схемы A^* равны как произведения равных множителей. Поэтому

$$p_{0,0,\dots,0}^* = p_{1,1,\dots,1}, \quad p_{0,0,\dots,1}^* = p_{1,1,\dots,0}, \dots, \\ p_{1,1,\dots,0}^* = p_{0,0,\dots,1}, \quad p_{1,1,\dots,1}^* = p_{0,0,\dots,0}. \quad (3)$$

Следовательно, из формул (1) и (2), учитывая равенства (3), получаем $P_0(S, \tilde{a}) = P_1(S^*, \tilde{a})$. Тогда $P_1(S, \tilde{a}) = P_0(S^*, \tilde{a})$.

Теорема доказана.

Следствие. Для любых двойственных схем S и S^* верно равенство $P(S) = P(S^*)$.

Таким образом, ненадежности двойственных схем равны не только в случае, когда базисные элементы двухходовые [2], но и в случае, когда базисные элементы имеют m входов ($m \geq 2$).

Работа выполнена при финансовой поддержке РГНФ, проекты 08-06-00503а, 09-06-28615а/В.

Список литературы

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

2. Алехина М. А. Синтез асимптотически оптимальных по надежности схем: монография. — Пенза: Информационно-издательский центр ПГУ, 2006.

МНОГОЧЛЕНЫ ЭЙЛЕРА И ИХ СВЯЗЬ С ПЕРМАНЕНТАМИ И ГАФНИАНАМИ

Л. Н. Бондаренко (Пенза)

Многочлен $Q(t)$ называется f -эйлеровым, если последовательность $\{f(k)\}_0^\infty$ значений многочлена f при $m \in \{0\} \cup \mathbf{N}$ имеет производящую функцию $\sum_{k=0}^\infty f(k) t^k = Q(t)(1-t)^{-m-1}$, $\deg Q \leq m$, причем $\deg f \leq m$, а $\deg f = m \Leftrightarrow Q(1) \neq 0$ [1]. К таким многочленам относятся, в частности, многочлены Эйлера $A_{n,r}(t)$, $\deg A_{n,r} = n$, которые определим операторным соотношением

$$A_{n,r}(t) = (1-t)^{rn+1} (t(1-t)^{1-r} D_t)^n (1-t)^{-1}, \quad n \in \{0\} \cup \mathbf{N}, \quad (1)$$

где $D_t = d/dt$, а параметр $r \in \mathbf{N}$ назовем родом многочлена $A_{n,r}(t)$.

Обычные многочлены Эйлера $A_n(t) = A_{n,1}(t)$ находят применение в комбинаторном анализе, теории сплайнов, теории z -преобразования, вейвлет-анализе и т. п.

Также определим сопряженные многочлены Эйлера $\bar{A}_{n,r}(z)$

$$\bar{A}_{n,r}(z) = (1+z)^n A_{n,r}(z/(1+z)), \quad A_{n,r}(t) = (1-t)^n \bar{A}_{n,r}(t/(1-t)). \quad (2)$$

Из (1)–(2) получаем $\bar{A}_{n,r}(z) = (1+z)^{(1-r)n-1} (z(1+z)^r D_z)^n z$, а также рекуррентные соотношения для многочленов $A_{n,r}(t)$, $\bar{A}_{n,r}(z)$ и их коэффициентов при $A_{0,r}(t) = A_{0,r}(z) = 1$, $n \in \mathbf{N}$, $k \in \mathbf{Z}$

$$A_{n,r}(t) = (r(n-1) + 1)tA_{n-1,r}(t) + t(1-t)A'_{n-1,r}(t), \quad (3)$$

$$\bar{A}_{n,r}(z) = ((r-1)(n-1) + 1)z\bar{A}_{n-1,r}(z) + z(1+z)\bar{A}'_{n-1,r}(z), \quad (4)$$

$$A_{0,r,k} = \delta_{0,|k|}, A_{n,r,k} = kA_{n-1,r,k} + (r(n-1) - k + 2)A_{n-1,r,k-1}, \quad (5)$$

$$\bar{A}_{0,r,k} = \delta_{0,|k|}, \bar{A}_{n,r,k} = k\bar{A}_{n-1,r,k} + ((r-1)(n-1) + k)\bar{A}_{n-1,r,k-1},$$

$\delta_{i,j}$ — символ Кронекера, а $A_{n,r}(t) = \sum_1^n A_{n,r,k} t^k$, $\bar{A}_{n,r}(z) = \sum_1^n \bar{A}_{n,r,k} z^k$.

Пусть $S_{n,r}$ — множество перестановок мультимножества $\{i^r\}_{i=1}^n$ (r — кратность i) таких, что все числа между двумя встречающимися i в $\sigma \in S_{n,r}$ больше этого i . Тогда с помощью (5) доказывается, что $A_{n,r,k}$ — число всех перестановок $\sigma \in S_{n,r}$ с k подъемами, причем при нахождении подъемов полагается $\sigma_0 = 0$. Эта комбинаторная интерпретация тривиальна при $r=1$, так как $A_{n,k} = A_{n,1,k}$ — обычные числа Эйлера [2], а при $r=2$ она установлена в [3].

Если $D(\sigma) = \{i : \sigma_i > \sigma_{i+1}\}$ — множество спуска перестановки $\sigma \in S_{n,r}$ с j подъемами, то $|D(\sigma)| = n - j$, а из формулы $\bar{A}_{n,r,k} = \sum_{j=1}^k \binom{n-j}{k-j} A_{n,r,j}$, получаемой из (2), следует, что $\bar{A}_{n,r,k}$ — число способов размещения $n-k$ черточек в местах спуска всех перестановок $\sigma \in S_{n,r}$ с j подъемами, $1 \leq j \leq k$. Отметим также, что $\bar{A}_{n,1,k} = \Delta^k 0^n$ — число размещений n различных объектов по k различным ячейкам при отсутствии пустых ячеек, где $\Delta^k 0^n$ — числа Моргана (Δ — разностный оператор), а $\bar{A}_{n,2,k}$ связаны с многочленами разбиений для производных обратных функций. $\bar{A}_{n,1,k} = \sum_{\lambda(n)} n!k! / (k_1!1!^{k_1} \dots k_n!n^{k_n})$, $\bar{A}_{n,2,k} = \sum_{\lambda(n)} (n+k)! / (k_1!2!^{k_1} \dots k_n!(n+1)^{k_n})$, где сумма берется по всем разбиениям $\lambda(n) = (1^{k_1} \dots n^{k_n})$ числа n с $k = k_1 + \dots + k_n$ [4].

Теорема 1. *Все корни каждого из многочленов $t^{-1}A_{n,r}(t)$, $z^{-1}\bar{A}_{n,r}(z)$ при $n \geq 2$ различны и отрицательны.*

Доказательство. Теорема 1 доказывается индукцией по n с помощью равенства $A_{n,r}(t) = t(1-t)^{r(n-1)+2} ((1-t)^{-r(n-1)-1} A_{n-1,r}(t))'$, получаемого из соотношения (3), и применением выражения (2).

Определим $P_{n,r}(t) = A_{n,r}(t)/A_{n,r}(1)$ и $\bar{P}_{n,r}(z) = \bar{A}_{n,r}(z)/\bar{A}_{n,r}(1)$.

Теорема 2. *Распределения коэффициентов полиномов $P_{n,r}(t)$ и $\bar{P}_{n,r}(z)$ асимптотически нормальны с параметрами*

$$\mu_{n,r} = \frac{rn+1}{r+1}; \sigma_{n,1}^2 = \frac{n+1}{12}, \sigma_{n,r}^2 = \frac{r\mu_{n,r} - g_{n,r}}{(r+1)(r+2)}, r \geq 2, \quad (6)$$

$$\bar{\mu}_{n,r} = \bar{a}_{n,r} - b_{n,r}, \bar{\sigma}_{n,r}^2 = \bar{a}_{n,r} \left(\bar{\mu}_{n+1,r} - \bar{\mu}_{n,r} - \frac{1}{2} \right) - \frac{b_{n,r}}{2}, \quad (7)$$

где $g_{n,r} = \Gamma(r^{-1}) \Gamma(n-r^{-1}) / (\Gamma(1-r^{-1}) \Gamma(n+r^{-1}))$, $\Gamma(z)$ — гамма-функция, а $\bar{a}_{n,r} = 2^{-1} \bar{A}_{n+1,r}(1) / \bar{A}_{n,r}(1)$, $b_{n,r} = 2^{-1}((r-1)n+1)$. Формулы (6), (7) справедливы при $n \geq 1$, кроме соотношения для дисперсии $\sigma_{n,1}^2$, справедливого при $n \geq 2$.

Доказательство. $\mu_{n,r} = P'_{n,r}(1)$ и $\sigma_{n,r}^2 = P''_{n,r}(1) + P'_{n,r}(1) - P_{n,r}^2(1)$, а также имеем аналогичные равенства для $\bar{\mu}_{n,r}$ и $\bar{\sigma}_{n,r}^2$. Выражения (6) и (7) находятся соответственно с помощью этих равенств и формул (3) и (4), причем при получении математического ожидания $\mu_{n,r}$ и дисперсии $\sigma_{n,r}^2$ в (6) используется метод математической индукции. Теорема 1 показывает, что многочлены $P_{n,r}(t)$ и $\bar{P}_{n,r}(z)$ являются производящими функциями для числа успехов в n испытаниях Бернулли с переменными вероятностями. Поэтому предельные соотношения $\sigma_{n,r} \rightarrow \infty$, $\bar{\sigma}_{n,r} \rightarrow \infty$ при $n \rightarrow \infty$ обеспечивают выполнение условия Линдберга [5], позволяющего применить центральную предельную теорему для доказательства асимптотической нормальности рассматриваемых распределений.

Из соотношения (3) следует, что $A_{n,r}(1) = r^n \Gamma(n+r^{-1}) / \Gamma(r^{-1})$, а использование теоремы 2 при больших n дает

$$A_{n,r} \left(\frac{1}{2} \right) \approx \frac{A_{n,r}(1)}{\sigma_{n,r} \sqrt{2\pi}} \int_0^n e^{-\frac{(\nu - \mu_{n,r})^2}{2\sigma_{n,r}^2} - \nu \ln 2} d\nu.$$

Преобразуя это выражение выделением полного квадрата в показателе экспоненты и применением формулы для $\mu_{n,r}$ из (6), а также используя равенство $\bar{A}_{n,r}(1) = 2^n A_{n,r}(1/2)$, вытекающее из соотношения (2), находим

$$\bar{A}_{n,r}(1) \approx A_{n,r}(1) 2^{(n-1)/(r+1) + \sigma_{n,r}^2 \ln 2/2}. \quad (8)$$

Для уточнения (8) следует учитывать моменты высших порядков.

Полагая $S_n = S_{n,1}$, определим множество T_n слов $\tau = \sigma \oplus \varepsilon \pmod{n}$, где $\tau = \tau_1 \dots \tau_n$, а знак " \oplus " означает побуквенное сложение перестановки $\sigma \in S_n$ и тождественной перестановки $\varepsilon \in S_n$ по \pmod{n} , причем результаты сложения по \pmod{n} — наименьшие неотрицательные вычеты. Это задает биекцию $\varphi : S_n \rightarrow T_n$.

Перестановка $\varepsilon \in S_n$ является фиксированным ключом, а операция " \oplus " применяется в криптографии. Также зададим на множестве перестановок S_n весовую функцию $w(\sigma) = 1 + n^{-1} \sum_{i=1}^n \tau_i$.

С использованием рекуррентного соотношения (5) в [2] доказана

Теорема 3. *Многочлен Эйлера $A_{n,1}(t) = \sum_{\sigma \in S_n} t^{w(\sigma)}$.*

Отметим, что последнее утверждение выполняется для любой перестановки $\varepsilon \in S_n$.

Так как перманент квадратной матрицы $C = (c_{ij})$ порядка n задается формулой $\text{per } C = \sum_{\sigma \in S_n} c_{1\sigma_1} \dots c_{n\sigma_n}$, то непосредственно из теоремы 3 вытекает [2]

Следствие 1. $A_{n,1}(t) = \text{per circ } L$, где $L = (t^{1/n}, t^{2/n}, \dots, t)$.

Это следствие определяет связь перманента циклической матрицы (циркулянта) с образующим вектором L и многочлена $A_{n,1}(t)$, причем из следствия 1 и формулы (2) получаем

Следствие 2. *Сопряженный многочлен $\bar{A}_{n,1}(z) = \text{per circ } \bar{L}$, где образующий вектор $\bar{L} = (z^{1/n}(1+z)^{1-1/n}, z^{2/n}(1+z)^{1-2/n}, \dots, z)$.*

Заметим, что следствия 1 и 2 можно принять соответственно в качестве определений многочленов $A_{n,1}(t)$ и $\bar{A}_{n,1}(z)$.

Известно, что для простого двудольного графа G с равными долями мощности n и матрицей смежности C число 1-факторов равно $\sqrt{\text{per } C}$. Так как в [6] показано, что сложность вычисления перманента $(0, 1)$ -матриц порядка n NP -трудна, то следствия 1 и 2 представляют определенный интерес.

В частности, из следствия 1 для комплексной матрицы, определенной соотношением $C = (t^{j-i})_{i,j=1}^n$, где $t = \exp(2\pi i/n)$ является корнем n -й степени из единицы, находим $\text{per } C = A_{n,1}(1) = n!$, а из следствия 2 при $z=1$ получаем $\text{per circ } (2^{1-1/n}, 2^{1-2/n}, \dots, 1) = \bar{A}_{n,1}(1)$.

Так как из формул (1)–(2) для многочленов $\bar{A}_{n,1}(z)$ нетрудно получить экспоненциальную производящую функцию следующего вида $\sum_{n=0}^{\infty} \bar{A}_{n,1}(z) u^n / n! = (1+z-ze^u)^{-1}$, то при $z=1$ получаем соотношение $\sum_{n=0}^{\infty} \bar{A}_{n,1}(1) u^n / n! = (2-e^u)^{-1}$. Функция $(2-e^u)^{-1}$ является аналитической в окрестности точки $u=0$ и имеет наименьший по абсолютной величине полюс при $u = \ln 2$, поэтому с использованием [7] получаем асимптотическую формулу $\bar{A}_{n,1}(1) \sim (\ln 2)^{-n} n!$.

Из этой асимптотики следует, что $\bar{A}_{n+1,1}(1)/\bar{A}_{n,1}(1) \sim (n+1)/\ln 2$, где $(\ln 2)^{-1} \approx 1,44270$, а из (8) имеем $\bar{A}_{n+1,1}(1)/\bar{A}_{n,1}(1) \approx c(n+1)$, где $c=2^{1/2+\ln 2/24} \approx 1,44281$. Эти результаты позволяют судить о точности приближенной формулы (8).

Гафнианом квадратной матрицы $C=(c_{ij})$ порядка $2n$ называется сумма $\text{haf } C = \sum_{\sigma \in U_{2n}} c_{1\sigma_1} \dots c_{2n\sigma_{2n}}$, где $U_{2n} \subset S_{2n}$ — множество всех $2^{-n}(2n)!/n!$ перестановок σ степени $2n$, разлагающихся в произведение n независимых транспозиций. Так, например, при $n=3$ имеем $\text{haf } C = c_{12}c_{21}c_{34}c_{43} + c_{13}c_{24}c_{31}c_{42} + c_{14}c_{23}c_{32}c_{41}$.

Для симметрической матрицы $C=(c_{ij})$ порядка $2n$ выражение для вычисления гафниана упрощается и принимает следующий вид: $\text{haf } C = \sum_{\sigma \in U_{2n}} c_{\sigma_1\sigma_2} \dots c_{\sigma_{2n-1}\sigma_{2n}}$, причем для $\sigma \in U_{2n}$ имеем $\sigma_{2i-1} < \sigma_{2i}$, $1 \leq i \leq n$ и $\sigma_1 < \sigma_3 < \dots < \sigma_{2n-1}$. Отметим, что число 1-факторов простого графа G с $2n$ вершинами и матрицей смежности C равно $\text{haf } C$, но эффективные методы вычисления гафнианов неизвестны [8].

Фиксируя перестановку $\eta = \eta_1 \dots \eta_{2n}$, $\eta \in S_{2n}$, элементы которой задаются равенствами: $\eta_{2i-1} = 2n-i$, $\eta_{2i} = n-i$, $1 \leq i \leq n$, $\eta_{2n-1} = 2n$, $\eta_{2n} = n$, определим множество V_{2n} слов $\tau = \sigma \oplus \eta \pmod{n}$, где $\tau = \tau_1 \dots \tau_{2n}$, а $\sigma \in U_{2n}$. Следует подчеркнуть, что в этом случае знак " \oplus " также означает побуквенное сложение по $\text{mod } n$, причем отображение $\psi : U_{2n} \rightarrow V_{2n}$ уже не является биекцией.

Введение на множестве перестановок U_{2n} весовой функции вида $\tilde{w}(\sigma) = 1 + n^{-1} \sum_{i=1}^{2n} \tau_i$ и применение соотношения (5) приводит к следующему утверждению:

Теорема 4. *Многочлен Эйлера $A_{n,2}(t) = \sum_{\sigma \in U_{2n}} t^{\tilde{w}(\sigma)}$.*

Вычисления показывают, что число перестановок $\eta \in S_{2n}$, для которых выполняется теорема 4, равно $3 \cdot 2^n$ при $n=2, 4, 5, \dots$ и $4 \cdot 2^n$ при $n=3$. Для всех таких перестановок $\eta \in S_{2n}$ из теоремы 4 и определения гафниана вытекает

Следствие 3. *Пусть $C=(t^{n_i+j})_{i,j=1}^{2n}$ — комплексная матрица, а $t = \exp(\pi i/n)$ — корень n -й степени из -1 . Тогда имеет место следующее равенство: $\text{haf } C = A_{n,2}(1) = 2^{-n}(2n)!/n!$.*

Это следствие указывает на связь гафнианов некоторых комплексных матриц с многочленами Эйлера II рода.

Работа выполнена при финансовой поддержке РФНФ (проект 09-06-28615 а/В).

Список литературы

1. Стенли Р. Перечислительная комбинаторика. — М.: Мир, 1990.
2. Бондаренко Л. Н. О статистиках Эйлера на группе перестановок // Материалы IX Международного семинара "Дискретная ма-

тематика и ее приложения” (Москва, МГУ, 18–23 июня 2007 г.) — М.: Изд-во механико-математического факультета МГУ, 2007. — С. 206–208.

3. Gessel I., Stanley R. Stirling polynomials // Journal of Combinatorial Theory, Series A. — 1978. — 24. — P. 24–33.

4. Риордан Дж. Комбинаторные тождества. — М: Наука, 1982.

5. Феллер В. Введение в теорию вероятностей и ее приложения. Т. 2. — М: Мир, 1984.

6. Valiant L. G. The complexity of computing the permanent // Theoretical Computer Science. — 1979. — 8. — P. 181–201.

7. Бендер Э. А. Асимптотические методы в теории перечислений // Перечислительные задачи комбинаторного анализа: сб. переводов. — М.: Мир, 1979. — С. 266–310.

8. Минк Х. Перманенты. — М: Мир, 1982.

ОЦЕНКИ НЕНАДЕЖНОСТИ ОПТИМАЛЬНЫХ СХЕМ В БАЗИСЕ $\{x_1 \& x_2, \bar{x}_1\}$ ПРИ ИНВЕРСНЫХ НЕИСПРАВНОСТЯХ НА ВЫХОДАХ ЭЛЕМЕНТОВ

А. В. Васин (Пенза)

Пусть $B = \{x_1 \& x_2, \bar{x}_1\}$ — базис, а его элементы подвержены инверсным неисправностям на выходах. Эти неисправности характеризуются тем, что в исправном состоянии функциональный элемент реализует приписанную ему булеву функцию e , а в неисправном — функцию \bar{e} . Предполагаем, что все элементы схемы переходят в неисправные состояния независимо друг от друга с вероятностью $\varepsilon \in (0; 1/2)$. Будем считать, что схема из ненадежных элементов реализует булеву функцию $f(x_1, x_2, \dots, x_n)$, если при поступлении на входы схемы набора $\tilde{a} = (a_1, a_2, \dots, a_n)$ при отсутствии неисправностей в схеме на ее выходе появляется значение $f(\tilde{a})$.

Ненадежность $P(S)$ схемы S определяется как максимальная вероятность ошибки на выходе схемы при всевозможных входных наборах. Надежность схемы S равна $1 - P(S)$.

Пусть $P_\varepsilon(f) = \inf_S P(S)$, где инфимум берется по всем схемам S из ненадежных элементов, реализующим функцию $f(x_1, x_2, \dots, x_n)$. Схема A из ненадежных элементов, реализующая функцию f , называется асимптотически оптимальной по надежности, если $P(A) \sim P_\varepsilon(f)$ при $\varepsilon \rightarrow 0$, т. е. $\lim_{\varepsilon \rightarrow 0} \frac{P_\varepsilon(f)}{P(A)} = 1$.

С. И. Аксеновым [1] получена верхняя оценка ненадежности схем в произвольном полном конечном базисе при инверсных неисправностях на выходах элементов. Он доказал, что при $\varepsilon \in (0; \varepsilon_0]$, $0 < \varepsilon_0 < 1/2$, любую булеву функцию можно реализовать такой схемой S , что

$$P(S) \leq 5\varepsilon + c\varepsilon^2. \quad (1)$$

Константы c , ε_0 положительны и зависят от базиса.

Это утверждение верно и в базисе $\{x_1 \& x_2, \bar{x}_1\}$. В работе [2] явно найдены константы c , ε_0 и доказана теорема 1.

Теорема 1 [2]. *При $\varepsilon \in (0, 1/240]$ любую булеву функцию f в базисе $\{x_1 \& x_2, \bar{x}_1\}$ можно реализовать схемой S с ненадежностью $P(S) \leq 5\varepsilon + 99\varepsilon^2$.*

Вопрос о возможности понижения константы 5 в оценке ненадежности до сих пор оставался открытым.

Пусть $K(n)$ — множество булевых функций f , зависящих от переменных x_1, x_2, \dots, x_n , не представимых в виде $(x_i^a \& g(\tilde{x}))^b$, где $i = 1, 2, \dots, n$, $a, b \in \{0, 1\}$, $g(\tilde{x})$ — произвольная булева функция.

Заметим, что 1) константы $0, 1 \notin K(n)$, 2) в базисе $\{x_1 \& x_2, \bar{x}\}$ любая схема S , реализующая функцию $f(\tilde{x}) \in K(n)$, содержит не менее 5 элементов.

Теорема 2. *Пусть $\varepsilon \in (0, 1/240]$, функция $f(\tilde{x}) \in K(n)$, и S — любая схема, реализующая функцию f . Тогда $P(S) \geq 5\varepsilon(1 - \varepsilon)^4$.*

Теорема 2 доказана в [3].

Из теоремы 2 следует, что любая схема, удовлетворяющая условиям теоремы 1 и реализующая булеву функцию $f(\tilde{x}) \in K(n)$, является асимптотически оптимальной по надежности и функционирует с ненадежностью асимптотически равной 5ε при $\varepsilon \rightarrow 0$.

А также из теоремы 2 следует, что оценка (1), полученная С. И. Аксеновым [1] для произвольного конечного полного базиса B , не может быть снижена в общем случае, так как в базисе $\{x_1 \& x_2, \bar{x}_1\}$ асимптотически оптимальные по надежности схемы функционируют с ненадежностью равной 5ε при $\varepsilon \rightarrow 0$.

Список литературы

1. Аксенов С. И. О надежности схем над произвольной полной системой функций при инверсных неисправностях на выходах элементов // Известия высших учебных заведений. Поволжский регион. Естественные науки. — 2005. — № 6 (21). — С. 42–55.

2. Алехина М. А., Шилов А. В. Верхние оценки ненадежности схем в некоторых базисах при инверсных неисправностях на выхо-

дах элементов // Известия высших учебных заведений. Поволжский регион. Естественные науки. — 2006. — № 5 (26). — С. 4–12.

3. Васин А. В. Об асимптотически оптимальных схемах в базисе $\{x_1, x_2, \bar{x}_1\}$ при инверсных неисправностях на выходах элементов // Дискретный анализ и исследование операций. — В печати.

СЛОЖНОСТЬ БУЛЕВЫХ ФУНКЦИЙ В НЕКОТОРЫХ КЛАССАХ ОБРАТИМЫХ СХЕМ

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

В работе исследуется сложность представления булевых функций обратимыми логическими схемами из определенного класса. Интерес к исследованиям обратимых схем связан с квантовыми вычислениями. По этому вопросу имеется обширная литература, например, [1]. В общем случае на обратимую схему можно смотреть как на схему, позволяющую по сигналам на ее выходах однозначно восстановить входные сигналы. В частности, будем рассматривать схемы с числом входов равным числу выходов, а входные и выходные значения которых принадлежат множеству $\{0, 1\}^{n+1}$. В этом случае обратимая схема S задает однозначное отображение $S : \{0, 1\}^{n+1} \rightarrow \{0, 1\}^{n+1}$. Такие отображения иногда называют однозначными многовыходными булевыми функциями.

В работе будет использоваться термин — обратимая функция. В общем случае обратимую функцию $f(x_1, \dots, x_n)$ можно представить системой булевых функций $f_1(x_1, \dots, x_n), \dots, f_n(x_1, \dots, x_n)$ такой, что отображение

$$f : \{(\alpha_1, \dots, \alpha_n)\} \rightarrow \{(f_1(\alpha_1, \dots, \alpha_n), \dots, f_n(\alpha_1, \dots, \alpha_n))\}$$

является однозначным.

Пусть T обозначает подкласс обратимых функции, состоящий из функций вида:

$$f : (x_1, \dots, x_n, x_{n+1}) \rightarrow (x_1, \dots, x_n, x_{n+1} \oplus x_1 \cdot \dots \cdot x_n)$$

и одностной функции $N(x)$, реализующей отрицание.

При построении обратимой логической схемы набор (или библиотека) элементарных гейтов будет состоять из гейтов, реализующих класс T . Эти элементы получили название элементов Тоффоли [2]. Несколько функций, соответствующих этим гейтам, представлены в

таблицах и для краткости обозначены $N(x)$, $T(x_1, x_2)$ и $T(x_1, x_2, x_3)$, соответственно.

$N(x_1):$	<table border="1" style="display: inline-table;"><tr><td>x_1</td><td>x'_1</td></tr><tr><td>0</td><td>1</td></tr><tr><td>1</td><td>0</td></tr></table>	x_1	x'_1	0	1	1	0
x_1	x'_1						
0	1						
1	0						

$T(x_1, x_2):$	<table border="1" style="display: inline-table;"><tr><td>x_1</td><td>x_2</td><td>x'_1</td><td>x'_2</td></tr><tr><td>0</td><td>0</td><td>0</td><td>0</td></tr><tr><td>0</td><td>1</td><td>0</td><td>1</td></tr><tr><td>1</td><td>0</td><td>1</td><td>1</td></tr><tr><td>1</td><td>1</td><td>1</td><td>0</td></tr></table>	x_1	x_2	x'_1	x'_2	0	0	0	0	0	1	0	1	1	0	1	1	1	1	1	0
x_1	x_2	x'_1	x'_2																		
0	0	0	0																		
0	1	0	1																		
1	0	1	1																		
1	1	1	0																		

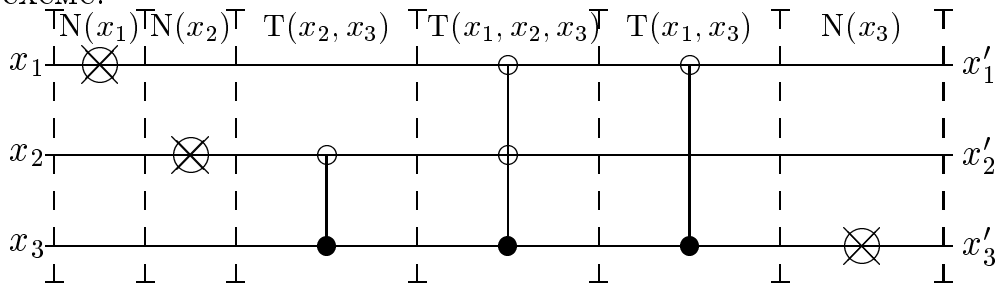
$T(x_1, x_2, x_3):$	<table border="1" style="display: inline-table;"><tr><td>x_1</td><td>x_2</td><td>x_3</td><td>x'_1</td><td>x'_2</td><td>x'_3</td></tr><tr><td>0</td><td>0</td><td>0</td><td>0</td><td>0</td><td>0</td></tr><tr><td>0</td><td>0</td><td>1</td><td>0</td><td>0</td><td>1</td></tr><tr><td>0</td><td>1</td><td>0</td><td>0</td><td>1</td><td>0</td></tr><tr><td>0</td><td>1</td><td>1</td><td>0</td><td>1</td><td>1</td></tr><tr><td>1</td><td>0</td><td>0</td><td>1</td><td>0</td><td>0</td></tr><tr><td>1</td><td>0</td><td>1</td><td>1</td><td>0</td><td>1</td></tr><tr><td>1</td><td>1</td><td>0</td><td>1</td><td>1</td><td>1</td></tr><tr><td>1</td><td>1</td><td>1</td><td>1</td><td>1</td><td>0</td></tr></table>	x_1	x_2	x_3	x'_1	x'_2	x'_3	0	0	0	0	0	0	0	0	1	0	0	1	0	1	0	0	1	0	0	1	1	0	1	1	1	0	0	1	0	0	1	0	1	1	0	1	1	1	0	1	1	1	1	1	1	1	1	0
x_1	x_2	x_3	x'_1	x'_2	x'_3																																																		
0	0	0	0	0	0																																																		
0	0	1	0	0	1																																																		
0	1	0	0	1	0																																																		
0	1	1	0	1	1																																																		
1	0	0	1	0	0																																																		
1	0	1	1	0	1																																																		
1	1	0	1	1	1																																																		
1	1	1	1	1	0																																																		

Естественно полагать, что в схеме с n входами каждый гейт действует на все входы. Поэтому если функция не зависит от какого-либо аргумента, например x_3 , то считаем ее действие тождественным по x_3 . Из этих соображений, например, действие N зависит от переменной.

$N(x_1):$	<table border="1" style="display: inline-table;"><tr><td>x_1</td><td>x_2</td><td>x_3</td><td>x'_1</td><td>x'_2</td><td>x'_3</td></tr><tr><td>0</td><td>0</td><td>0</td><td>1</td><td>0</td><td>0</td></tr><tr><td>0</td><td>0</td><td>1</td><td>1</td><td>0</td><td>1</td></tr><tr><td>0</td><td>1</td><td>0</td><td>1</td><td>1</td><td>0</td></tr><tr><td>0</td><td>1</td><td>1</td><td>1</td><td>1</td><td>1</td></tr><tr><td>1</td><td>0</td><td>0</td><td>0</td><td>0</td><td>0</td></tr><tr><td>1</td><td>0</td><td>1</td><td>0</td><td>0</td><td>1</td></tr><tr><td>1</td><td>1</td><td>0</td><td>0</td><td>1</td><td>1</td></tr><tr><td>1</td><td>1</td><td>1</td><td>0</td><td>1</td><td>0</td></tr></table>	x_1	x_2	x_3	x'_1	x'_2	x'_3	0	0	0	1	0	0	0	0	1	1	0	1	0	1	0	1	1	0	0	1	1	1	1	1	1	0	0	0	0	0	1	0	1	0	0	1	1	1	0	0	1	1	1	1	1	0	1	0
x_1	x_2	x_3	x'_1	x'_2	x'_3																																																		
0	0	0	1	0	0																																																		
0	0	1	1	0	1																																																		
0	1	0	1	1	0																																																		
0	1	1	1	1	1																																																		
1	0	0	0	0	0																																																		
1	0	1	0	0	1																																																		
1	1	0	0	1	1																																																		
1	1	1	0	1	0																																																		

$N(x_3):$	<table border="1" style="display: inline-table;"><tr><td>x_1</td><td>x_2</td><td>x_3</td><td>x'_1</td><td>x'_2</td><td>x'_3</td></tr><tr><td>0</td><td>0</td><td>0</td><td>0</td><td>0</td><td>1</td></tr><tr><td>0</td><td>0</td><td>1</td><td>0</td><td>0</td><td>0</td></tr><tr><td>0</td><td>1</td><td>0</td><td>0</td><td>1</td><td>1</td></tr><tr><td>0</td><td>1</td><td>1</td><td>0</td><td>1</td><td>0</td></tr><tr><td>1</td><td>0</td><td>0</td><td>1</td><td>0</td><td>1</td></tr><tr><td>1</td><td>0</td><td>1</td><td>1</td><td>0</td><td>0</td></tr><tr><td>1</td><td>1</td><td>0</td><td>1</td><td>1</td><td>1</td></tr><tr><td>1</td><td>1</td><td>1</td><td>1</td><td>1</td><td>0</td></tr></table>	x_1	x_2	x_3	x'_1	x'_2	x'_3	0	0	0	0	0	1	0	0	1	0	0	0	0	1	0	0	1	1	0	1	1	0	1	0	1	0	0	1	0	1	1	0	1	1	0	0	1	1	0	1	1	1	1	1	1	1	1	0
x_1	x_2	x_3	x'_1	x'_2	x'_3																																																		
0	0	0	0	0	1																																																		
0	0	1	0	0	0																																																		
0	1	0	0	1	1																																																		
0	1	1	0	1	0																																																		
1	0	0	1	0	1																																																		
1	0	1	1	0	0																																																		
1	1	0	1	1	1																																																		
1	1	1	1	1	0																																																		

На рисунке приведен пример различного расположения гейтов в схеме.



Будем говорить, что булева функция $f(x_1, \dots, x_n)$ реализуется обратимой схемой, если существует обратимая схема, реализующая отображение F

$$F : (x_1, \dots, x_n, x_{n+1}) \rightarrow (x_1, \dots, x_n, x_{n+1} \oplus f(x_1, \dots, x_n))$$

Теорема 1. Любая булева функция $f(x_1, \dots, x_n)$ может быть реализована обратимой схемой с $n + 1$ входами в базе T .

Естественно за меру сложности $L(S)$ схемы S , реализующей функцию f , принять количество ее элементов. Тогда функция Шеннона $L(n)$ для класса булевых функций определяется стандартно

$$L(n) = \max_{f \in P_2} \min_S L(S).$$

Теорема 2. Для функции $L(n)$ выполняются неравенства

$$\left\lfloor \frac{2}{3} 2^n \right\rfloor \leq L(n) < \left\lfloor \frac{2}{3} 2^n \right\rfloor + 2n.$$

Следствие. Функция $L(n)$ асимптотически равна $\lfloor \frac{2}{3} 2^n \rfloor$.

Работа выполнена при финансовой поддержке РФФИ (проект 09-01-00476-а).

Список литературы

1. Pittenger A. An introduction to quantum computing algorithms // Progress in computer science and applied logic. — V. 19. — 2001.
2. Toffoli T. Reversible computing. Tech. Memo MIT/LCS/TM-151, MIT Lab. for Comp. Sci., 1980.

О СХЕМНОМ РАСПОЗНАВАНИИ СВОЙСТВ ДООПРЕДЕЛИМОСТИ

А. А. Вороненко (Москва)

В настоящей работе рассматриваются новые применения известного метода разложения, впервые использованного в работе [1] и точно сформулированного в работе [2]. При помощи данного метода можно строить последовательность схем невысокой сложности, распознающих принадлежность дискретных функций, заданных столбцом значений, наследственному классу. Здесь, хотя фактически мы будем применять основную теорему работы [2], в изложении это большое по объему утверждение формулироваться не будет.

1. Доопределимость до неповторной.

Пусть задан наследственный относительно константных подстановок базис булевых функций B . Требуется построить схему из

функциональных элементов, которая по вектору значений не всюду определенной функции распознавала бы ее доопределимость до некоторой функции, неповторной в базисе B .

Пусть n — число переменных нашей функции. Тогда несложно построить схему сложности не выше $c_1 \cdot 2^n \cdot C_B(n)$, решающую нашу задачу. Здесь $C_B(n)$ — количество неповторных функций n переменных в базисе B (экспоненциально растущая величина [3]; основание экспоненты всегда больше двух). Константа c_1 зависит только от схемного базиса. Такая схема ищет возможность доопределения перебором по всем неповторным функциям.

Теорема. *Существует последовательность схем $\{S_n\}$ сложности не превосходящей $c_2 \cdot C_B(n)$, распознающих доопределимость не всюду определенных функций до неповторных (где c_2 — константа, зависящая от схемного базиса).*

Доказательство. Вектор-столбец входной функции мы будем рассматривать как расположенный на минус первом уровне код. Далее на каждом уровне j от нулевого до n -го будут располагаться возможные коды подфункций j переменных в количестве 2^{n-j} штук. При этом длина кода на каждом уровне равняется количеству возможных неповторных функций; 0 обозначает отсутствие возможности соответствующего доопределения, 1 — наличие такой возможности.

Из разложения функции по одной переменной и наследственности базиса B следует, что каждый бит на j -ом уровне, начиная с $j = 1$ определяется как конъюнкция двух битов $j - 1$ -го уровня. На нулевом уровне 0 минус первого уровня заменяется на 10, 1 — на 01, а — (код неопределенности) на 11. Нетрудно видеть, что ответ на вопрос о доопределимости дает дизъюнкция битов n -го уровня. При этом сложность схемы равна

$$2 \cdot c_0 \cdot 2^n + c_v(2^n - 1) + \sum_{j=1}^n 2^{n-j} \cdot C_B(j) \cdot C_{\&}, \quad (1)$$

где c_0 — сложность получения бита на первом уровне, а $c_{\&}$ и c_v — сложность получения конъюнкции и дизъюнкции двух переменных соответственно. Для доказательства теоремы остается вынести множитель 2^n за знак суммирования и оценить сумму в формуле (1) с учетом скорости роста функции $C_B(n)$.

2. Доопределимость до линейной.

Рассмотрим вопрос схемного распознавания доопределимости k -значной функции до линейной по модулю k . Если рассмотреть

столбец значений функции $f(x_1, \dots, x_n)$ и фиксировать произвольным образом значения первых j переменных, то предположение о линейности функции $f(x_1, \dots, x_n) = \alpha + \alpha_1 x_1 + \dots + \alpha_n x_n$ дает линейное уравнение по модулю k относительно $j + 2$ переменных $\alpha, \alpha_1, \dots, \alpha_j, \alpha_{j+1} x_{j+1} + \dots + \alpha_n x_n$. Системы подобных уравнений можно привести к виду, содержащему не более $j + 2$ уравнений. Подставив в преобразованную систему константы на место $j + 1$ -й переменной, получим систему из не более чем $(j + 2)k$ уравнений, которую мы можем свести к системе $j + 3$ уравнений. Анализ сложности соответствующих преобразований, аналогичный проведенному в [2] показывает, что соответствующая последовательность схем имеет линейную сложность относительно длины входа k^n .

Работа выполнена при финансовой поддержке РФФИ (проекты 09-01-00701 и 09-01-00817)

Список литературы

1. Вороненко А. А. О сложности распознавания монотонности // Математические вопросы кибернетики. Вып. 8. — М.: Физматлит, 1999. — С. 301–303.
2. Вороненко А. А. О методе разложения для распознавания принадлежности инвариантным классам // Дискретная математика. — 2002. — Т. 14, вып. 4. — С. 110–116.
3. Зубков О. В. О числе неповторных функций в базисе $\{\&, \vee, \oplus, \neg\}$ // Дискретный анализ и исследование операций. — 2003. — Т. 10, № 1. — С. 41–60.

О БИТОВОЙ ДЛИНЕ РАЗБИЕНИЙ ВХОДНОГО ПОТОКА АЛГОРИТМА ХАФФМАНА ПРИ РЕАЛИЗАЦИИ НА МАШИНАХ ТЬЮРИНГА С ПОЧТИ ЛИНЕЙНЫМ ВРЕМЕНЕМ

М. А. Герасимов (Санкт-Петербург)

Рассматривается алгоритм Хаффмана, применяемый к битовой последовательности входных данных, разделяемой на разбиения фиксированной длины. Выбор длины разбиения определяет количество символов во входном алфавите.

Для анализа алгоритма рассматривается одноленточная, одноголовочная машина Тьюринга со входной и выходной лентой. Предполагается, что входные данные записаны на входной ленте, обрабатываются на рабочей ленте и результат записывается на выходной

ленте. При работе машины Тьюринга используется алфавит, состоящий из четырех символов $\{\#, b, 0, 1\}$. Результатом работы алгоритма считается битовая последовательность, кодирующая исходные данные и соответствующее дерево кодирования, позволяющее однозначно восстановить исходную последовательность.

В дальнейшем будем считать, что входные данные записаны в виде битовой последовательности на входной ленте между двумя маркерами '#'. Считывание второго маркера означает конец цепочки входных данных. Входная лента позволяет считывать входные данные произвольное количество раз.

Выходная лента позволяет только записывать результат вычисления в виде последовательности символов рабочего алфавита. Кроме преобразованной входной последовательности символов, результат вычисления содержит код кодирующего дерева, позволяющий восстанавливать исходную входную битовую последовательность. Каждый символ выходной цепочки записывается только один раз и больше не изменяется.

Доказано, что при выборе длины разбиения (битового представления входного алфавита) $m = \frac{1}{k} \log n$, где n — общая длина входных данных, время работы алгоритма Хаффмана может быть сделано «почти линейным», более точно, с верхней оценкой $O\left(n^{\frac{k+1}{k}}\right)$ при $k \geq 2$.

Структуры данных

Рассматриваемая реализация алгоритма Хаффмана использует линейный список входных разбиений с их частотными характеристиками и дерево частотного кодирования входного алфавита префиксными кодами. Предполагается, что поступающий входной поток битов разбивается на отдельные блоки (разбиения) фиксированной длины. Каждое разбиение рассматривается как некоторая буква в соответствующем входном алфавите. Таким образом, при разбиении потока на блоки по m битов, входной алфавит содержит не более чем 2 в степени m символов. Если n не кратно m , последнее разбиение может быть дополнено нулями до длины m . При восстановлении исходного потока эти нули могут быть отброшены, поскольку известно n .

Оценка времени работы алгоритма

Рассмотрим размер списка входных разбиений при ограничениях на длину одного разбиения $m \leq \frac{1}{k} \log n$, где n — длина входной цепочки данных. В этом случае бинарный входной поток данных разбивается на $\frac{kn}{\log n}$ разбиений, которые могут рассматриваться как

символы входного алфавита. При длине m , максимальное количество различных разбиений в таблице не превосходит $\sqrt[k]{n}$.

Рассмотрим худший случай для оценки размера таблицы. Нетрудно заметить, что максимальный размер таблицы достигается при одинаковом количестве различных разбиений. В этом случае каждое разбиение встречается во входном потоке не более $\frac{kn}{\log n \sqrt[k]{n}}$ раз. Общая длина двоичной записи частоты повторения разбиения в этом случае не превосходит $\frac{k-1}{k} \log n - \log \log n + \log k$. Учитывая общее количество различных разбиений в таблице, получаем, что размер общей частотной таблицы не превосходит $\sqrt[k]{n} (\frac{k-1}{k} \log n - \log \log n + \log k)$. Таким образом, увеличение счетчика частоты повторения для одного разбиения во входном потоке, потребует совершить не более $\sqrt[k]{n} (\frac{k-1}{k} \log n - \log \log n + \log k)$ шагов машины Тьюринга, что дает общую оценку времени заполнения частотной таблицы $\frac{kn}{\log n} \sqrt[k]{n} (\frac{k-1}{k} \log n - \log \log n + \log k)$. Откуда получается, что частотная таблица, в этом случае, может быть заполнена не более чем за $(k-1)n^{\frac{k+1}{k}}$ шагов машины Тьюринга. Поскольку рассматривался худший случай для частотной таблицы, в общем случае эта оценка продолжает оставаться верной. Построение кодирующего дерева по заданной частотной таблице и вывод результатов алгоритма Хаффмана могут быть сделаны не более чем за $O(n)$ шагов машины Тьюринга. Таким образом, наиболее сложная часть алгоритма — построение частотной таблицы — дает верхнюю оценку $O(n^{\frac{k+1}{k}})$ шагов машины Тьюринга, где $\log n \geq k \geq 2$.

Список литературы

1. Ахо А, Хопкрофт Дж., Ульман Дж. Построение и анализ вычислительных алгоритмов. — М.: Мир, 1979.
2. Минский М. Вычисления и автоматы. — М.: Радио и связь, 1971.
3. Huffman D.A. A method for construction of minimum redundancy codes // Proceeding of IRE. — 1952. — V. 40. — P. 1098–1101.
4. Horowitz E., Sahni S. Fundamentals of computer algorithms. — Computer Science Press, 1978.

СРАВНИТЕЛЬНЫЙ АНАЛИЗ ДИНАМИЧЕСКОЙ ИНФОРМАЦИОННОЙ МОДЕЛИ DIM И ORM СИСТЕМ

А. А. Груздов (Ярославль)

В различных областях человеческой деятельности для описания процессов часто используются дискретные детерминированные модели, характеризующиеся конечным числом объектов, конечным рядом свойств с множествами их значений, детерминированными законами взаимодействия и динамикой объектов, при которой на смену одним объектам могут прийти другие. Целью создания динамической информационной модели DIM являлось создание нового средства информационного описания таких моделей.

Так сложилось, что в области обработки данных самыми популярными являются объектно-ориентированные языки программирования, а в области хранения данных — реляционные базы данных.

ORM (Object-relational mapping) — это подход, позволяющий конвертировать данные между реляционными базами данных и объектно-ориентированными языками программирования, тем самым нивелируя так называемый object-relational impedance mismatch (“объектно-реляционное несоответствие”).

На первый взгляд может показаться, что объектная и реляционная модели должны быть хорошо совместимы, но при ближайшем рассмотрении выявляются фундаментальные различия. Во-первых, объекты не обязаны иметь явные идентификаторы. Как правило, за идентификацию объектов отвечает неявный или скрытый указатель `this`, который фактически представляет собой адрес в памяти. В отличие от объектов строки любой таблицы явно идентифицируются при помощи первичных ключей, построенных на некотором множестве атрибутов. Во-вторых, инкапсуляция в реляционных базах данных осуществляется за счет скрытия деталей реализации обработки запросов и других операций над данными, в то время как в объектных системах инкапсуляция работает на уровне объектов (с учетом того, что класс может наследовать поведение от родителей). Но самое главное заключается в том, что реляционная модель является замкнутой системой, в которой результат одной операции — набор кортежей — может служить в качестве входных данных для другой. В частности, благодаря этому возможно использование вложенных операторов `SELECT`. Это невозможно при использовании объектной модели. Также в качестве результата не могут возвращаться частично созданные объекты. Объекты в ООСУБД едины и неделимы, в отличие от РСУБД, которые способны возвращать

данные, описываемые подмножеством колонок таблицы или набора таблиц.

Раньше разработчики пытались связывать объектную и реляционную модели, вручную описывая соответствие (mapping) объектов и таблиц. Одним из ярких примеров подобных действий является выполнение операторов SQL через JDBC (или ADO.NET) и сохранение результатов в полях объектов. Иногда реляционные данные просто принимаются в качестве модели, с которой следует работать, и объекты подстраиваются под этот подход. В своем лексиконе паттернов Фаулер называет эту форму ОР-отображения Row Data Gateway ("шлюз к данным строк таблицы"). Этот подход используется во многих слоях доступа к данным в Java и .NET. Далее появляются программные средства, автоматизирующие ОР-отображения, такие как Hibernate или ADO.NET Entity Framework.

Работа через такие системы зависит от реализации и очень часто не отличается высокой производительностью. Действительно, ORM система берет на себя не только отображение данных между двумя моделями, но и поддерживает целостность, транзакции и декларативный уровень доступа к данным.

Серьезная проблема заключается ещё и в том, что очень сложно спроектировать масштабную модель данных, описывающую ту или иную область, если заранее знать, что придется, либо ограничивать модель в соответствии с возможностями базы данных, либо жертвовать некоторыми функциями базы данных, связанными с выполнением операций над моделью, либо и тем, и другим.

Динамическая информационная модель DIM позволяет описывать любые дискретные объекты и детерминированные процессы, происходящие с этими объектами. Как и ORM система, DIM работает с параметризованными объектами и метаданными. Однако, она не проецирует реляционную модель в объектную, а всего лишь хранит данные в persistent-хранилище. Текущая реализация DIM хранит данные в РСУБД MSSQL и является "надстройкой" над этой БД. Система DIM ограничивается четырьмя базовыми отношениями: наследования, включения, взаимодействия и истории.

Рассмотрим наследование. Разработчикам при ОР-отображении приходится применять один из трех вариантов отображения наследования в реляционную модель: таблица на класс, таблица на конкретный класс и таблица на семейство классов. В первом случае каждому классу в иерархии наследования соответствует отдельная таблица, и объекты порожденных типов устанавливают такую связь путем соединения различных таблиц. Известно, что операция соединения является самой трудоемкой для реляционных БД, и в случае

большого количества объектов в иерархии, необходимо столько операций соединения, сколько таких объектов. Это сильно сказывается на производительности. Второй способ, таблица на конкретный класс, связана с денормализацией и нацелена на замыкание цепочки наследования конкретного класса. При больших объемах данных работа с сильно денормализованными данными неэффективна. Третий способ заключается в создании одной общей таблицы для всех классов в иерархии с поддержкой неопределенных значений. При таком подходе мы отказываемся от ограничений целостности.

В системе DIM наследование реализуется на уровне ядра. Отношение наследования классов порождает отношение наследования объектов, при котором для любого объекта дочернего класса в каждом его родительском классе определяется точно один родительский объект. Родительский объект может быть определен в том же классе дочернего объекта, тогда такое наследование называется внутренним наследованием объектов.

ORM система, в отличие от DIM не берет на себя заботу о "динамике объектов" и лишена понятий "взаимодействие" и "история объектов". Рефакторинг в ORM системе производится над классом, сгенерированным на высокоуровневом языке (Java, .NET). После этого измененные свойства автоматически имплицитно вносятся в базу данных. Если не предусмотреть установку необходимых атрибутов в коде, то целостность данных будет нарушена и соответствие объектной и реляционной модели будет рассинхронизировано. В то же время, разработчик имеет возможность очень легко добавлять методы в класс объекта, регламентируя его поведение на клиенте. В системе DIM данные и метаданные обо всех объектах, параметрах, свойствах и методах находятся в хранилище данных. Кроме того, при изменении любых данных полное состояние сущности сохраняется в отношении истории. Тем самым, имеем возможность работать с различными версиями сущностей. Рассинхронизация на уровне модели невозможна (на уровне данных за этим следит сама система DIM).

Кроме API для работы с данными, DIM имеет несколько реализаций функционального языка ODQL (Object dynamic query language), который схож с SQL и OQL, но имеет множество конструкций, облегчающий работу с иерархическими данными, версионностью, взаимодействиями и т.п. ODQL является объектным языком запросов.

Таким образом, система DIM не может быть заменена ORM системой над реляционной моделью (как и объектной БД). Уникальные свойства и невероятная гибкость в манипулировании объектами делает DIM более привлекательной для разработки приложений со

сложными иерархическими структурами данных и нетривиальным поведением объектов.

Сейчас очень популярным является cloud computing (“облачные вычисления”). Это технология обработки данных, в которой программное обеспечение предоставляется пользователю как Интернет-сервис. Пользователь имеет доступ к собственным данным, но не может управлять и не должен заботиться об инфраструктуре, операционной системе и собственно программном обеспечении, с которым он работает. “Облаком” метафорически называют Интернет, который скрывает все технические детали. В роли хранилища данных в таких сервисах выступают так называемые key/value БД. Например, BigTable от Google или SimpleDb от Amazon. Такие БД нацелены на хранение большого количества простых данных в виде многомерной матрицы “ключ-значение”. Такое решение позволяет производить горизонтальное масштабирование самым простым и эффективным способом. Одна такая БД (в распределенном виде) может содержать более петабайта данных. Однако, так как отношение в такой БД одно (само отношение “ключ-значение”), работа со сложными объектами полностью лежит в слое клиентского приложения на уровне доступа к данным, что неизбежно усложняет разработку. Стоит заметить, что языки запросов в таких БД поддерживают поиск по индексам данных объекта, но десериализация объекта при получении не происходит.

Дальнейшее видение DIM видится в интеграции с хранилищем данных в “облаке” и использованием модели web-сервисов. Таким образом, можно получить выигрыш в производительности, система получит возможность масштабироваться и будет независимой от аппаратных средств.

Список литературы

1. Дарвин Х., Дейт К. Дж. Основы будущих баз данных. Третий манифест (Изд. 2-е) // СУБД. 2004. — № 1. — С. 110–123.
2. Fowler M. Patterns of enterprise application architecture // Addison-Wesley Professional. — November 15, 2002. — С. 213–219.
3. Mark L. Fussell. Foundations of object relational mapping // White Paper. — ChiMu Corp., 1997.
4. Neward T. The Vietnam of computer science // <http://blogs.tedneward.com/2006/06/26/The+Vietnam+Of+Computer+Science.aspx>
5. Chang F., Dean J., Ghemawat S., Hsieh W. C., Wallach D. A., Burrows M., Chandra T., Fikes A., Gruber R. E. Bigtable: a distributed storage system for structured data // OSDI’06: Seventh Symposium on Operating System Design and Implementation. — Seattle, November

2006.

6. Рублев В. С., Юсупов А. Р. Концепции объектной динамической информационной модели DIM // Математика в Ярославском университете: Сборник обзорных статей к 30-летию математического факультета. — Ярославль: ЯрГУ, 2006. — С. 335–354.

7. Писаренко Д. С., Груздов А. А. Архитектура объектно-ориентированной реализации Динамической информационной модели DIM // Современные проблемы математики и информатики. Выпуск 7. — Ярославль, 2005. — С. 204–215.

8. Писаренко Д. С., Рублев В. С. Объектная СУБД Динамическая информационная модель и ее основные концепции // Моделирование и анализ информационных систем. — 2009. — Т. 16, № 1.

ОБ ОДНОМ КЛАССЕ ПСЕВДОЛИНЕЙНЫХ ФУНКЦИЙ

Д. А. Дагаев (Москва)

В настоящей работе рассматривается задача о реализации функций формулами над одним базисом \mathfrak{E} , состоящим из псевдолинейных функций трехзначной логики. Получено точное значение функции Шеннона для класса $[\mathfrak{E}]$. Понятие псевдолинейной функции вводится в [1]. В той же работе приводятся оценки функций Шеннона для всех конечнопорожденных замкнутых классов псевдолинейных функций трехзначной логики за исключением $[\mathfrak{E}]$. Все необходимые определения можно найти в [2, 3].

Пусть $E_k = \{0, 1, \dots, k-1\}$, $k \geq 2$. Обозначим через E_k^n множество всех наборов $\tilde{\alpha} = (\alpha_1, \dots, \alpha_n)$, таких, что $\alpha_1, \dots, \alpha_n \in E_k$. Множество всех функций трехзначной логики обозначим через P_3 , а множество всех функций из P_3 , принимающих значения только из множества E_2 , — через $P_{3,2}$. Пусть $F \subseteq P_3$. Обозначим через $[F]$ замыкание множества F относительно операций суперпозиции и введения несущественной переменной (см. [2]), а через $F(n)$ — множество всех функций из F , зависящих от переменных x_1, \dots, x_n , $n \geq 1$.

Пусть $f(x_1, \dots, x_n) \in P_{3,2}$. Проекцией функции $f(x_1, \dots, x_n)$ называется такая булева функция $(prf)(x_1, \dots, x_n)$, значение которой на произвольном наборе $\tilde{\alpha} \in E_2^n$ определяется равенством $(prf)(\tilde{\alpha}) = f(\tilde{\alpha})$. В дальнейшем функцию $(prf)(x_1, \dots, x_n)$ будем обозначать через $prf(x_1, \dots, x_n)$. Проекцией prF множества функций $F \subseteq P_{3,2}$ называется множество $\bigcup \{prf\}$, где объединение берется по всем функциям $f \in F$. Нетрудно убедиться, что для любого замкнутого класса

$F \subseteq P_{3,2}$ множество prF является замкнутым классом булевых функций. Положим $\mathcal{L} = \{f \in P_{3,2} | prf \in L\}$. Функция $f(x_1, \dots, x_n) \in P_{3,2}$ называется псевдолинейной, если $f \in \mathcal{L}$.

Обозначим через $j_i(x)$ функцию из $P_{3,2}$, равную 1 при $x = i$ и 0 в остальных случаях, $i \in E_3$, а через $x + y$ и $x \cdot y$ — функции из $P_{3,2}$, такие, что для любых $\alpha, \beta \in E_3$ выполняются равенства $\alpha + \beta = j_1(\alpha) \oplus j_1(\beta)$ и $\alpha \cdot \beta = j_1(\alpha) \& j_1(\beta)$ соответственно.

Определим псевдолинейные функции $\lambda(x, y)$, $\mu(x, y)$ и $1(x)$ следующим образом. Положим $\lambda(x, y) = j_1(x) + j_1(y)$, $\mu(x, y) = j_1(x)j_2(y)$. Обозначим через $1(x)$ псевдолинейную функцию, тождественно равную единице. Положим $\mathfrak{C} = \{1(x), \lambda(x, y), \mu(x, y)\}$ и $L_2 = [\mathfrak{C}]$.

Опишем множество всех функций, принадлежащих классу L_2 . Пусть $f(x_1, \dots, x_n) \in L_2$. Нетрудно видеть, что выполняется равенство

$$f(x_1, \dots, x_n) = \sum j_{\sigma_1}(x_1) \cdot \dots \cdot j_{\sigma_n}(x_n),$$

где суммирование производится по всем наборам $\tilde{\sigma} = (\sigma_1, \dots, \sigma_n) \in E_3^n$, таким, что $f(\tilde{\sigma}) = 1$. Заменим каждое вхождение функции $j_0(y)$ в правой части этого равенства на равную ей функцию $1 + j_1(y) + j_2(y)$ и раскроем скобки. Получим представление функции $f(x_1, \dots, x_n)$ в следующем виде:

$$f(x_1, \dots, x_n) = \eta_f(x_1, \dots, x_n) + \delta_f(x_1, \dots, x_n),$$

где

$$\eta_f(x_1, \dots, x_n) = a + \sum_{i=1}^n a_i j_1(x_i), \quad \delta_f(x_1, \dots, x_n) = \sum_{I, J} a_{I, J} \kappa_{I, J}(x_1, \dots, x_n),$$

$$\kappa_{I, J}(x_1, \dots, x_n) = \left(\prod_{i \in I} j_1(x_i) \right) \cdot \left(\prod_{j \in J} j_2(x_j) \right)$$

$a, a_i, a_{I, J} \in \{0, 1\}$, а суммирование в определении функции δ_f производится по всем множествам I, J , таким, что $I \cup J \subseteq \{1, \dots, n\}$, $I \cap J = \emptyset$, $J \neq \emptyset$. В случае $a_{I, J} = 1$ функция $\kappa_{I, J}(x_1, \dots, x_n)$ называется компонентой функции f . Множество всех компонент функции f будем обозначать через K_f . Положим $K = \bigcup K_f$, где объединение берется по всем псевдолинейным функциям f . Известно [3], что

$$L_2 = \{f \in \mathcal{L} | K_f \subseteq \{\kappa_{I, J} \in K \mid |I| \leq 1\}\}.$$

Обозначим через $L_{\mathfrak{C}}(L_2(n))$ функцию Шеннона для класса L_2 .

Теорема. При всех $n \geq 2$ имеет место соотношение

$$L_{\mathfrak{C}}(L_2(n)) = n2^{n-1} + 2^{n+1} - 1.$$

Автор выражает благодарность проф. А. Б. Угольникову за внимание к работе.

Работа выполнена при финансовой поддержке РФФИ (проект 08-01-00863), программы поддержки ведущих научных школ РФ (проект НШ-4470.2008.1) и программы фундаментальных исследований ОМН РАН «Алгебраические и комбинаторные методы математической кибернетики» (проект «Задачи оптимального синтеза управляющих систем»).

Список литературы

1. Дагаев Д. А. Оценки сложности псевдолинейных функций // Материалы VII молодежной научной школы по дискретной математике и ее приложениям. Часть 1. — С. 28–30.

2. Яблонский С. В. Введение в дискретную математику. — М.: Высшая школа, 2008.

3. Lau D. Function Algebras on Finite Sets. — Berlin: Springer-Verlag, 2006.

О СЛОЖНОСТИ РЕАЛИЗАЦИИ БУЛЕВЫХ ФУНКЦИЙ КОНТАКТНЫМИ СХЕМАМИ С ОГРАНИЧЕНИЯМИ НА СТРУКТУРУ

А. Б. Дайняк, Д. С. Романов, М. С. Шуплецов (Москва)

Одной из основных задач современной микроэлектроники является реализация того или иного управляющего устройства схемой на кристалле с учетом имеющихся технологических ограничений. Такими ограничениями являются, например, условия, накладываемые на минимальное расстояние между транзисторами на кристалле, расположение проводников. Математически эту задачу можно рассматривать в следующей постановке. Имеется набор множеств конструктивных объектов (S_1, \dots, S_r) , и набор функций $(\phi_1, \dots, \phi_{r-1})$. Функция ϕ_i ставит каждому объекту $\Sigma_i \in S_i$ подмножество $S_{i+1}|_{\Sigma_i} \subseteq S_{i+1}$. Объект Σ_i можно назвать *каркасом* для любого из объектов $\Sigma \in S_{i+1}|_{\Sigma_i}$. При этом последовательность объектов

$$\Sigma_1 \in S_1, \Sigma_2 \in S_2|_{\phi_1(\Sigma_1)}, \dots, \Sigma_r \in S_r|_{\phi_{r-1}(\Sigma_{r-1})}$$

моделирует процесс построения объекта Σ_r за счет постепенного уточнения его структуры. На каждом из множеств S_i можно ввести функционал сложности \mathcal{L}_i , тогда можно говорить о *цепочке синтеза схемы* Σ_r с учетом минимизации величин $\mathcal{L}_i(\Sigma_i)$.

Например, пусть S_1 — множество мультиграфов, а S_2 — множество всех контактных схем, получающихся всевозможными помечиваниями мультиграфов из S_1 . Функция ϕ_1 ставит в соответствие мультиграфу $G \in S_1$ множество КС из S_2 , получающихся помечиваниями графа G . Вводя различные ограничения на множество S_1 , мы вводим ограничения на структуру КС. В качестве ограничений на структуру можно рассмотреть запреты на подграфы, порожденные подграфы или миноры определенного типа. Так, например, запрет на звезды $K_{1,t}$ в качестве подграфов мультиграфов из S_1 соответствует ограничению на степени вершин в синтезируемых КС (задача синтеза схем из таких классов была рассмотрена в [2]). Запрещая миноры K_5 и $K_{3,3}$ в графах из S_1 , приходим к планарным КС.

Обозначим через E_2 множество $\{0, 1\}$. Через $P_2(n)$ будем обозначать булевы функции от переменных x_1, \dots, x_n . Класс всех планарных мультиграфов обозначим через \mathcal{P} .

Внешнепланарным называется планарный граф, для которого существует плоская укладка, в которой все вершины графа принадлежат одной грани (обычно в качестве такой грани рассматривается внешняя). Класс всех внешнепланарных мультиграфов обозначим \mathcal{OP} (от англ. outerplanar).

Планарной (внешнепланарной) контактной схемой назовем КС, граф которой является планарным (соответственно, внешнепланарным).

Цепной контактной схемой будем называть такую двухполюсную КС, что лежащий в ее основе граф может быть уложен без пересечений ребер в полуплоскости так, чтобы все вершины графа лежали на прямой, ограничивающей эту полуплоскость, причем все вершины КС лежали между полюсами. Отметим, что любая цепная КС является внешнепланарной. Класс цепных КС обозначим через $\mathcal{U}_G^{\text{КС}}$. Для класса графов \mathcal{G} через $\mathcal{U}_G^{\text{КС}}$ обозначим класс контактных схем, полученных в результате размечивания графов из \mathcal{G} . Пусть \mathcal{L} — функционал сложности, определенный на $\mathcal{U}_G^{\text{КС}}$. Функция Шеннона для класса схем $\mathcal{U}_G^{\text{КС}}$ относительно функционала сложности \mathcal{L} вводится стандартным образом:

$$L_G^{\text{КС}}(n) = \max_{f \in P_2(n)} \min_{\substack{\Sigma \in \mathcal{U}_G^{\text{КС}} \\ \Sigma \text{ реализует } f}} \mathcal{L}(\Sigma).$$

Везде далее в качестве функционала сложности выступает число контактов в схеме.

Обозначим через $\log^{[k]} x$ функцию $\underbrace{\log_2 \log_2 \dots \log_2 x}_{k \text{ раз}}$. Для удобства

положим по определению $\log^{[0]} n = n$.

Теорема 1. *Для любого фиксированного k при всех достаточно больших n справедлива оценка*

$$L_C^{KC}(n) \lesssim 2^n \log^{[k]} n.$$

Доказательство. Для краткости положим $L(n) = L_G^{KC}(n)$. Для произвольной булевой функции $f(x_1, \dots, x_n)$ справедливо разложение

$$f(x_1, \dots, x_n) = \bigwedge_{(\sigma_1, \dots, \sigma_t) \in E_2^t} (x_1^{\bar{\sigma}_1} \vee \dots \vee x_t^{\bar{\sigma}_t} \vee f(\sigma_1, \dots, \sigma_t, x_{t+1}, \dots, x_n)).$$

Если функции $f(\sigma_1, \dots, \sigma_t, x_{t+1}, \dots, x_n)$ уже реализованы цепными схемами $U_{(\sigma_1, \dots, \sigma_t)}$, то цепную схему для функции $f(x_1, \dots, x_n)$ можно построить, соединив последовательно блоки, получающиеся из схем $U_{(\sigma_1, \dots, \sigma_t)}$ добавлением параллельных контактов, помеченных буквами $x_1^{\bar{\sigma}_1}, \dots, x_t^{\bar{\sigma}_t}$. Отсюда вытекает неравенство

$$L(n) \leq 2^t(t + L(n - t)),$$

справедливое при всех t , $1 \leq t \leq n - 1$. Отсюда индукцией по k несложно вывести утверждение теоремы. Базу индукции составляет случай $k = 0$, в котором, рассмотрев КС, построенную для функции f по совершенной КНФ, получаем оценку $L(n) \leq n2^n$. Пусть утверждение теоремы выполнено для $k = k_0$. Тогда

$$L(n) \leq 2^t(t + L(n - t)) \lesssim t \cdot 2^t + 2^n \log^{[k_0]}(n - t).$$

Положив $t = \lceil n - \log_2 n \rceil$, получаем

$$L(n) \lesssim \frac{2^n(n - \log_2 n)}{n} + 2^n \log^{[k_0+1]} n \lesssim 2^n \log^{[k_0+1]} n.$$

Теорема 2. *Справедливы соотношения*

$$L_{\mathcal{P}}^{KC}(n) \sim L_{\mathcal{OP}}^{KC}(n) \sim \frac{2^n}{\log_2 n}.$$

Доказательство. Поскольку при всех n справедливо очевидное неравенство $L_{\mathcal{P}}^{\text{KC}}(n) \leq L_{\mathcal{OP}}^{\text{KC}}(n)$, то достаточно обосновать совпадающие асимптотическую нижнюю оценку для $L_{\mathcal{P}}^{\text{KC}}(n)$ и верхнюю оценку для $L_{\mathcal{OP}}^{\text{KC}}(n)$. Нижняя оценка $L_{\mathcal{P}}^{\text{KC}}(n)$ может быть получена мощностным методом [4]. Число планарных простых непомеченных графов с p вершинами не превосходит 33^p (см., например, [1]). Отсюда следует, что число связных планарных простых графов с не более чем L ребрами не превосходит 33^{L+1} . Планарный мультиграф можно получить, заменяя в простом планарном графе некоторые ребра кратными. Количество упорядоченных разбиений числа L на слагаемые не превосходит 2^L , откуда следует верхняя оценка 66^{L+2} на число связных планарных мультиграфов с не более чем L ребрами. Для каждого такого мультиграфа существует менее $L^2 \cdot (2n)^L$ способов выбрать два полюса и пометить все ребра элементами множества $\{x_1, \dots, x_n, \bar{x}_1, \dots, \bar{x}_n\}$. Таким образом, число $N(n, L)$ планарных КС, реализующих функцию n переменных, и имеющих сложность не выше L , не превосходит $L^2 \cdot (132n)^{L+2}$. Очевидное соотношение $N(n, L_{\mathcal{P}}^{\text{KC}}(n)) \geq 2^{2^n}$ влечет неравенство $(L_{\mathcal{P}}^{\text{KC}}(n))^2 \cdot (132n)^{L_{\mathcal{P}}^{\text{KC}}(n)+2} > 2^{2^n}$, откуда следует нижняя асимптотическая оценка $L_{\mathcal{P}}^{\text{KC}}(n) \gtrsim \frac{2^n}{\log_2 n}$.

Докажем теперь, что $L_{\mathcal{OP}}^{\text{KC}}(n) \lesssim \frac{2^n}{\log_2 n}$. Воспользуемся техникой, приведенной в работах [3, 4]. Пусть $f, f \in P_2(n)$, — произвольная функция. Разобьем множество переменных $x = (x_1, \dots, x_n)$ на две группы $x' = (x_1, \dots, x_q)$ и $x'' = (x_{q+1}, \dots, x_n)$.

Определим m -регулярное разбиение $\Delta = (\delta_1, \dots, \delta_{2^{q-m}})$ куба E_2^q следующим образом [3]. Компонента δ_1 содержит 2^m наборов, и префиксы длины m этих наборов попарно различны. В этом случае множеству наборов δ_1 соответствует система функций от m переменных. Выберем множество δ_1 так, чтобы эта система функций образовывала дизъюнктивно-универсальное множество [3] порядка $(q - m)$ ранга p . Это можно сделать, если для некоторого s выполнены соотношения $p = \lceil \frac{2^m}{s} \rceil$ и $q = m + p2^s$. Каждая из остальных компонент разбиения Δ получается по координатным сложением всех наборов компоненты δ_1 с некоторым ненулевым набором из E_2^q , первые m координат которого равны нулю. Обозначим через χ_i функцию от переменных x' , равную нулю на наборах, принадлежащих i -й компоненте разбиения Δ , и единице на остальных наборах.

Рассмотрим представление функции f в виде

$$f(x) = \bigwedge_{i=1}^{2^{q-m}} \left(\chi_i(x') \vee \bigwedge_{\sigma''=(\sigma_{q+1}, \dots, \sigma_n)} \left(x_{q+1}^{\bar{\sigma}_{q+1}} \vee \dots \vee x_n^{\bar{\sigma}_n} \vee f_{\sigma''}(x') \right) \right).$$

На наборах из i -й компоненты разбиения Δ каждая из функций $f_{\sigma''}(x')$ совпадает с некоторой элементарной дизъюнкцией $J_{\sigma'', i}$ ранга p от переменных x_{m+1}, \dots, x_q . Каждая из функций χ_i может быть реализована совершенной КНФ \mathfrak{A}_i . В итоге для функции f получаем формулу с поднятыми отрицаниями

$$f(x) = \bigwedge_{i=1}^{2^{q-m}} \left(\mathfrak{A}_i \vee \bigwedge_{\sigma''=(\sigma_{q+1}, \dots, \sigma_n)} \left(x_{q+1}^{\bar{\sigma}_{q+1}} \vee \dots \vee x_n^{\bar{\sigma}_n} \vee J_{\sigma'', i} \right) \right).$$

Можно проверить, что π -схема, моделирующая приведенную выше формулу, является внешнепланарной, и её сложность не превосходит

$$2^{q-m} \cdot (q \cdot 2^m + 2^{n-q}(n - q + p)).$$

Выбирая значения параметров: $m = \lfloor 3 \log_2 \log_2 n \rfloor$, $s = \lfloor \log_2(n - 2 \log_2 n) - 2 \log_2 \log_2 n \rfloor$, получаем, что сложность полученной π -схемы может быть оценена следующим образом:

$$\frac{2^n}{\log_2(n - 2 \log_2 n) - \log_2 \log_2 n} + O\left(\frac{2^n}{n}\right) = \frac{2^n}{\log_2 n} \left(1 + O\left(\frac{\log n}{n}\right)\right).$$

Теорема доказана.

Работа выполнена при финансовой поддержке РФФИ (гранты 07-01-00444а, 09-01-00817а).

Список литературы

1. Bonichon N., Gavoille C., Hanusse N. An information-theoretic upper bound of planar graphs using triangulation // 20 Annual Symposium on Theoretical Aspects of Computer Science (STACS). LNCS — Springer, February 2003. — V. 2607. — P. 499–510.

2. Коршунов А. Д. Об асимптотических оценках сложности контактных схем заданной степени // Дискретный анализ. Вып. 5. — Новосибирск: Ин-т математики, 1965. — С. 35–63.

3. Ложкин С. А. Лекции по основам кибернетики. — М.: Издательский отдел ф-та ВМиК МГУ им. М. В. Ломоносова, 2004.

4. Лупанов О. Б. Асимптотические оценки сложности управляющих систем. — М.: Изд-во МГУ, 1984.

О КОНЕЧНОЙ ПОРОЖДЕННОСТИ ПРЕДПОЛНЫХ КЛАССОВ МОНОТОННЫХ ФУНКЦИЙ ДЕВЯТИЗНАЧНОЙ ЛОГИКИ

О. С. Дудакова (Москва)

Известно, что каждый замкнутый класс булевых функций имеет конечный базис [1, 2]. В многозначных логиках этот результат не сохраняется: для любого $k \geq 3$ в P_k существуют замкнутые классы, не являющиеся конечно-порожденными [3]. К настоящему времени отсутствует полное описание конечно-порожденных классов функций многозначной логики даже для семейства всех предполных классов; описание семейства всех предполных классов см. в [4]. При $k \leq 7$ все предполные классы в P_k являются конечно-порожденными [5], а начиная с $k = 8$ существуют предполные классы монотонных функций, не имеющие конечного базиса [6] (см. также [7–9]). В данной работе получен критерий конечной порожденности для семейства всех предполных классов монотонных функций в P_k , где $k \leq 9$.

Пусть \mathcal{P} — некоторое частично упорядоченное множество с отношением порядка \leq . Пусть $a_1, a_2 \in \mathcal{P}$, элементы a_1 и a_2 несравнимы. Элемент $b \in \mathcal{P}$ называется *верхней гранью* элементов a_1, a_2 , если выполняются неравенства $b \geq a_1$ и $b \geq a_2$. Верхняя грань b элементов a_1, a_2 называется *минимальной верхней гранью* этих элементов, если ни для какой другой верхней грани x этих элементов не выполняется неравенство $b > x$; b называется *точной верхней гранью* a_1, a_2 (обозначение $\sup(a_1, a_2)$), если для любой верхней грани x этих элементов выполняется неравенство $b \leq x$.

Через $|\mathcal{P}|$ будем обозначать число элементов множества \mathcal{P} . Положим $w_{\mathcal{P}} = \max |J|$, где максимум берется по всем антицепям J множества \mathcal{P} ; величину $w_{\mathcal{P}}$ будем называть *шириной* множества \mathcal{P} .

Через $\mathcal{M}_{\mathcal{P}}$ будем обозначать класс всех функций, монотонных относительно частично упорядоченного множества \mathcal{P} . Обозначим через \mathbb{A} семейство всех частично упорядоченных множеств с наименьшим и наибольшим элементами. Отметим, что класс $\mathcal{M}_{\mathcal{P}}$ является предполным тогда и только тогда, когда $\mathcal{P} \in \mathbb{A}$ [4]. Наименьший и наибольший элементы множества $\mathcal{P} \in \mathbb{A}$ будем обозначать через 0

и 1 соответственно. Далее, обозначим через \mathbb{A}_1 семейство всех множеств $\mathcal{P} \in \mathbb{A}$, не содержащих шестерки элементов $a_1, a_2, b_1, b_2, c_1, c_2$, где a_1 и a_2 — несравнимые элементы, b_1 и b_2 — минимальные верхние грани элементов a_1 и a_2 , а c_1 и c_2 — минимальные верхние грани элементов b_1 и b_2 .

Теорема. Пусть $\mathcal{P} \in \mathbb{A}$, $|\mathcal{P}| \leq 9$. Класс $\mathcal{M}_{\mathcal{P}}$ является конечно-порожденным тогда и только тогда, когда $\mathcal{P} \in \mathbb{A}_1$.

Доказательство. Обозначим через \mathbb{A}_2 семейство всех множеств $\mathcal{P} \in \mathbb{A}$, которые не содержат четверки элементов a_1, a_2, a_3, a_4 , таких что $a_1, a_2 < a_3$, элементы a_1 и a_2 не имеют точной верхней грани и элементы a_3 и a_4 не имеют точной верхней грани. Легко видеть, что $\mathbb{A}_2 \subset \mathbb{A}_1$. В работе [10] показано, что для любого множества $\mathcal{P} \in \mathbb{A}_2$ класс $\mathcal{M}_{\mathcal{P}}$ содержит некоторую мажоритарную функцию, а значит, является конечно-порожденным [11]. Таким образом, для доказательства теоремы достаточно рассмотреть случай $\mathcal{P} \notin \mathbb{A}_2$.

В силу соотношения $\mathcal{P} \notin \mathbb{A}_2$ в \mathcal{P} содержится четверка элементов a_1, a_2, a_3, a_4 , таких что $a_1, a_2 < a_3$ и при этом не существует $\sup(a_1, a_2)$ и не существует $\sup(a_3, a_4)$. Пусть b_1 и b_2 — минимальные верхние грани элементов a_1 и a_2 . Из неравенства $|\mathcal{P}| \leq 9$ следует, что по крайней мере один из элементов a_3, a_4 является минимальной верхней гранью элементов a_1, a_2 . Поэтому возможны два случая: либо оба элемента a_3 и a_4 являются минимальными верхними гранями элементов a_1, a_2 , либо один из элементов a_3, a_4 является минимальной верхней гранью элементов a_1, a_2 , а другой — не является.

Предположим, что a_3 и a_4 являются минимальными верхними гранями элементов a_1, a_2 , т. е. $\{a_3, a_4\} = \{b_1, b_2\}$. Тогда $\mathcal{P} \notin \mathbb{A}_1$. Покажем, что в этом случае класс $\mathcal{M}_{\mathcal{P}}$ не является конечно-порожденным.

Из соотношений $\mathcal{P} \notin \mathbb{A}_1$ и $|\mathcal{P}| \leq 9$ следует, что $2 \leq w_{\mathcal{P}} \leq 3$. При этом если $w_{\mathcal{P}} = 3$, то $|\mathcal{P}| = 9$. Рассмотрим три случая.

1. Пусть $w_{\mathcal{P}} = 2$. Тогда, согласно критерию конечной порожденности предполных классов функций, монотонных относительно множеств ширины два [7–9], класс $\mathcal{M}_{\mathcal{P}}$ не имеет конечного базиса.

2. Пусть $w_{\mathcal{P}} = 3$ и пусть множество \mathcal{P} представляется в виде объединения "слоев", т. е. непересекающихся подмножеств, состоящих из попарно несравнимых элементов, причем любые два элемента из разных подмножеств сравнимы между собой. Тогда, согласно результату из работы [12], класс $\mathcal{M}_{\mathcal{P}}$ не имеет конечного базиса.

3. Пусть теперь $w_{\mathcal{P}} = 3$ и для множества \mathcal{P} не выполняются условия предыдущего случая. Обозначим через c_1 и c_2 минимальные верхние грани элементов b_1 и b_2 . Положим $\mathcal{P}' = \{0, a_1, a_2, b_1, b_2, c_1, c_2, 1\}$. Заметим, что класс $\mathcal{M}_{\mathcal{P}'}$ не имеет конечного

базиса [6]. Можно показать, что в этом случае существует такое монотонное отображение $\varphi : \mathcal{P} \rightarrow \mathcal{P}'$, что для каждого элемента $x \in \mathcal{P}'$ выполняется равенство $\varphi(x) = x$, а также существует взаимно однозначное монотонное отображение $\xi : \mathcal{P} \rightarrow \mathcal{P}'_\xi$, где $\mathcal{P}'_\xi \subset \mathcal{P}'^2$, такое что обратное отображение $\xi^{-1} : \mathcal{P}'_\xi \rightarrow \mathcal{P}$ доопределяется до монотонного отображения $\Xi : \mathcal{P}'^2 \rightarrow \mathcal{P}$. Следовательно [13–15], класс $\mathcal{M}_\mathcal{P}$ не имеет конечного базиса.

Пусть теперь один из элементов a_3 и a_4 является минимальной верхней гранью элементов a_1, a_2 , а другой — не является. Легко видеть, что в этом случае $|\mathcal{P}| = 9$, $2 \leq w_\mathcal{P} \leq 3$. Без ограничения общности будем считать, что $a_3 = b_1$, $a_4 \neq b_2$. Рассмотрим два случая.

1. Пусть элементы a_4 и b_2 сравнимы. В этом случае $w_\mathcal{P} = 2$. Легко видеть, что $\mathcal{P} \notin \mathbb{A}_1$. Тогда, согласно критерию из работ [7–9], класс $\mathcal{M}_\mathcal{P}$ не является конечно-порожденным.

2. Пусть теперь элементы a_4 и b_2 несравнимы. Тогда $w_\mathcal{P} = 3$. В этом случае выполняется соотношение $\mathcal{P} \in \mathbb{A}_1$. Нетрудно показать, что класс $\mathcal{M}_\mathcal{P}$ содержит мажоритарную функцию, зависящую от 7 переменных. А значит, класс $\mathcal{M}_\mathcal{P}$ является конечно-порожденным.

Таким образом, теорема доказана.

Работа выполнена при финансовой поддержке РФФИ (проект 08-01-00863), программы поддержки ведущих научных школ РФ (проект НШ-4470.2008.1) и программы фундаментальных исследований ОМН РАН «Алгебраические и комбинаторные методы математической кибернетики и информационные системы нового поколения» (проект «Задачи оптимального синтеза управляющих систем»).

Список литературы

1. Post E. L. Introduction to a general theory of elementary propositions // Amer. J. Math. — 1921. — V. 43, № 3. — P. 163–185.
2. Post E. L. The two-valued iterative systems of mathematical logic // Ann. Math. Stud. Princeton Univ. Press. — 1941. — V. 5.
3. Янов Ю. И., Мучник А. А. О существовании k -значных замкнутых классов, не имеющих конечного базиса // ДАН СССР. — 1959. — Т. 127, № 1. — С. 44–46.
4. Яблонский С. В., Гаврилов Г. П., Набебин А. А. Предполные классы в многозначных логиках. — М.: Изд-во МЭИ, 1997.
5. Lau D. Bestimmung der Ordnung maximaler Klassen von Funktionen der k -wertigen Logik // Z. math Log. und Grundl. Math. — 1978. — 24. — S. 79–96.

6. Tardos G. A not finitely generated maximal clone of monotone operations // Order. — 1986. — V. 3. — P. 211–218.

7. Дудакова О. С. О свойствах предполных классов монотонных функций k -значной логики // Тр. VII Междунар. конф. "Дискретные модели в теории управляющих систем" (Покровское, 4–6 марта 2006 г.). — М.: МАКС Пресс. — 2006. — С. 107–113.

8. Дудакова О. С. О классах функций k -значной логики, монотонных относительно множеств ширины два // Вестн. Моск. ун-та. Серия 1. Математика. Механика. — 2008. — № 1. — С. 31–37.

9. Дудакова О. С. О конечной порожденности предполных классов монотонных функций многозначной логики // Математические вопросы кибернетики. Вып. 17. — М.: Физматлит, 2008. — С. 13–104.

10. Demetrovics J., Hannák L., Rónyai L. On algebraic properties of monotone clones // Order. — 1986. — V. 3. — P. 219–225.

11. Baker K., Pixley A. Polynomial interpolation and the Chinese remainder theorem for algebraic systems // Math. Z. — 1975. — V. 143. — P. 165–174.

12. Дудакова О. С. Семейства предполных классов монотонных функций в P_k , не имеющих конечного базиса // Тр. XXVIII Конф. молодых ученых мех.-матем. ф-та МГУ (10–15 апреля 2006 г.). — М.: Изд-во ЦПИ при мех.-матем. ф-те МГУ. — 2006. — С. 55–59.

13. Дудакова О. С. О конечной порожденности замкнутых классов монотонных функций в P_k // Тезисы докладов XV Междунар. конф. "Проблемы теоретической кибернетики" (Казань, 2–7 июня 2008 г.). — Казань: Отечество. — 2008. — С. 29.

14. Дудакова О. С. О конечной порожденности замкнутых классов монотонных функций k -значной логики // Тр. VIII Междунар. конф. "Дискретные модели в теории управляющих систем" (Москва, 6–9 апреля 2009 г.). — М.: МАКС Пресс. — 2009. — С. 81–82.

15. Дудакова О. С. О конечной порожденности замкнутых классов монотонных функций в P_k // Учен. зап. Казан. ун-та. Серия Физ.-матем. науки. — 2009. — Т. 151, кн. 2. — С. 65–71.

О СВОЙСТВАХ МАТРИЦЫ ПЕРВЫХ МОМЕНТОВ И ДЕРЕВЬЕВ ВЫВОДА ДЛЯ РАЗЛОЖИМОЙ СТОХАСТИЧЕСКОЙ КС-ГРАММАТИКИ В КРИТИЧЕСКОМ СЛУЧАЕ

Л. П. Жильцова, А. А. Рызаев (Нижний Новгород)

В [1] рассматривались свойства деревьев вывода слов стохастического контекстно-свободного языка (стохастического КС-языка), при условии, что матрица первых моментов порождающей грамматики неразложима, непериодична, и ее перронов корень строго равен единице e (критический случай). При неразложимой матрице первых моментов нетерминальные символы грамматики образуют один класс.

В настоящей работе рассматриваются стохастические КС-грамматики с произвольным числом классов нетерминальных символов без ограничений на порядок следования классов.

Стохастической КС-грамматикой называется система $G = \langle V_T, V_N, R, s \rangle$, где V_T и V_N — конечные множества терминальных и нетерминальных символов (терминалов и нетерминалов) соответственно; $s \in V_N$ — аксиома, $R = \cup_{i=1}^k R_i$, где k — мощность алфавита V_N и R_i — множество правил с одинаковой левой частью A_i . Каждое правило r_{ij} из R_i имеет вид

$$r_{ij} : A_i \xrightarrow{p_{ij}} \beta_{ij}, \quad j = 1, \dots, n_i,$$

где $A_i \in V_N$, $\beta_{ij} \in (V_T \cup V_N)^*$ и p_{ij} — вероятность применения правила r_{ij} (вероятность правила r_{ij}), причем $0 < p_{ij} \leq 1$ и $\sum_{j=1}^{n_i} p_{ij} = 1$.

Применение правила грамматики к слову в алфавите $V_T \cup V_N$ состоит в замене вхождения нетерминала из левой части правила на слово, стоящее в его правой части. КС-язык определяется как множество всех слов в алфавите V_T , выводимых из аксиомы s с помощью конечного числа применений правил грамматики.

Каждому слову α КС-языка соответствует последовательность правил грамматики (вывод), с помощью которой α выводится из аксиомы s . Левым выводом называется вывод, в котором каждое правило применяется к самому левому нетерминалу в слове.

Вероятность вывода определяется как произведение вероятностей правил, образующих вывод.

Дерево вывода строится по левому выводу слова следующим образом. Корень дерева помечается аксиомой s . Пусть при выводе слова α на очередном шаге в процессе левого вывода применяется

правило $A_i \xrightarrow{p_{ij}} b_{i_1} b_{i_2} \dots b_{i_m}$, где $b_{i_l} \in V_N \cup V_T$ ($l = 1, \dots, m$). Тогда из самой левой вершины-листа дерева, помеченной символом A_i (при обходе листьев дерева слева направо), проводится m дуг в вершины следующего яруса, которые помечаются слева направо символами $b_{i_1}, b_{i_2}, \dots, b_{i_m}$ соответственно. После построения дуг и вершин для всех правил грамматики в выводе слова языка само слово получается при обходе листьев дерева слева направо. Высотой дерева называется максимальная длина пути от корня к листу.

По стохастической КС-грамматике строится матрица первых моментов. Для матрицы A первых моментов ее элемент a_i^j определяется как $\sum_j p_{ij} s_l^{(ij)}$, где величина $s_l^{(ij)}$ равна числу нетерминальных символов A_l в правой части правила r_{ij} . По смыслу значение элемента a_i^j есть математическое ожидание числа нетерминальных символов A_l в правых частях правил грамматики с одинаковым нетерминалом A_i в левой части.

Перронов корень матрицы первых моментов обозначим через r . Рассматривается случай $r = 1$.

Введем некоторые обозначения. Будем говорить, что нетерминал A_j непосредственно следует за нетерминалом A_i (и обозначать $A_i \rightarrow A_j$), если в грамматике существует правило вида $A_i \xrightarrow{p_{ij}} \alpha_1 A_j \alpha_2$, где $\alpha_1, \alpha_2 \in (V_T \cup V_N)^*$. Рефлексивное транзитивное замыкание отношения \rightarrow обозначим \rightarrow_* .

Классом нетерминалов назовем максимальное по включению подмножество $K \subseteq V_N$ такое, что $A_i \rightarrow_* A_j$ для любых $A_i, A_j \in K$. Для различных классов нетерминалов K_1 и K_2 будем говорить, что класс K_2 непосредственно следует за классом K_1 (и обозначать $K_1 \prec K_2$), если существуют $A_1 \in K_1$ и $A_2 \in K_2$, такие, что $A_1 \rightarrow A_2$. Рефлексивное транзитивное замыкание отношения \prec обозначим через \prec_* и назовем отношением следования.

Пусть $\{K_1, K_2, \dots, K_m\}$ — множество классов нетерминалов грамматики, $m \geq 2$. Будем полагать, что классы нетерминалов перенумерованы таким образом, что $K_i \prec K_j$ тогда и только тогда, когда $i < j$.

В общем случае соответствующая разложимой грамматике матрица первых моментов A имеет следующий вид:

$$A = \begin{pmatrix} A_{11} & A_{12} & \dots & A_{1m-1} & A_{1m} \\ 0 & A_{22} & \dots & A_{2m-1} & A_{2m} \\ \dots & \dots & \dots & \dots & \dots \\ 0 & 0 & \dots & A_{m-1m-1} & A_{m-1m} \\ 0 & 0 & \dots & 0 & A_{mm} \end{pmatrix}. \quad (1)$$

Один класс нетерминалов представлен в матрице множеством подряд идущих строк и соответствующим множеством столбцов с теми же номерами. Для класса K_i квадратная подматрица, образованная соответствующими строками и столбцами, обозначается через A_{ii} . Подматрица A_{ij} является нулевой, если $K_i \not\prec K_j$. Блоки, расположенные ниже главной диагонали, нулевые в силу упорядоченности классов.

Для каждого класса K_i матрица A_{ii} неразложима. Без ограничения общности будем считать, что она строго положительна и непериодична. Этого всегда можно добиться, применяя метод укрупнения правил грамматики, описанный в [1].

Обозначим через r_i перронов корень матрицы A_{ii} . Для неразложимой матрицы перронов корень является действительным и простым [2]. В силу структуры матрицы первых моментов $r = \max_i \{r_i\}$, и $r > 0$.

Пусть $J = \{i_1, i_2, \dots, i_l\}$ — множество всех номеров i_j классов, для которых $r_{i_j} = r$.

Зафиксируем пару (l, h) , $l, h \in \{1, 2, \dots, m\}$, и рассмотрим всевозможные последовательности классов $K_{i_1} \prec K_{i_2} \prec \dots \prec K_{i_s}$, где $i_1 = l, i_s = h$. Среди всех таких последовательностей выберем ту, которая содержит наибольшее число классов с номерами из J . Это число обозначим через s_{lh} .

Дополнительно переупорядочим классы по неубыванию величины s_{1l} , причем при одинаковых значениях s_{1l} сначала поставим классы с номерами из J .

Рассмотрим подматрицу A_{lh} матрицы первых моментов A . Запись $A_{lh}^{(t)}$ будем применять для обозначения соответствующей подматрицы матрицы A^t .

Теорема 1. При $t \rightarrow \infty$

$$A_{lh}^{(t)} = H_{lh} \cdot t^{s_{lh}-1} + o(t^{s_{lh}-1}),$$

где H_{lh} — матрица, не зависящая от t .

Рассмотрим всевозможные последовательности классов $K_{i_1} \prec K_{i_2} \prec \dots \prec K_{i_s}$, где $i_1 = i$. Среди всех таких последовательностей выберем ту, которая содержит наибольшее число классов с номерами из J . Это число обозначим через q_i . Множество последовательностей, содержащих q_1 классов с номерами из J , обозначим через \mathcal{M} . Последовательности из \mathcal{M} будем называть максимальными путями.

Через $Q_i(t)$ обозначим вероятность множества деревьев вывода, высота которых больше t , и корень помечен нетерминалом A_i . Эту

вероятность назовем вероятностью продолжения по аналогии с теорией ветвящихся процессов [3].

Теорема 2. Пусть $A_i \in K_j$. Тогда при $t \rightarrow \infty$

$$Q_i(t) \sim \frac{c_i}{t^{(\frac{1}{2})^{q_j-1}}},$$

где $c_i > 0$ — некоторая константа.

Через $M_i^{>t}$ обозначим условное математическое ожидание числа вершин на ярусе t , помеченных нетерминалом A_i , в деревьях вывода, высота которых больше t .

Теорема 3. Пусть $A_i \in K_j$. Тогда при $t \rightarrow \infty$

$$M_i^{>t} \sim d_i \cdot t^{s_j + (\frac{1}{2})^{q_1-1} - 1},$$

где $d_i > 0$ — некоторая константа.

Из теоремы 3 следует, что общее число вершин в деревьях вывода высоты, большей t , определяют классы нетерминалов, для которых s_j имеет наибольшее значение, то есть классы, являющиеся последними в максимальных путях.

Работа выполнена при финансовой поддержке РФФИ (проект 07-01-00739-а).

Список литературы

1. Жильцова Л. П. Закономерности в деревьях вывода слов стохастического контекстно-свободного языка и нижняя оценка стоимости кодирования. Критический случай // Дискретный анализ и исследование операций. Серия 1. — 2003. — Т. 10, № 3. — С. 23–53.
2. Гантмахер Ф. Р. Теория матриц. — М.: Наука, 1966.
3. Севастьянов Б. А. Ветвящиеся процессы. — М.: Наука, 1971.

ПРЕОБРАЗОВАНИЯ БУЛЕВЫХ ФУНКЦИЙ, СОХРАНЯЮЩИЕ СЛОЖНОСТЬ ПОЛИНОМОВ

А. С. Казимиров (Иркутск)

Рассматриваемые операторные преобразования интересны, в первую очередь, в применении к задачам представления булевых функций минимальными полиномами и их обобщениями — операторными формами. Эти преобразования являются обобщением преобразований однотипности. Ранее уже предпринимались попытки

подобного обобщения [1]. Но отсутствие хорошей формальной записи таких преобразований затрудняло их исследование. Аффинные преобразования, которые также являются обобщением преобразований однотипности, не сохраняют сложность полинома по числу слагаемых.

Пусть \tilde{x} — сокращение для набора x_1, \dots, x_n . Будем рассматривать класс операторов на булевых функциях, которые удобно представить последовательностями $\mathbf{a}_1 \dots \mathbf{a}_n$, где $\mathbf{a}_i \in \{\mathbf{d}, \mathbf{e}, \mathbf{p}\}$. Действие оператора $\mathbf{a} = \mathbf{a}_1 \dots \mathbf{a}_n$ на функцию $f(\tilde{x})$ определяется по правилу: $\mathbf{a}(f(\tilde{x})) = f_n(\tilde{x})$, где $f_0(\tilde{x}) = f(\tilde{x})$ и

$$f_i(\tilde{x}) = \begin{cases} f_{i-1}(\tilde{x}), & \text{если } \mathbf{a}_i = \mathbf{e}; \\ f_{i-1}(x_1, \dots, x_{i-1}, \bar{x}_i, x_{i+1}, \dots, x_n), & \text{если } \mathbf{a}_i = \mathbf{p}; \\ (f_{i-1}(\tilde{x}))'_{x_i}, & \text{если } \mathbf{a}_i = \mathbf{d}. \end{cases}$$

Любую булеву функцию можно представить в виде суммы операторных образов от некоторой базисной функции — в виде операторной формы:

$$f(\tilde{x}) = \mathbf{a}_1(g(\tilde{x})) \oplus \dots \oplus \mathbf{a}_t(g(\tilde{x}))$$

Для операторных форм можно определить преобразования следующим образом. Пусть P — полная группа подстановок на множестве $\{\mathbf{d}, \mathbf{e}, \mathbf{p}\}$. Пусть φ — последовательность $\varphi_1 \dots \varphi_n$, где $\varphi_i \in P$. Тогда преобразование φ действует на оператор $\mathbf{a}_1 \dots \mathbf{a}_n$ следующим образом: $\varphi(\mathbf{a}_1 \dots \mathbf{a}_n) = \varphi_1(\mathbf{a}_1) \dots \varphi_n(\mathbf{a}_n)$. Такие преобразования будем называть S-преобразованиями. SP-преобразования получаются комбинацией S-преобразований и перестановок операторных символов [2]. Действие S- и SP-преобразований распространяется на множество функций.

Определение. Функции f и g называются SP(S)-эквивалентными, если существует SP(S)-преобразование φ , что $g = \varphi(f)$.

S- и SP-преобразования сохраняют сложность операторной формы, в частности — сложность полиномиального представления.

Теорема. Число S-классов $K_S(n)$ булевых функций n переменных выражается формулой:

$$K_S(n) = \frac{1}{6^n} \sum_{i=0}^n 2^i C_n^i \left((4^{n-i} - 1) 2^{\frac{2^{n-i}(2^i+2(-1)^i)}{6}} + 2^{\frac{2^{n-i}(2^i+2(-1)^i)}{3}} \right)$$

Для числа S-классов и числа SP-классов ($K_{SP}(n)$) n -местных булевых функций имеют место следующие асимптотические оценки:

$$K_S(n) \sim \frac{2^{2^n}}{6^n}, \quad K_{SP}(n) \sim \frac{2^{2^n}}{6^n \cdot n!}$$

Построение классификации булевых функций связано с нахождением как числа классов эквивалентности булевых функций, так и непосредственно представителей этих классов. Для S- и SP-преобразований важность нахождения представителей связана с их непосредственным использованием в алгоритмах минимизации.

Для построения классификаций обычно пользуются понятием инварианта группы преобразований.

Показано, что некоторые свойства специальной операторной формы являются инвариантами для группы SP-преобразований.

Для любого оператора размерности n существует представление в виде суммы 2^n операторов, отличающихся в каждой позиции от данного, называемой полным разложением оператора [3].

Определение. Форма, полученная полным разложением каждого оператора некоторой операторной формы булевой функции f с последующим удалением одинаковых слагаемых, называется *специальной операторной формой* (СОФ) функции f .

Количество слагаемых СОФ является инвариантом SP-преобразований и позволяет различить все классы при $n = 3$.

По СОФ можно построить таблицу размерами $3 \times n$ частот операторных символов — по каждой переменной подсчитывается количество появлений символов **d**, **e** или **p**. Таблица частот также является инвариантом и при $n = 4$ составляет полную систему инвариантов.

При $n = 5$ указанные инварианты не образуют полную систему. Однако для этого случая также найден полный инвариант. Аналогично таблице частот строится таблица размерами $3n \times 3n$, состоящая из $n \times n$ квадратов размерами 3×3 . Квадрат ij соответствует паре $x_i x_j$, столбцы и строки квадрата помечены символами **{d, e, p}**. Элемент квадрата, например с индексом **de**, равен количеству пар вхождений символов **d** и символов **e** в СОФ по переменным x_i и x_j , соответственно. Такая таблица также является инвариантом SP-преобразований, причем для $n = 5$ это полный инвариант.

Работа выполнена при финансовой поддержке РФФИ, проект 09-01-00476-а.

Список литературы

1. Koda N., Sasao T. An upper bound on the number of products in minimum ESOPs // Workshop in Application of the Reed-Muller Expansion Application in Circuit Design. Japan, 1995. — P. 94–101.

2. Казимиров А. С. Оценка числа классов LR-эквивалентности булевых функций // Вестник Бурятского университета: Математика и информатика. — Улан-Удэ: Бурятский государственный ун-т, 2005. — Серия 13. — Выпуск 2. — С. 17–22.

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

О ЧИСЛЕ СЛОВ ДЕЖАН НАД АЛФАВИТОМ ИЗ 5, 6 И 7 БУКВ

Р. М. Колпаков (Москва),
М. Раффино (Париж), М. Рао (Бордо)

Пусть $w = a_1 \cdots a_n$ — произвольное слово длины n над некоторым алфавитом Σ . Слово $a_i \cdots a_j$, где $1 \leq i \leq j \leq n$, называется *фактором* слова w . Положительное целое p называется *периодом* слова w , если $a_i = a_{i+p}$ для любого $i = 1, \dots, n - p$. Если p — минимальный период слова w , число n/p называется *порядком* слова w . Для любого конечного множества A через $|A|$ обозначается число элементов этого множества.

Множество слов W называется *факторным*, если для каждого слова из W все факторы этого слова также содержатся в W . Через $W(n)$ мы обозначаем подмножество множества W , состоящее из всех слов длины n . Если множество W является факторным, то, как несложно убедиться (см., например, [1, 3]), существует предел $\lim_{n \rightarrow \infty} \sqrt[n]{|W(n)|}$, который мы называем *предельной экспонентой роста* числа слов множества W .

В данной работе под периодичностью мы понимаем любое слово порядка, большего 1. Наиболее известным примером периодичностей является *квадрат*, т. е. слово вида ui , где u — произвольное непустое слово. Слово называется *бесквадратным*, если оно не содержит квадратов в качестве факторов. Аналогичным образом, *кубом* называется слово вида uui для произвольного непустого слова u . Слово называется *бескубным*, если оно не содержит кубов в качестве факторов. Нетрудно заметить, что не существует двухбуквенных бесквадратных слов длины, большей 3. С другой стороны, согласно классическим результатам Туэ [12, 13], существуют сколь угодно длинные трехбуквенные бесквадратные слова и сколь угодно длинные двухбуквенные бескубные слова. Результаты Туэ для

трехбуквенных слов усилила Дежан в [5]. Она установила существование сколь угодно длинных трехбуквенных слов, не содержащих в качестве факторов периодичностей порядка, большего, чем $7/4$. С другой стороны, было показано, что любое достаточно длинное трехбуквенное слово содержит в качестве фактора периодичность порядка, не меньшего, чем $7/4$. Таким образом, число $7/4$ является предельным минимальным порядком запретных факторов для трехбуквенных слов сколь угодно большой длины. Поэтому мы называем трехбуквенные слова, не содержащие в качестве факторов периодичностей порядка, большего, чем $7/4$, *предельно неповторными* трехбуквенными словами или трехбуквенными *словами Дежан*. Дежан также высказала гипотезу, что предельный минимальный порядок запретных факторов для k -буквенных слов сколь угодно большой длины равен $7/5$ при $k = 4$ и $k/(k - 1)$ при $k \geq 5$. Эта гипотеза была доказана для $k = 4$ в [10], для $5 \leq k \leq 11$ в [9] и для $12 \leq k \leq 14$ в [8]. Принципиальное продвижение в доказательстве гипотезы Дежан было сделано в работе Карпи [4], в которой данная гипотеза была доказана для $k \geq 38$. В этом году Рао завершил доказательство гипотезы, доказав ее для оставшихся случаев числа k . Таким образом, на основании доказанной гипотезы Дежан, мы можем определить предельно неповторные слова над алфавитом любой мощности. Отметим, что множество всех предельно неповторных слов над алфавитом любой мощности является, очевидно, факторным. Поэтому для любого $k > 1$ существует предельная экспонента $\gamma^{(k)}$ роста числа предельно неповторных k -буквенных слов.

Задача оценки числа неповторных слов различного вида активно исследовалась в научной литературе в течение последних десятилетий (обзоры результатов, полученных в этой области вплоть до 2008 г., можно найти в [2, 6]). В [7] нами был предложен принципиально новый универсальный подход для получения нижних оценок числа неповторных слов различного вида, основанный на мощностных соображениях. В частности, с помощью данного подхода в [7] были получены точные нижние оценки для экспонент роста числа двухбуквенных бескубных слов, трехбуквенных бесквадратных слов и трехбуквенных предельно неповторных слов. Естественным направлением для дальнейших исследований в данной области является применение данного подхода для оценки числа неповторных слов в "предельных" случаях, когда накладываемые на слова запретные ограничения являются максимально возможными для существования сколь угодно длинных слов, удовлетворяющих данным ограничениям. Такие случаи являются естественным образом наи-

более сложными для получения требуемых нижних оценок. Непосредственным примером таких ”предельных” случаев является случай предельно неповторных слов. При этом наибольший интерес представляет случай предельно неповторных k -буквенных слов при $k \geq 5$, поскольку случай предельно неповторных k -буквенных слов при $k = 3, 4$ является, как несложно заметить, исключительным, отличным от общего случая, когда предельный минимальный порядок запретных факторов для k -буквенных слов сколь угодно большой длины равен $k/(k - 1)$. Поэтому данные исследования посвящены получению нижних оценок для $\gamma^{(k)}$ при $k \geq 5$. Отметим, что предложенный в [7] метод оказывается неприменимым для решения поставленной задачи вследствие чрезмерно большого объема компьютерных вычислений. В данной работе предлагается нетривиальная модификация этого метода, позволяющая существенно сократить требуемый для его реализации объем компьютерных вычислений в случае оценки числа предельно неповторных слов. Используя предложенную модификацию, для случаев $k = 5, 6, 7$ мы получили оценки $\gamma^{(5)} \geq 1,154717$, $\gamma^{(6)} \geq 1,220299$, $\gamma^{(7)} \geq 1,235069$. Из сравнения полученных нижних оценок с полученными в [11] верхними оценками $\gamma^{(5)} \leq 1,158151$, $\gamma^{(6)} \leq 1,224837$, $\gamma^{(7)} \leq 1,236964$ вытекает, что нам удалось оценить $\gamma^{(5)}$, $\gamma^{(6)}$ и $\gamma^{(7)}$ с точностью до 0.01.

Работа первого автора выполнена при частичной финансовой поддержке РФФИ (проект 08-01-00863) и программы поддержки ведущих научных школ РФ (проект НШ-4470.2008.1).

Список литературы

1. Baake M., Elser V., Grimm U. The entropy of square-free words // Math. Comput. Modelling. — 1997. — V. 26. — P. 13–26.
2. Berstel J., Growth of repetition-free words — a review // Theoret. Comput. Science. — 2005. — V. 340. — P. 280–290.
3. Brinkhuis J. Nonrepetitive sequences on three symbols // Quart. Journal Math. Oxford. — 1983. — V. 34. — P. 145–149.
4. Carpi A. On the repetition threshold for large alphabets // Lecture Notes in Computer Science. — 2006. — V. 4162. — P. 226–237.
5. Dejean F. Sur un théorème de Thue // Journal Combin. Theory, Ser. A. — 1972. — V. 13. — P. 90–99.
6. Grimm U., Heuer M. On the entropy and letter frequencies of powerfree words // Entropy. — 2008. — V. 10. — P. 590–612.
7. Kolpakov R. Efficient lower bounds on the number of repetition-free words // Journal of Integer Sequences. — 2007. — V. 10. — Article 07.3.2.
8. Mohammad-Noori M., Currie J. Dejean’s conjecture and Sturmian

words // European Journal of Combinatorics. — 2007. — V. 28. — P. 876–890.

9. Moulin Ollagnier J. Proof of Dejean’s conjecture for alphabets with 5, 6, 7, 8, 9, 10 and 11 letters // Theoret. Comput. Science. — 1992. — V. 95. — P. 187–205.

10. Pansiot J.J. A propos d’une conjecture de F. Dejean sur les répétitions dans les mots // Discrete Appl. Math. — 1984. — V. 7. — P. 297–311.

11. Shur A., Gorbunova I. On the growth rates of complexity of threshold languages // 12th Mons Theoretical Computer Science Days. — Mons, Belgium, 2008.

12. Thue A., Über unendliche Zeichenreihen // Norske Vidensk. Selsk. Skrifter. I. Mat.-Nat. Kl. — Christiania, 1906. — V. 7. — P. 1–22.

13. Thue A., Über die gegenseitige Lage gleicher Teile gewisser Zeichenreihen. // Norske Vidensk. Selsk. Skrifter. I. Mat.-Nat. Kl. — Christiania, 1912. — V. 10. — P. 1–67.

О СЛОЖНОСТИ ВЕНТИЛЬНЫХ СХЕМ С КРАТНЫМ ЧИСЛОМ ПУТЕЙ

В. В. Кочергин (Москва)

Напомним классическое определение вентиляльной схемы [1].

Пусть $A = (a_{ij})$ — булева (двоичная) матрица размера $p \times q$. Ориентированный граф S без ориентированных циклов называется *вентиальной схемой, реализующей матрицу A* , если: 1) в S выделено p вершин — входных полюсов и q вершин — выходных полюсов; 2) в S нет ориентированных путей от одного входа к другому, от одного выхода к другому, от выхода к входу; 3) для любой пары (i, j) , $1 \leq i \leq p$, $1 \leq j \leq q$, ориентированный путь от i -го входа к j -му выходу существует тогда и только тогда, когда $a_{ij} = 1$.

Через $L_{BC}(S)$ обозначается *сложность вентиляльной схемы S* , т. е. число ребер (вентилей) схемы S . *Сложность $L_{BC}(A)$ реализации булевой матрицы A вентиальными схемами* определяется следующим образом: $L_{BC}(A) = \min L_{BC}(S)$, где минимум берется по всем вентиальным схемам, реализующим матрицу A .

В 1956 г. О. Б. Лупановым [1] предложен асимптотически наилучший метод построения вентиляльных схем глубины (максимальной длины пути от входа к выходу) 2, из которого, в частности, вытекает при условии $p + q \rightarrow \infty$ следующая асимптотическая оценка

сложности реализации вентиляльными схемами матрицы A размера $p \times q$:

$$L_{BC}(A) \leq \frac{pq}{\log_2 \max(p, q)} (1 + o(1)) + O(p + q).$$

Эта оценка при выполнении естественного условия $p + q = o\left(\frac{pq}{\log(p+q)}\right)$ и дополнительного условия $\frac{\log \min(p, q)}{\log \max(p, q)} \rightarrow 0$ дает для почти всех булевых матриц асимптотически наилучшую оценку сложности реализации вентиляльными схемами без ограничения на глубину. Однако при одновременном выполнении условий $\log p = O(\log q)$ и $\log q = O(\log p)$ эта верхняя оценка асимптотически не совпадает с «мощностной» нижней оценкой (при этом и превосходит ее асимптотически не более, чем в два раза).

Далее, в 1963 г. Э. И. Нечипорук [2] установил асимптотически неулучшаемую верхнюю оценку при некоторых соотношениях на размеры матрицы, в частности, для важного случая, когда выполняется условие $\frac{\log_2 p}{\log_2 q} \rightarrow 1$.

Окончательное асимптотически точное решение этой задачи при естественных ограничениях на соотношение числа полюсов и сложности было получено Н. Пиппенджером [3] в 1976 г. Более точно, для функции Шеннона $L_{BC}(p, q)$, численно равной максимуму по всем булевым матрицам размера $p \times q$ величин $L_{BC}(A)$, было установлено при $p + q \rightarrow \infty$ асимптотическое равенство

$$L_{BC}(p, q) = \frac{pq}{\log_2(pq)} \left(1 + O \left(\left(\frac{\log \log(pq)}{\log(pq)} \right)^{1/2} \right) \right) + O(p + q).$$

В дальнейшем этот результат был обобщен на естественным образом возникающую, например, в задаче о сложности вычисления систем мономов [4], следующую модификацию классических вентиляльных схем.

Пусть $A = (a_{ij})$ — целочисленная матрица размера $p \times q$ с неотрицательными элементами. Ориентированный граф S без ориентированных циклов будем называть *вентильной схемой с кратными путями* (или *вентильной схемой с предписанным числом путей*), реализующей матрицу A , если: в S выделено p вершин — входных полюсов и q вершин — выходных полюсов; в S нет ориентированных путей от одного входа к другому, от одного выхода к другому, от выхода к входу; для любой пары (i, j) , $1 \leq i \leq p$, $1 \leq j \leq q$, число ориентированных путей от i -го входа к j -му выходу равно в точности a_{ij} . Аналогично случаю классических вентиляльных схем,

через $L_{BC}^{\kappa p}(S)$ обозначим число ребер (вентилей) схемы S и положим $L_{BC}^{\kappa p}(A) = \min L_{BC}^{\kappa p}(S)$, где минимум берется по всем схемам, реализующим матрицу A .

Для функции Шеннона, определяемой равенством $L_{BC}^{\kappa p}(p, q, K) = L_{BC}^{\kappa p}(A)$, где максимум берется по всем матрицам размера $p \times q$ с неотрицательными целыми элементами, не превосходящими K , Н. Пиппенджером при слабых ограничениях установлена при $pq \log(K + 1) \rightarrow \infty$ асимптотика роста:

$$L_{BC}^{\kappa p}(p, q, K) = 3 \min(p, q) \log_3 K + \frac{pq \log_2(K + 1)}{\log_2(pq \log(K + 1))} (1 + o(1)) + O(\max(p, q)).$$

Этот результат сформулирован в [5], а его доказательство можно восстановить, объединив доказательства из [4] и [5].

Тем самым для обеих модификаций вентиляльных схем при слабых ограничениях на число полюсов (входов и выходов) установлена асимптотика роста функций Шеннона и предложен метод синтеза вентиляльных схем, дающий для почти всех матриц асимптотически минимальную верхнюю оценку. Однако при попытках получения асимптотически точных оценок сложности индивидуальных последовательностей матриц при реализации классическими схемами возникают стандартные трудности с доказательством нижних оценок [6, 7], в той или иной степени близких к «мощностной», которые удается так или иначе преодолеть лишь в некоторых случаях (см., например, [8, 9]). При реализации матриц вентиляльными схемами с кратным числом путей ситуация, вообще говоря, не такая — в наиболее естественном и интересном случае, когда размеры матриц ограничены (или очень слабо растут), слагаемое, получающееся из мощностных соображений, дает не основной по порядку вклад в рост функции Шеннона. Это дает надежду получать асимптотически точные нижние оценки для индивидуальных последовательностей (матриц). И в этом направлении получены значительные продвижения, переходя к которым далее под вентиляльными схемами условимся понимать вентиляльные схемы с кратным числом путей.

Лемма. Пусть k вершинам вентиляльной схемы S , приписаны наборы $(a_{11}, a_{12}, \dots, a_{1k})$, $(a_{21}, a_{22}, \dots, a_{2k})$, \dots , $(a_{k1}, a_{k2}, \dots, a_{kk})$, задаваемые матрицей $A = (a_{ij})$ размера $k \times k$. Тогда

$$3^{L_{BC}^{\kappa p}(S)} \geq |\det A|^3.$$

Доказательство будем вести индукцией по числу вершин схемы, в которые входит хотя бы один вентиль. Для схемы, не содержащей ни одного вентиля, утверждение леммы очевидно.

В схеме S среди k выбранных вершин обозначим через v_k ту, вершину, от которой к другим выделенным вершинам не ведут пути (хотя бы одна такая вершина всегда найдется в силу ацикличности вентильной схемы). Пусть в вершину v_k ведут r вентиляей. Вершины, из которых выходят эти вентиляи, обозначим соответственно через $v_k^{(1)}, v_k^{(2)}, \dots, v_k^{(r)}$. Пусть этим вершинам приписаны наборы $(a_{k1}^{(i)}, a_{k2}^{(i)}, \dots, a_{kk}^{(i)})$, $i = 1, 2, \dots, r$. Тогда набор $(a_{k1}, a_{k2}, \dots, a_{kk})$ есть покомпонентная сумма наборов $(a_{k1}^{(i)}, a_{k2}^{(i)}, \dots, a_{kk}^{(i)})$, $i = 1, 2, \dots, r$. Матрицу, получающуюся из матрицы A путем замены строки $(a_{k1}, a_{k2}, \dots, a_{kk})$ на строку $(a_{k1}^{(i)}, a_{k2}^{(i)}, \dots, a_{kk}^{(i)})$, обозначим через $A^{(i)}$. Схему, получающуюся из схемы S путем выбрасывания вершины v_k и всех вентиляей, входящих в v_k , обозначим через S' . Применяя предположение индукции, имеем:

$$\begin{aligned} |\det A| &= \left| \sum_{i=1}^r \det A^{(i)} \right| \leq \sum_{i=1}^r |\det A^{(i)}| \leq \\ &\leq r \left(3^{L_{BC}^{kp}(S')} \right)^{1/3} = r \left(3^{L_{BC}^{kp}(S)-r} \right)^{1/3} \leq \left(3^{L_{BC}^{kp}(S)} \frac{r^3}{3^r} \right)^{1/3} \leq \left(3^{L_{BC}^{kp}(S)} \right)^{1/3}. \end{aligned}$$

Лемма доказана.

Обозначим через $D(A)$ максимум абсолютных величин миноров матрицы A , где максимум берется по всем минорам.

Из доказанной леммы непосредственно выводится

Теорема 1. *Для любой ненулевой целочисленной матрицы A с неотрицательными элементами справедливо неравенство*

$$L_{BC}^{kp}(A) \geq 3 \log_3 D(A).$$

Оказывается, что нижняя оценка из теоремы 1 является хорошей базой для исследования асимптотического поведения сложности индивидуальных последовательностей матриц фиксированного размера, что подтверждает следующая

Теорема 2. *Для произвольного натурального t и произвольной последовательности матриц $\{A_n\}$ с неотрицательными элементами, каждая из которых имеет размер либо $2 \times q_n$, где $q_n \leq t$, либо $p_n \times 2$, где $p_n \leq t$, либо 3×3 , при условии $D(A_n) \rightarrow \infty$ выполняется соотношение*

$$L_{BC}^{kp}(A_n) \sim 3 \log_3 D(A_n).$$

Доказательство верхней оценки этой теоремы в идейном плане не сильно отличается от доказательства верхних оценок сложности вычисления систем одночленов [10–12] и технически достаточно тяжелое. Частичное разъяснение природы трудностей, возникающих при доказательстве верхней оценки теоремы 2 дает следующий факт. Казалось бы логично вытекающее из теоремы 2 предположение о том, что, возможно, при всех фиксированных значениях p и q для матриц размера $p \times q$ величина $L_{BC}^{kp}(A)$ асимптотически растет как $3 \log_3 D(A)$, оказывается неверным уже для квадратных матриц порядка 4.

Обозначим через $A(t, n)$ квадратную матрицу порядка $2t$, $t \geq 2$, определяемую таким образом. Первой строкой матрицы $A(t, n)$ является набор длины $2t$, первая половина разрядов которого равна n , а вторая половина — 0. Остальные $2t - 1$ строк матрицы $A(t, n)$ получаются из первой строки последовательным циклическим сдвигом на один разряд вправо.

Теорема 3. *При условии $t = o(\log n)$ справедливо асимптотическое равенство*

$$L_{BC}^{kp}(A(t, n)) \sim 6t \log_3 n.$$

Доказательство этой теоремы очень похоже на доказательство теоремы 1 из [13].

Следствием теоремы 3 является такое утверждение — при условии $t \leq \frac{\log n}{\log \log n}$ выполняется соотношение $L_{BC}^{kp} \sim \frac{6t}{t+1} \log_3 D(A(t, n))$. Таким образом, приведен пример последовательности матриц размера $2t \times 2t$, для которой устанавливаемую теоремой 1 нижнюю оценку можно усилить асимптотически в $2t/(t+1)$ раз.

Работа выполнена при финансовой поддержке РФФИ (проект 08-01-00863) и программы поддержки ведущих научных школ РФ (проект НШ-4470.2008.1).

Список литературы

1. Лупанов О. Б. О вентилях и контактно-вентильных схемах // Доклады АН СССР. — 1956. — Т. 111, № 6. — С. 1171–1174.
2. Нечипорук Э. И. О топологических принципах самокорректирования // Проблемы кибернетики, вып. 21. — М.: Наука, 1969. — С. 5–102.
3. Pippenger N. On evaluation of powers and related problems // Proc. 17th Ann. IEEE Symp. on Found. of Computer Sci. (Houston, TX, 25–27 Oct. 1976.) — P. 258–263.

4. Pippenger N. On evaluation of powers and monomials // SIAM J. Comput. — 1980. — V. 9, N 2. — P. 230–250.
5. Pippenger N. The minimum number of edges in graphs with prescribed paths // Math. Systems Theory. — 1979. — V. 12, № 4. — P. 325–346.
6. Лупанов О. Б. О методах получения оценок сложности и вычисления индивидуальных функций // Дискретный анализ. — Новосибирск, 1974. — Вып. 25. — С. 3–18.
7. Нигматуллин Р. Г. Нижние оценки сложности и сложность универсальных схем. — Казань: Изд-во Казанского университета, 1990.
8. Нечипорук Э. И. Об одной булевой матрице // Проблемы кибернетики, вып. 21. — М.: Наука, 1969. — С. 237–240.
9. Гринчук М. И. Осложности реализации циклических булевых матриц вентильными схемами // Известия ВУЗов. Математика. — 1988. — № 7. — 39–43.
10. Кочергин В. В. О сложности вычисления пары одночленов от двух переменных // Дискретная математика. — Т. 17, вып. 4. — 2005. — С. 116–142.
11. Кочергин В. В. О сложности вычисления систем одночленов от двух переменных // Труды VII Международной конференции „Дискретные модели в теории управляющих систем“ (Покровское, 4–6 марта 2006 г.). — М.: МАКС Пресс, 2006. — С. 185–190.
12. Кочергин В. В. О сложности вычисления системы из трех одночленов от трех переменных // Математические вопросы кибернетики, вып. 15. — М.: Физматлит, 2006. — С. 79–155.
13. Кочергин В. В. Об одном соотношении двух мер сложности вычисления систем одночленов // Вестник Московского университета. Сер. 1. Математика. Механика. — 2009, № 4. — С. 8–13.

О НАДСТРУКТУРЕ НЕКОТОРЫХ СЕМЕЙСТВ ЗАМКНУТЫХ КЛАССОВ МОНОТОННЫХ k -ЗНАЧНЫХ ФУНКЦИЙ

В. Б. Ларионов (Москва)

Обозначим множество $E_k = \{0, 1, \dots, k - 1\}$.

Определение 1. Функция $f(x_1, \dots, x_n)$ называется *функцией k -значной логики* ($k \geq 2$), если она определена на E_k^n и все ее значения принадлежат E_k .

Будем использовать следующие стандартные обозначения. Множество всех функций k -значной логики обозначим P_k . Для любого подмножества A из P_k через $[A]$ будем обозначать замыкание относительно операции суперпозиции (для функций далее везде будет идти речь именно об этом типе замыкания).

Пусть на E_k задано некоторое отношение частичного порядка r .

Определение 2. Функция $f(x_1, \dots, x_n)$ называется *монотонной относительно частичного порядка r* , если для любых двух наборов $\tilde{a}, \tilde{b} \in E_k^n$ таких, что $\tilde{a} \leq_r \tilde{b}$, выполнено $f(\tilde{a}) \leq_r f(\tilde{b})$. Множество всех функций из P_k , монотонных относительно r , называется *монотонным классом M_r* .

Для краткости мы будем задавать частичный порядок r частично упорядоченным множеством (ЧУМ) H из элементов E_k , а соответствующий монотонный класс обозначать M_H .

Определение 3. ЧУМ H будем называть *несвязным* множеством, если его диаграмма Хассе представляет собой несвязный граф G . Подмножества множества H , образующие компоненты связности графа G , назовем компонентами связности ЧУМ H .

Будем считать известным понятие сохранения функцией предиката и обозначать через A_r множество функций, сохраняющих предикат r .

Класс M_H является [3] замкнутым классом функций, сохраняющих предикат $R(x, y) = TRUE \iff x \leq_r y$. Везде далее, когда мы будем писать, что монотонный класс задается предикатом R , мы будем подразумевать именно описанный предикат $R(x, y)$.

Одним из семейств предполных классов в P_k при $k \geq 3$ является семейство \mathbf{M} — подмножество множества всех классов монотонных функций [4]. Известно [5], что монотонный класс является предполным (принадлежит множеству \mathbf{M}) тогда и только тогда, когда частичный порядок, сохраняемый им, обладает в точности одним минимальным и одним максимальным элементом.

Ранее автором изучался вопрос о строении надструктуры монотонных классов, не входящих в семейство \mathbf{M} [1, 2]. Было показано, что существуют монотонные классы с бесконечной надструктурой, минимальной логикой с подобным классом является P_4 .

В данной работе рассматривается надструктура монотонных классов, сохраняющих несвязное ЧУМ H . Далее будет показано, что вопрос о существовании бесконечной надструктуры у данных классов сводится к подобному вопросу для монотонных классов, сохраняющих компоненты связности H в соответствующих меньших логиках.

Также в данной работе указаны некоторые необходимые условия для того, чтобы над монотонным классом была бесконечная надструктура.

Пусть предикат $p \in [R]$, где R — предикат, задающий монотонный класс. Запишем p в виде формулы F . Заметим, что в формуле F можно вынести вперед все кванторы существования, не изменив предикат p . Везде далее мы будем считать, что предикат задается формулой именно такого вида.

В [1] показано, что для любого $p \in [R]$ можно выбрать такую формулу F с вынесенными вперед кванторами существования, что ей можно сопоставить ЧУМ L_F по следующему правилу: между множеством элементов L_F и множеством переменных F (учитываем и свободные и связанные) существует взаимно однозначное соответствие. Элемент, соответствующий переменной x будем обозначать v_x . В диаграмме Хассе ЧУМ L_F есть ребро (v_x, v_y) тогда и только тогда, когда в формуле F содержится запись $R(y, x)$. Везде далее будем задавать предикаты $p \in [R]$ именно такими формулами.

Определение 4. Предикат $p \in [R]$ назовем *несвязным*, если существует задающая его формула F указанного выше вида такая, что ЧУМ L_F несвязно. В противном случае предикат p называется *связным*.

Лемма 1. Пусть предикат $p \in [R]$. Соотношение $A_p = A_R$ выполнено тогда и только тогда, когда в ЧУМ L_p найдется пара сравнимых элементов, соответствующих свободным переменным предиката p .

Предположим, что на E_k задано отношение частичного порядка, описываемое ЧУМ H , являющимся несвязным множеством. Пусть H_1, \dots, H_h — все компоненты связности ЧУМ H , $|H_i| = l_i$. Предикат $R(x, y)$ задает монотонный класс M_H , как описано выше. Далее, если не оговаривается иное, будем полагать, что речь идет именно об указанном монотонном классе, сохраняющем несвязное ЧУМ.

Пусть $p \in [R]$ — связный предикат.

Лемма 2. Для любого набора $\tilde{a} \in E_k^n$ из $p(a_1, \dots, a_n) = TRUE$ следует, что существует номер $j \in \{1, \dots, h\}$, такой что для любого $i \in \{1, \dots, n\}$ справедливо $a_i \in H_j$.

Обозначим через $T(p)$ множество истинности предиката $p(x_1, \dots, x_n)$, то есть $T(p) = \{\tilde{a} \in E_k^n : p(\tilde{a}) = TRUE\}$.

Последняя лемма показывает, что множество истинности $T(p)$ связного предиката состоит из непересекающихся подмножеств T_1, \dots, T_h таких, что $T_i \subseteq H_i$. Используя этот факт, можно доказать следующее утверждение.

Лемма 3. Любому замкнутому классу $A \supseteq M_H$ в E_k можно однозначно поставить в соответствие некоторый набор замкнутых классов B_1, \dots, B_h из многозначных логик P_{l_1}, \dots, P_{l_h} , удовлетворяющий следующим условиям:

- 1) для всех $j \in \{1, \dots, h\}$ выполнено $B_j \supseteq M_{H_j}$ в P_{l_j} ;
- 2) если классам A_1, A_2 соответствуют наборы B_1, \dots, B_h и C_1, \dots, C_h , то из $A_1 \subseteq A_2$ следует, что для любого $i \in \{1, \dots, h\}$ верно $B_i \subseteq C_i$.

Отметим, что указанную лемму можно усилить. Если рассмотреть в качестве классов $A \supseteq M_H$ классы, для которых существует функция $f \notin A$ и для любого $B \supset A$ выполнено $f \in B$, то в последней лемме дополнительно будет выполнено следующее:

Если классам A_1, A_2 соответствуют наборы B_1, \dots, B_h и C_1, \dots, C_h , то

- 1) если $A_1 \neq A_2$, то найдется i такое, что $B_i \neq C_i$;
- 2) $A_1 \subseteq A_2$ тогда и только тогда, когда для любого $i \in \{1, \dots, h\}$ выполнено $B_i \subseteq C_i$.

Указанные классы A обладают рядом интересных свойств, однако объем статьи не позволяет их детально рассмотреть. Для нас здесь важно лишь то, что произвольный класс из P_k можно представить пересечением описанных классов.

Данная лемма позволяет свести задачу описания надструктуры монотонного класса M_H в P_k к задачам описания надструктуры монотонных классов M_{H_i} в P_{l_i} .

Основным результатом данной работы является следующий.

Теорема 1. Для того, чтобы монотонный класс M_H в P_k имел бесконечную надструктуру необходимо и достаточно, чтобы хотя бы один из классов M_{H_1}, \dots, M_{H_h} в соответственно P_{l_1}, \dots, P_{l_h} имел бесконечную надструктуру.

Рассмотрим теперь основные свойства надструктуры монотонного класса M_H .

Определение 5. Пусть H_1, \dots, H_h — некоторое разбиение множества E_k , $E_i \cap E_j = \emptyset$ при $i \neq j$. Классом U_{H_1, \dots, H_h} называется множество всех функций из P_k , сохраняющих указанное разбиение.

Определенные классы при нетривиальном разбиении множества E_k образуют одно из семейств предполных классов \mathbf{U} .

Из леммы 1 и 3 следует следующее утверждение.

Теорема 2. *Монотонный класс M_H из всех предполных классов содержится только в классе U_{H_1, \dots, H_h} .*

Рассмотрим теперь важный частный случай.

Теорема 3. *Если каждый из классов M_{H_i} является предполным в P_{I_i} (что эквивалентно наличию у каждого множества H_i единственного минимального и максимального элементов), то монотонный класс M_H является предполным в классе U_{H_1, \dots, H_h} .*

В заключение рассмотрим вопрос о необходимых условиях для бесконечной надструктуры. Достаточные для этого условия установлены в [1].

Рассмотрим произвольное ЧУМ H из элементов E_k (тут уже не обязательно несвязное) и монотонный класс M_H .

Теорема 4. *Если для произвольных элементов a, b, c, d из множества H таких, что $c \leq a$, $c \leq b$, $d \leq a$, $d \leq b$, существует элемент $e \in H$ такой, что $e \leq a$, $e \leq b$, $c \leq e$, $d \leq e$, то число замкнутых классов, содержащих M_H , конечно.*

Работа выполнена при поддержке РФФИ, грант 09-01-00701.

Список литературы

1. Ларионов В. Б. О положении некоторых классов монотонных k -значных функций в решетке замкнутых классов // Дискретная математика. — 2009. — Т. 21, вып. 5. — С. 111–116.

2. Ларионов В. Б. О монотонных замкнутых классах функций многозначной логики с бесконечной надструктурой // Материалы VII молодежной научной школы по дискретной математике и ее приложениям (18–23 мая 2009 г.). — М.: ИПМ им. М. В. Келдыша РАН, 2009. — С. 7–12.

3. Яблонский С. В., Гаврилов Г. П., Набебин А. А. Предполные классы в многозначных логиках. — М.: Издательский дом МЭИ, 1997.

4. Rosenberg I. La structure des fonctions de plusieurs variables sur un ensemble fini // Comptes Rendus, de l'Academ. — 1965. — V. 260. — 3817–3819.

5. Мартынюк В. В. Исследование некоторых классов функций в многозначных логиках // Проблемы кибернетики. Вып. 3. — 1960. — С. 49–61.

ПРИМЕНЕНИЕ ТЕОРЕМЫ О РАЗБИЕНИИ ГИПЕРГРАФА К ЗАДАЧЕ ОПТИМИЗАЦИИ РАСПИСАНИЯ

А. М. Магомедов (Махачкала)

Для одного частного случая рассмотрены условия жесткой оптимизации расписания с нефиксированными маршрутами и без отношения частичного предшествования.

Задача о жесткой оптимизации расписания. Пусть $L = \{1, \dots, l\}$ — множество преподавателей, m — директивный срок, $m = 0 \pmod{2}$, $N = \{1, \dots, n\}$ — множество учебных групп. Учебные нагрузки преподавателей представлены мультимножествами ω_i с элементами из множества N :

$$|\omega_i| \in \{2, m - 2, m\}, \quad \sum_{i=1}^l |\omega_i|_j = m \quad \forall j \in N;$$

здесь $|\omega_i|_j$ — количество вхождений элемента $j \in N$ в ω_i .

Расписанием будем называть $(l \times m)$ – матрицу M с элементами $M_{i,j} \in \{0, 1, \dots, n\}$, такую, что в каждой i -й строке ненулевые элементы образуют мультимножество ω_i , а ненулевые элементы каждого столбца — множество N .

Для исходных данных, описанных выше, расписание всегда существует. Спрашивается, можно ли с сохранением наборов в каждой строке и в каждом столбце (порядок расположения элементов можно изменить) привести расписание к виду, где в каждой строке ненулевые элементы расположены *непрерывно*, в подряд идущих ячейках?

Ассоциированная сеть. В следующей сети, *ассоциированной* с рассматриваемой задачей, источник и сток обозначены соответственно через S и T , пропускные способности приведены на схеме под соответствующими дугами, а нижние потоковые ограничения — над соответствующими дугами (S, x_j) и (x_j, y_i) ; $j \in N$, $i \in L$; для дуг (y_i, T) эти значения определяются в зависимости от равенства мощности $|\omega_i|$ мультимножества ω_i значению 2 (и в этом случае составляют 2 и 0 соответственно) или же — одному из значений: $m - 2$ и m (в этом случае как пропускные значения, так и нижние потоковые ограничения суть $m - 4$); обозначение $|\omega_i|_j$ на дуге (x_j, y_i) указывает, что количество кратных дуг вида (x_j, y_i) равно $|\omega_i|_j$ (все

остальные дуги — простые):

$$S \xrightarrow[m-4]{m-4} x_j \xrightarrow[0]{1} |\omega_i|_j \rightarrow y_i \xrightarrow[\frac{m-4}{m-4}, |\omega_i| \in \{m-2, m\}]{\frac{2}{0}, |\omega_i|=2} T$$

Условие разрешимости. Необходимым и достаточным условием разрешимости задачи о жесткой оптимизации расписания является существование в ассоциированной сети такого целочисленного потока f , что для каждой вершины v , $v \neq S$, $v \neq T$, соблюдается *условие четности*: $f(v) = 0 \pmod{2}$.

Доказательство необходимости несложно, однако вопрос проверки существования потока указанного вида представляет самостоятельный интерес и рассматривался в [1].

Достаточность вытекает из следующего утверждения для двудольной интерпретации $G = (X, Y, E)$ гиперграфа, где степень произвольной вершины множества Y равна 2 или $2r$ (другими словами, “ребрами” гиперграфа служат наборы мощности 2 или $2r$), а степень каждой вершины множества X равна $2r$ (т. е. для каждой вершины множества X сумма вхождений в “ребра” гиперграфа равна $2r$); через Y_r далее обозначено подмножество, образованное в множестве Y вершинами степени $2r$.

Утверждение. Гиперграф G допускает разбиение на r однородных реберно-непересекающихся подграфов $G_i = (V_i, E_i)$ степени 2, где $X \subseteq V_i$, $Y_r \subseteq V_i$.

Работа выполнена при финансовой поддержке гранта 09-01-96504-р_юг_а и гранта РФФИ 07-01-00143-а.

Список литературы

1. Магомедов А. М. // Тезисы докладов XV международной конференции “Проблемы теоретической кибернетики” (2–7 июня 2008 г.). — Казань: Отечество, 2008. — С. 77.

НЕПРЕРЫВНОЕ 3-ТЕСТИРОВАНИЕ

Т. А. Магомедов (Махачкала)

Пусть $L = \{1, \dots, l\}$ — «числовое» множество студентов, A — «буквенное» множество учебных дисциплин. Для каждого студента

$i \in L$ задано мультимножество ω_i из трех (необязательно различных) учебных дисциплин, по которым студент должен пройти тестирование. Тестирование студента по каждой учебной дисциплине занимает один день, запрещается одновременное тестирование: нескольких студентов по одной учебной дисциплине и/или одного студента по нескольким учебным дисциплинам. Задача заключается в составлении расписания длительностью в $m = 5$ дней, в котором для тестирования каждого студента выделены три последовательных дня. В сообщении найдены условия существования расписания и полиномиальный алгоритм его составления.

Введем обозначения: $\Omega = \{\omega_i; i \in L\}$, $|\omega_i|$ — мощность мультимножества ω_i , $|\omega_i| = 3 \quad \forall i \in L$; $|\omega_i|_a$ — количество вхождений буквы $a \in A$ в ω_i , $|\Omega|_{\omega_i}$ — количество вхождений мультимножества ω_i в семейство Ω ; $t(a) = \sum_{i \in L} |\omega_i|_a \leq m \quad \forall a \in A$.

Элементы матрицы M будем обозначать $M_{i,j}$; $M[i]$ — мультимножество, образованное буквами i -го столбца матрицы M . Матрица $l \times m$ с элементами из множества $0 \cup A$ называется *непрерывным расписанием* для Ω , если

- 1) количество строк матрицы, мультимножество букв в каждом из которых равно ω_i , составляет $|\Omega|_{\omega_i}$;
- 2) все элементы в $M[i]$ попарно различны;
- 3) все элементы строки, расположенные между двумя буквами, также являются буквами (*свойство непрерывности*).

Размещение элементов в i -й строке расписания M будем называть *нормальным*, если хотя бы один из двух элементов, $M_{i,1}$ или $M_{i,m}$, является буквой. Непрерывное расписание называется *нормальным*, если размещение в каждой его строке является нормальным.

Утверждение 1. *Если для мультимножества Ω непрерывное расписание существует, то существует и нормальное расписание.*

Специальной трансверсалью семейства Ω назовем трансверсаль (множество из l различных представителей, выбранных по одному из каждого $\omega_i \in \Omega$), которая включает все элементы $a \in A$, для которых $t(a) = 5$.

Утверждение 2. *Нормальное расписание для Ω существует тогда и только тогда, когда Ω обладает специальной трансверсалью.*

В транспортной сети N , изображенной ниже, $c(e)$ и $l(e)$ — соответственно пропускная способность и нижнее потоковое ограничение дуги e : значение потока $f(e)$ по дуге e удовлетворяет неравенству $l(e) \leq f(e) \leq c(e)$; узлы x_j ассоциированы с буквами $a_j \in A$,

узлы y_i соответствуют ω_i , S — «источник», T — «сток»; количество кратных дуг (x_j, y_i) равно $|\omega_i|_{a_j}$.

$$S \xrightarrow[\substack{c(e)=1 \\ l(e)=1 \text{ при } t(a_j)=5, l(e)=0 \text{ при } t(a_j)<5}]{1 \leq j \leq |A|} x_j \xrightarrow[\substack{c(e)=1 \\ l(e)=0}]{1 \leq i \leq l} y_i \xrightarrow[\substack{c(e)=1 \\ l(e)=1}]{T}$$

Следующее очевидное утверждение сводит проверку существования специальной трансверсали у семейства Ω к проверке существования *допустимого* потока [1] в транспортной сети.

Утверждение 3. Семейство Ω обладает специальной трансверсалью тогда и только тогда, когда в сети N существует допустимый поток.

Работа выполнена при финансовой поддержке гранта 09–01–96504–р_юг_а.

Список литературы

1. Форд Л. Р., Фалкерсон Д. Р. Потоки в сетях. — М.: Мир, 1966.

МОДЕЛИ МНОГОКОМПОНЕНТНЫХ СИСТЕМ НА ОСНОВЕ МАРКИРОВАННЫХ ГРАФОВ

П. П. Макарычев (Пенза)

Рассматривается организация моделирования многокомпонентных динамических систем с применением маркированных графов. Обсуждается процедура построения модели и результаты моделирования многокомпонентной динамической системы.

Организация компьютерного моделирования многокомпонентных систем предполагает формализованное описание взаимосвязей и процесса последовательных вычисления реакций отдельных компонент. Эта задача может быть решена с использованием различных графовых и сетевых представлений модели системы [1, 2]. В данной работе предлагается организация моделирования с применением маркированных графов.

Ориентированный маркированный граф может быть представлен тройкой $G = \langle V, W, M \rangle$, где $V = \{v_1, v_2, \dots, v_n\}$ — конечное множество вершин, $W = \{w_1, w_2, \dots, w_m\}$ — конечное множество дуг, M — функция маркировки $M : V \rightarrow N$ вершин или дуг $M : W \rightarrow N$

графа, отображающая множество вершин V или дуг W во множество неотрицательных целых чисел N . Множество дуг $W(v_i)$, инцидентных вершине v_i , разделяется на подмножество входящих в вершину $I(v_i)$ и подмножество выходящих из вершины $O(v_i)$ дуг. При графическом представлении маркированного орграфа вершины $V(v_i)$ изображаются в виде окружностей, функции $I(v_i)$, $O(v_i)$ — дугами, а маркировка M изображается с помощью фишек (маркеров), размещенных внутри окружности или на дугах графа.

Рассмотрим процедуру смены маркировки в ориентированном графе $G = \langle V, W, M \rangle$ с маркировкой в вершинах $M : V \rightarrow N$. Вершины v_i , $i = \overline{1, n}$, из которых дуги входят в вершину v_j , $j = \overline{1, n}$, считаются входными относительно v_j . Вершины v_i , в которые дуги входят из вершины v_j , считаются выходными относительно v_j . Комплект входных вершин для v_j обозначен как $E(v_j)$, а комплект выходных вершин — $T(v_j)$. Маркировка M_k определяет для каждой вершины v_i графа количество маркеров $m^k(v_i)$ на текущем шаге k , $k = 0, 1, 2, \dots$ смены маркировки. Логическое условие активизации вершины v_j в маркированном орграфе имеет вид:

$$m^k(v_i) \geq \#(v_i, E(v_j)), v_i \in E(v_j),$$

где $E(v_j)$ — комплект вершин v_i , входящих в вершину v_j , $\#(\cdot)$ — число вершин в комплекте.

При запуске разрешенной вершины v_j происходит смена текущей маркировки графа M_k на новую M_{k+1} :

$$m^{k+1}(v_i) = \begin{cases} m^k(v_i) - \#(v_i, E(v_j)), & \text{если } i \neq j; \\ m^k(v_i) + \sum_{i=1}^n \#(v_i, T(v_j)), & \text{если } i = j. \end{cases}$$

При матричном описании орграфа с маркированными вершинами задается матрицами смежности $S_1 = [s_{1ij}]$, $S_2 = [s_{2ij}]$ и вектором начальной маркировки $M_0 = (m_1^0, m_2^0, \dots, m_n^0)$ вершин графа. Текущая маркировка графа M_k определяется как вектор-строка $M_k = (m^k(v_1), m^k(v_2), \dots, m^k(v_n))$, где $n = |V|$ и каждое $m^k(v_i) \in N$.

Любая многокомпонентная динамическая система содержит совокупность взаимосвязанных компонентов. Каждый из компонентов характеризуется множеством входных и выходных сигналов, функцией, описывающей зависимость выходного сигнала от входных сигналов. В соответствии с таким представлением вычислительная модель, используемая при имитации, может быть определена как кортеж: $Mv = \langle \{x_j\}, \{f_i\}, \{c_l\} \rangle$, где $\{x_j\}$ — множество переменных;

$\{f_i\}$ — множество функциональных отношений; $\{c_i\}$ — множество элементов управляющей структуры.

Для каждого компонента системы можно задать класс сигналов X , содержащий два непересекающихся подкласса. Это подкласс входных сигналов X_1 и подкласс выходных сигналов X_2 , т. е. $X = X_1 \cup X_2$ и $X_1 \cap X_2 = \emptyset$. На классе сигналов X можно задать отношение следования: вычисления значений выходных сигналов в моменты времени $t_k = \Delta t \cdot k$, где $k = 0, 1, 2, \dots$, Δt — шаг дискретизации по времени. Таким образом, состояние динамического компонента в момент времени t_k можно определить наборами значений входных и выходных сигналов. Определим эти наборы в виде упорядоченных пар, введенных Куратовским: $\langle x, y \rangle = \{\{x\}, \{x, y\}\}$.

На основе упорядоченных пар можно определить упорядоченные тройки, четвертки и т. д.: $\langle x_1, \dots, x_n \rangle = \langle \langle x_1, \dots, x_{n-1} \rangle, x_n \rangle$.

В данном определении упорядоченная n -ка при $n > 0$ одновременно и упорядоченная пара. Для компонента с отношением R перед вычислением значения x_k^3 выходного сигнала в момент времени t_k наборы значений входных $\tilde{x}_1(k)$, $\tilde{x}_2(k)$ и выходного $\tilde{x}_3(k-1)$ сигналов определяются следующим образом:

$$\begin{cases} \tilde{x}_1(k) = \langle x_{k-\alpha}^1, x_{k-\alpha+1}^1, \dots, x_k^1 \rangle; \\ \tilde{x}_2(k) = \langle x_{k-\gamma}^2, x_{k-\gamma+1}^2, \dots, x_k^2 \rangle; \\ \tilde{x}_3(k-1) = \langle x_{k-\eta-1}^3, x_{k-\eta}^3, \dots, x_{k-1}^3 \rangle. \end{cases}$$

Зададим общее правило P вычисления выходного сигнала каждого компонента системы в виде:

$$P : A; A \Rightarrow B; U, \quad (1)$$

где A — условие активизации правила; B — заключение правила, « \Rightarrow » — знак логической секвенции; U — постусловие логического правила.

Условие A , характеризующее активизацию процесса вычисления значения выходного сигнала компонента, представим в виде логического выражения. Например, для компонента с двумя входами и одним выходом условие A имеет вид:

$$A = (x_1 = \tilde{x}_1(k)) \wedge (x_2 = \tilde{x}_2(k)) \wedge (x_3 = \tilde{x}_3(k-1)). \quad (2)$$

Заключение B , определяющее процедуру вычисления значения выходного сигнала в момент времени t_k , задается функциональным

отношением f_i , $i = \overline{1, n}$. Предположим, что для рассматриваемого компонента функциональное отношение f_i на наборах входных $\tilde{x}_1(k)$, $\tilde{x}_2(k)$ и выходного $\tilde{x}_3(k-1)$ сигналов имеет следующий вид:

$$f_i(\tilde{x}_1(k), \tilde{x}_2(k), \tilde{x}_3(k), x_3(k)). \quad (3)$$

С использованием постуловия U формируется новый набор значений выходного сигнала $x_3(k)$:

$$\langle x_{k-\eta}^3, \dots, x_k^3 \rangle = U(\langle x_{k-\eta-1}^3, x_{k-\eta}^3, \dots, x_{k-1}^3 \rangle, x_k^3). \quad (4)$$

Выражение (4) следует рассматривать как постуловие правила вычислений, которое выполняется в случае реализации вычисления выходного сигнала x_k^3 . С использованием (1–3) вычисления при компьютерном моделировании могут быть организованы с использованием систем продукционных правил, семантических сетей, Е-сетей, сетей Петри и маркированных графов.

Представление структуры моделируемой системы в виде маркированного орграфа позволяет упростить вычислительную модель, так как условие активизации вычисления выходного сигнала компонента (2) может быть заменено на условие поиска активной вершины маркированного орграфа. При этом смена текущей маркировки графа соответствует активизации логического правила (1).

Маркированный ориентированный мультиграф использован при организации компьютерного моделирования многокомпонентной динамической системы управления толщиной металлической полосы на выходе прокатного стана. Система содержит источник входного сигнала $R(s)$, ПИД-регулятор $C(s)$, объект управления $(G_1(s), G_2(s))$, возмущение $D_g(s)$, приложенное к входу объекта, и узел $G_f(s)$ упреждения возмущения. Исследование модели многокомпонентной системы выполнено в универсальном математическом пакете MathCad [3]. С использованием разработанной программы получены результаты моделирования системы при единичном ступенчатом входном воздействии и единичном ступенчатом возмущении. Результаты моделирования подтверждают высокую точность расчета переходных процессов в исследуемой системе при заданных параметрах компонентов. Используя настройку параметров компонентов модели, можно обеспечить заданное качество переходных процессов. Адекватность имитационной модели всей многокомпонентной системы подтверждена сравнением результатов численного моделирования с результатами аналитического решения для каждого компонента системы.

Список литературы

1. Бенькович Е. С., Колесов Ю. Б., Сениченков Ю. Б. Практическое моделирование динамических систем. — СПб.: БХВ-Петербург, 2002.
2. Емельянов С. В. Технология системного моделирования. — М.: Машиностроение, 1998.
3. Волгина М. А., Макарычев П. П. Моделирование сетей массового обслуживания на основе маркированных графов // Известия высших учебных заведений. Поволжский регион. Технические науки. — 2008. — № 3. — С. 33–39.

ОПРЕДЕЛЕНИЕ КОНЕЧНОСТИ МНОЖЕСТВА СОСТОЯНИЙ ФУНКЦИИ ЦЕПИ МАРКОВА

Р. Г. Мубаракзянов (Казань)

При исследовании свойств случайных последовательностей, реализуемых конечными вероятностными автоматами (КВА), представляет интерес проблема, имеет ли реализуемая последовательность конечное множество состояний [1]. В работах автора [2, 3] данная проблема была сведена к следующему вопросу.

Рассмотрим алфавит X , n -мерный стохастический вектор $\mu \in R_n$ и конечное множество стохастических $(n \times n)$ -матриц $\{A(x) | x \in X\}$. Максимальное подмножество неколлинеарных векторов в множестве $\{\mu A(v) | v \in X^*\}$, $\mu \in R_n$ назовем множеством, порожденным парой $(\mu, \{A(x) | x \in X\})$, где $A(x_1 x_2 \dots x_k) = A(x_1)A(x_2) \dots A(x_k)$. Существует ли конечный алгоритм, определяющий конечно ли порожденное множество? В результате исследования этого вопроса было доказано существование этого алгоритма, так как если порожденное множество конечно, то его мощность ограничена некоторой функцией, зависящей от n и $k = |X|$. Значение этой функции определяется довольно сложно и является в общем случае очень большим. В идеи доказательства существования такой функции лежит следующий факт. В случае конечности порожденного множества, вектор μ должен принадлежать так называемому допустимому множеству, количество возможных структур которого ограничено.

Известно [1, с. 213], что выходная последовательность автономного КВА является функцией конечной однородной цепи Маркова (ЦМ), то есть случайной последовательностью, получаемой следующим образом. Состояния ЦМ помечаются, то есть разбиваются на

блоки с уникальными пометками. При реализации ЦМ в качестве выхода определяется не состояние цепи, а его пометка. Таким образом, определение конечности множества состояний функции конечной однородной цепи Маркова разрешимо алгоритмом, время работы которого ограничено некоторым числом. Какова точная грань этого числа, определить непросто. Только в случае ряда ограниченный можно получить точную оценку.

Теорема 1. *Автономный КВА с 2-мя состояниями порождает случайную последовательность либо с бесконечным множеством состояний, либо с числом состояний, не большим $2(m+1)$, где m — число матриц, задающих автомат, соответствующих особенным операторам. Оценка теоремы достижима.*

Доказательство. Если число состояний случайной последовательности конечно, то допустимое множество либо пусто,

- а) либо состоит из двух одномерных пространств,
- б) либо совпадает с $\{R_2\}$.

В случае а) теорема доказана. Заметим, что выполнение а) возможно лишь, если существуют такое преобразование координат T , что для любого $x \in X$ матрица $A'(x) = T^{-1}A(x)T$ может иметь один из следующих видов:

$$\begin{pmatrix} \alpha(x) & 0 \\ 0 & \beta(x) \end{pmatrix}, \begin{pmatrix} 0 & \alpha(x) \\ \beta(x) & 0 \end{pmatrix}, \begin{pmatrix} \alpha(x) & 0 \\ 0 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 0 \\ 0 & \beta(x) \end{pmatrix}$$

В случае б) все неособенные операторы могут породить в R_2 из любого вектора $\mu_0 \in R_2^+$ лишь один неколлинеарный μ_0 вектор: μ_1 . Образующие неотрицательного ортанта R_2^+ отображаются этими операторами на себя. Таким образом, существуют числа α, β такие, что неособенный оператор $A(x), x \in X$ задается либо матрицей $\gamma(x)E_2$, либо $\gamma(x) \begin{pmatrix} 0 & \alpha \\ \beta & 0 \end{pmatrix}$ для некоторого числа $\gamma(x) \neq 0$.

Если для некоторых x_1, x_2 $\alpha(x_1)/\alpha(x_2) = \beta(x_1)/\beta(x_2)$, то для $A(x_1x_2)$ пространство R_2 не может быть допустимым множеством.

Любой особенный оператор $A(x)$ переводит любой вектор из R_2 в собственный вектор $A(x)$ ($\mu(x)$), либо в нулевой вектор. Все неособенные операторы могут породить из $\mu(x)$ не более еще одного нового вектора. Поэтому максимальное количество возможных неколлинеарных векторов в данном случае $2(m+1)$. Теорема доказана.

Хотя класс функций ЦМ совпадает с классом выходных последовательностей автономных КВА, но имеет свою специфику. Задание

функции ЦМ при помощи разбиения на блоки множества состояний ЦМ позволяет уменьшить возможности построения допустимого множества. В результате решение исследуемой задачи упрощается.

Матрицы автономного КВА, соответствующего функции ЦМ, имеют специальный вид. А именно, пусть функции ЦМ φ соответствует разбиение на блоки: $\{1, \dots, n_1\}$, $\{n_1 + 1, \dots, n_1 + n_2\}$, \dots , $\{\sum_{i=1}^{m-1} n_i + 1, \dots, \sum_{i=1}^m n_i = n\}$ — i -й блок соответствует i -му символу алфавита $X = \{1, \dots, m\}$ функции ЦМ, $i = \overline{1, m}$. Тогда матрица ЦМ имеет следующий блочный вид:

$$P = \begin{pmatrix} P_{11} & P_{12} & \dots & P_{1m} \\ P_{21} & P_{22} & \dots & P_{2m} \\ \dots & \dots & \dots & \dots \\ P_{m1} & P_{m2} & \dots & P_{mm} \end{pmatrix},$$

$$A(i) = \begin{pmatrix} 0 & & \\ P_{i1} & \dots & P_{im} \\ 0 & & \end{pmatrix}, i = \overline{1, m},$$

где P_{ij} — $(n_i \times n_j)$ -матрица.

Пусть η_i — вектор-столбец, состоящий из n_i единиц, а μ_i — вектор-строка распределения начальных состояний длины n_i , соответствующий i -му блоку разбиения. Определим пространства:

$$L_i = Lin\{\eta_i, P_{i i_1} \dots P_{i_{l-1} i_l} \eta_i | i_1 i_2 i_3 \dots i_l \in X^*\},$$

$$M_i(p) = Lin\{\mu_{i_1} P_{i_1 i_2} P_{i_2 i_3} \dots P_{i_l i} |$$

для слов $i_1 i_2 i_3 \dots i_l \in X^*$ таких, что $\varphi_{i_1 i_2 i_3 \dots i_l} = \varphi_p\}$.

Для слов $p_1 = i_1 i_2 \dots i_k$ и $p_2 = j_1 j_2 \dots j_t$ верно, что $\varphi_{p_1} = \varphi_{p_2}$ тогда и только тогда, когда для любого $i = \overline{1, m}$ и любого слова $m_1 m_2 \dots m_l \in X^*$

$$\left(\frac{\mu_0 A(p_1) \eta}{\mu_0 A(p_2) \eta} \mu_{i_1} P_{i_1 i_2} \dots P_{i_k i} - \mu_{j_1} P_{j_1 j_2} \dots P_{j_t i} \right) P_{i m_1} \dots P_{m_{l-1} m_l} \eta_{m_l} = 0.$$

Следовательно, для размерностей пространств верно

$$\dim M_i(p) + \dim L_i \leq n_i + 1, i = \overline{1, m}, p \in X^*. \quad (1)$$

Лемма 1. Пусть выполняется $\dim L_i = n_i$. Тогда состояния функции ЦМ, соответствующие словам $i_1 u_i$ и $j_1 v_i$, совпадают тогда и только тогда, когда вектора $\mu_{i_1} P_{i_1 u_i}$ и $\mu_{j_1} P_{j_1 v_i}$ коллинеарны.

Следующий оргграф назовем графом функции ЦМ. Корневая вершина, не имеющая входящих дуг, помечена R_n . Остальные вершины помечены Q_1, Q_2, \dots, Q_m : Q_i — n_i -мерное подпространство R_n соответствует i -му блоку разбиения состояний ЦМ. Дуги, ведущие из корневой вершины графа в Q_i , соответствуют проекциям R_n в Q_i , $1 \leq i \leq m$. Для любых i, j ($1 \leq i \leq m, 1 \leq j \leq m$) дуга между вершинами Q_i и Q_j помечена P_{ij} .

Итак, $Q_i P_{ij} \subseteq Q_j$, но может быть $Q_i P_{ij} \neq Q_j$. Для функции ЦМ построение структуры допустимого множества можно вести, исходя из структуры графа функции ЦМ. При построении возможных структур конкретный вид операторов не учитывается. Поскольку $n_i < n, i = \overline{1, m}$, то оценки мощности порожденного множества существенно уменьшаются. В частности, при $\dim L_i = 1$ (например, $n_i = 1$) вершина Q_i будет соответствовать одному состоянию случайной последовательности. Легко получается оценка и при $\dim L_i = 2$. В этом случае, минимизируя на таких состояниях автомат как линейный, можно перейти к $n_i = 2$ и воспользоваться теоремой 1.

Теорема 2. Пусть при разбиении состояний ЦМ на блоки функции ЦМ соответствуют матрицы $\{P_{ij} \mid i = \overline{1, m}, j = \overline{1, m}\}$. Тогда функция ЦМ снова является однородной цепью Маркова при любом начальном распределении исходной цепи в том и только в том случае, когда для любого $k = \overline{1, m}$: либо 1) $P_{kl} \eta_l = c_{kl} \eta_k$, $l = \overline{1, m}$; либо 2) $P_{jk} = 0$ для любого $j \neq k$; и найдется c_k : $P_{kk}(P_{kl} \eta_l) = c_k(P_{kl} \eta_l)$, $l = \overline{1, m}$, $P_{kk} \eta_k = c_k \eta_k$.

Доказательство. Требование теоремы для ЦМ выполнится тогда и только тогда, когда:

- 1) R_n является допустимым множеством.
- 2) Каждое пространство Q_i графа функции ЦМ соответствует одному состоянию функции ЦМ. Тогда возможно, что выполняется равенство $\dim L_i = 1$, т. е.

$$P_{i i_1} P_{i_1 i_2} \dots P_{i_{k-1} i_k} \eta_{i_k} = c(i_1, \dots, i_k) \eta_i, i_1 \dots i_k \in X^*, \quad (2)$$

где $c(i_1, \dots, i_k)$ — константа для фиксированных i_1, \dots, i_k .

Пусть $\dim L_i > 1$. Тогда при минимизации автомата как линейного новое пространство Q'_i , получаемое на месте Q_i , будет иметь

размерность, больше чем 1. Следовательно, если в Q'_i при фиксированном μ_0 могут получиться неколлинеарные векторы, то условие 2 не будет выполнено. Этого не произойдет, если для этого i :

2.1. Не существует $j \neq i$ такого, что $P_{ji} \neq 0$. В этом случае условие (2) выполняется. Если для некоторого $i = \overline{1, m}$ существует $j \neq i$ такое, что $P_{ji} \neq 0$, тогда существуют числа $\{c_{ik}\}$, для которых выполняется

$$P_{ik}\eta_k = c_{ik}\eta_k, k = \overline{1, m}. \quad (3)$$

Это условие необходимо и достаточно для выполнения (2).

2.2. Из 2.1 и (3) базис в пространстве L_i можно выбрать в множестве $\{\eta_j^{(i)}\} = \{\eta_i; P_{ij}\eta_j, j = \overline{1, m}\}$. После минимизации автомата как линейного перейдем к пространству L'_i векторов, для которых можно применять соотношение (1) или лемму 1. Тогда для произвольного $\mu \in Q'_i$ $\mu P'_{ii} = c_i\mu$, т. е. $P'_{ii} = c_i E_i$, где E_i — единичная матрица. Это условие выполняется в том и только в том случае, когда для любого вектора $\eta \in L'_i$ $P'_{ii}\eta = c_i\eta$. Так как базис $L_i: \{\eta_j^{(i)}\}$, то предыдущее равенство эквивалентно условиям

$$2.2.1. P_{ii}(P_{ik}\eta_k) = c_i P_{ik}\eta_k, k = \overline{1, m}.$$

$$2.2.2. P_{ii}\eta_i = c_i\eta_i.$$

Эти условия вместе с условием 2.1 являются необходимыми и достаточными для того, чтобы Q_i соответствовало одному состоянию функции ЦМ, если $\dim L_i > 2$. Теорема доказана.

Заметим, что эта теорема почти дословно совпадает с теоремой Боша [4, теорема 4].

Список литературы

1. Бухараев Р. Г. Основы теории вероятностных автоматов. — М.: Наука, 1985.
2. Мубаракзянов Р. Г. Конечность множества неколлинеарных векторов, порождаемого семейством линейных операторов // Известия вузов. Математика. — 1987. — № 4. — С. 82–84.
3. Mubarakzjanov R. Finiteness of a set of non-collinear vectors generated by a family of linear operators // Linear algebra and its application. — 1999. — 294. — P. 9–33.
4. Bosch K. Funktionen homogener Markoffscher Ketten als homogene bzw. inhomogene Markoffsche Ketten // Metrika. — 1979. — V. 26. — № 2. — P. 71–85.

О НЕКОТОРЫХ МАКСИМАЛЬНЫХ ЧАСТИЧНЫХ ГИПЕР- И УЛЬТРАКЛОНАХ

В. И. Пантелеев (Иркутск)

Пусть A — конечное множество. n -местной мультифункцией на множестве A называется отображение $f : A^n \rightarrow 2^A$, а n -местной мультипроекцией — отображение $e_n^i : (x_1, \dots, x_n) \rightarrow \{x_i\}$, $1 \leq i \leq n$.

На множестве мультифункций определим суперпозицию-1 и суперпозицию-2.

Суперпозиция-1 $f(f_1, \dots, f_m)$ с внешней мультифункцией f и внутренними мультифункциями $f_1(x_1, \dots, x_n), \dots, f_m(x_1, \dots, x_n)$ определяет мультифункцию $h_1(x_1, \dots, x_n)$ следующим образом:

$$h_1(a_1, \dots, a_n) = \begin{cases} \emptyset, & \text{если существует } i \in \{1, \dots, m\} \text{ такое, что} \\ & f_i(a_1, \dots, a_n) = \emptyset; \\ \bigcup_{b_i \in f_i(a_1, \dots, a_n)} f(b_1, \dots, b_m), & \text{иначе.} \end{cases}$$

А суперпозиция-2 определяет мультифункцию $h_2(x_1, \dots, x_n)$ следующим образом:

$$h_2(a_1, \dots, a_n) = \begin{cases} \emptyset, & \text{если существует } i \in \{1, \dots, m\} \text{ такое, что} \\ & f_i(a_1, \dots, a_n) = \emptyset; \\ \bigcap_{b_i \in f_i(a_1, \dots, a_n)} f(b_1, \dots, b_m), & \text{если } \bigcap f(b_1, \dots, b_m) \neq \emptyset; \\ \bigcup_{b_i \in f_i(a_1, \dots, a_n)} f(b_1, \dots, b_m), & \text{иначе.} \end{cases}$$

Частичным гипер(ультра)клоном называется множество мультифункций, содержащее все мультипроекции и замкнутое относительно суперпозиции-1 (суперпозиции-2). Максимальным называется собственный частичный гиперклон (ультраклон) такой, что единственным, содержащим его собственным частичным гиперклоном (ультраклоном), является он сам. Рангом частичного гипер(ультра)клона называется мощность множества A . Близкие определения частичного клона, гиперклона можно посмотреть, например, в [1].

Среди частичных гиперклонов ранга 2 максимальными будут следующие [2]:

$$\begin{aligned} K_1 &= \{f(x_1, \dots, x_n) \mid f \equiv \emptyset \text{ или } f(0, \dots, 0) \in \{\{0\}, A\}\}, \\ K_2 &= \{f(x_1, \dots, x_n) \mid f \equiv \emptyset \text{ или } f(1, \dots, 1) \in \{\{1\}, A\}\}, \\ K_3 &= \{f(x_1, \dots, x_n) \mid f(0, \dots, 0) \in \{\{0\}, \emptyset\}\}, \\ K_4 &= \{f(x_1, \dots, x_n) \mid f(1, \dots, 1) \in \{\{1\}, \emptyset\}\}. \end{aligned}$$

Заметим, что множества K_1 и K_2 не являются частичными ультраклонами. Эти множества не замкнуты относительно суперпозиции-2. В качестве примера можно привести суперпозицию-2 $f(f(x))$,

где $f(x) = (\{0, 1\}, \{1\})$ принадлежит множеству K_1 . Но $f(f(x)) = (\{1\}\{1\})$ уже не принадлежит множеству K_1 .

Несложно показать, что множества K_3 и K_4 являются максимальными частичными ультраклонами.

Пусть E — непустое подмножество множества A . Определим множество мультифункций T_E следующим образом:

$$T_E = \{f \mid f(a_1, \dots, a_n) = B, a_i \in E, B \subseteq E\}.$$

Теорема. *Множество T_E является максимальным частичным гипер(ультра)клоном.*

Доказательство. Покажем, что множество T_E является максимальным частичным ультраклоном. Это множество замкнуто относительно суперпозиции-2. Действительно, если

$$h(x_1, \dots, x_n) = f(f_1(x_1, \dots, x_n), \dots, f_m(x_1, \dots, x_n)),$$

то

$$h(a_1, \dots, a_n) = f(E_1, \dots, E_m), E_i \subseteq E.$$

Если одно из E_i есть \emptyset , то по определению $h(a_1, \dots, a_n) = \emptyset$, иначе мы рассматриваем пересечение (если оно не пусто) или объединение некоторых подмножеств из E . В любом случае получаем подмножество из E .

Пусть теперь $f \notin T_E$. Это означает, что для некоторых элементов a_1, \dots, a_n из E выполняется $f(a_1, \dots, a_n) = B$ и множество B не является подмножеством E . a_i , рассматриваемые как мультифункции-константы, принадлежат T_E . Поэтому мультифункция-константа B может быть получена из мультифункций множества T_E и f .

Пусть теперь $g(x_1, \dots, x_n)$ — произвольная мультифункция. Рассмотрим

$$h(x_1, \dots, x_n, x_{n+1}) = \begin{cases} \emptyset, & \text{если } x_{n+1} \in E; \\ g(x_1, \dots, x_n), & \text{иначе.} \end{cases}$$

Мультифункция h принадлежит T_E , так как на наборах из E она принимает значение равное \emptyset . И теперь суперпозиция $h(x_1, \dots, x_n, B)$ определяет мультифункцию g . Доказательство того, что T_E является максимальным частичным гиперклоном является аналогичным.

Работа выполнена при финансовой поддержке РФФИ, проект 07-01-00240.

Список литературы

1. Doroslovački R., Pantović J., Vojvodić G. One interval in the lattice of partial hyperclones // *Czechoslovak Mathematical Journal*. — 2005. — № 55 (130). — P. 719–724.
2. Пантелеев В. И. Критерий полноты для недоопределенных частичных булевых функций // *Вестник НГУ. Серия: Математика, механика, информатика*. — 2009. — Т. 9, вып 3. — С. 95–114.

О РЕАЛИЗАЦИИ НЕКОТОРЫХ ФУНКЦИЙ СХЕМАМИ С ПОДВЕДЕНИЕМ ПЕРЕМЕННЫХ, ВЛОЖЕННЫМИ В ЕДИНИЧНЫЙ КУБ

О. А. Садовников (Москва)

В теории синтеза управляющих систем рассматривается ряд моделей схем, в которых функционирование каждого элемента определяется значением одной из входных переменных схемы — так называемые, проводящие схемы. Самыми известными примерами таких моделей являются контактные схемы и двоичные решающие диаграммы (BDD). Как правило, такие схемы удобно представлять в виде графа, в котором вершины или рёбра (в зависимости от модели) помечены соответствующими символами из множества входных переменных схемы. Обычно при геометрической реализации сложность схемы учитывает число управляющих элементов и число элементов, осуществляющих коммутацию между ними, но не учитывает необходимость передачи значений входных переменных к соответствующим управляющим элементам.

В данной статье будет предложена конструкция, которая позволяет учитывать все вышеперечисленные факторы равноправно — так называемые схемы с подведением переменных. Основные определения будут сформулированы в общем виде, без привязки к какому-либо конкретному классу схем. Вместе с тем, уже упомянутые классы BDD и контактных схем мы будем рассматривать в качестве примеров подходящих моделей. Будет определён функционал сложности систем функций, связанный с их геометрической реализацией в единичном кубе, и для сложности некоторых систем функций будут приведены близкие верхние и нижние оценки.

Договоримся обозначать через $P_2(n)$ множество всех булевых функций от n переменных x_1, \dots, x_n , а через $P_2^m(n)$ — множество всех систем из m булевых функций от n переменных.

Мы будем рассматривать обобщение класса BDD — BDD, реализующие ортогональные системы функций. Напомним, что система функций $\vec{F} = (f_1, \dots, f_m) \in P_2^m(n)$, $m \geq 2$ называется *ортогональной*, если для любого двоичного набора $\tilde{\alpha} = (\alpha_1, \dots, \alpha_n)$ ровно одна функция из \vec{F} равна 1 на наборе $\tilde{\alpha}$.

Указанная BDD, реализующая ортогональную систему функций $\vec{F} = (f_1, \dots, f_m) \in P_2^m(n)$, $m \geq 2$, представляет собой помеченный ориентированный граф $\Sigma = \Sigma(x_1, \dots, x_n; 1, \dots, m)$ без ориентированных циклов с единственным истоком и m стоками (в отличие от классических BDD, где по определению $m = 2$). При этом стоки графа Σ считаются выходами схемы и пронумерованы числами $1, \dots, m$, а все остальные вершины помечены символами из множества $X = \{x_1, \dots, x_n\}$. Как и в классической модели BDD, из каждой вершины с пометкой x_i выходит ровно две дуги — одна с пометкой «0» и одна с пометкой «1». Множество X называется множеством входных (управляющих) переменных в Σ . По определению, $f_j(\alpha_1, \dots, \alpha_n) = 1$ тогда и только тогда, когда в $\Sigma(x_1, \dots, x_n; 1, \dots, m)$ существует цепь, которая начинается в истоке, заканчивается в выходе с номером j и из любой вершины с пометкой x_i выходит по ребру с пометкой α_i .

Описание классической модели BDD, как и описание класса контактных схем, можно найти, например, в [1].

Рассмотрим некоторую произвольную модель, в которой схемы представляются в виде графа и элементам соответствуют вершины графа (как в случае с BDD). Рассмотрим, не вдаваясь в подробности ее функционирования, некоторую схему $\Sigma = \Sigma(x_1, \dots, x_n)$ из этой модели, где $X = \{x_1, \dots, x_n\}$ — множество входных переменных схемы Σ . Как уже было сказано выше, схема $\Sigma = \Sigma(x_1, \dots, x_n)$ представляет собой граф с пометками из множества $X = \{x_1, \dots, x_n\}$ на некоторых (а возможно, что и на всех) вершинах.

Графом подводки для схемы $\Sigma = \Sigma(x_1, \dots, x_n)$ будем называть граф $T = \bigcup_{i=1}^n T_i$, где T_i , ($i = \overline{1, n}$) — дерево, связывающее все вершины Σ с пометкой x_i , такое, что:

- 1) множество вершин T_i включает в себя все вершины Σ , имеющие пометку x_i ;
- 2) T_i не имеет общих с Σ рёбер, а также общих с Σ вершин, не обладающих пометкой x_i ;

3) Для любого $j \neq i$ $T_i \cap T_j = \emptyset$.

Заметим, что для одной схемы графов подводки может быть несколько. Обозначим через $T(\Sigma)$ множество всех графов подводки для Σ .

Рассмотрим произвольную схему $\Sigma(X)$ исследуемого типа с пометками из множества X на вершинах. Схемой с подведением переменных $\hat{\Sigma}(X)$ для схемы $\Sigma(X)$ будем называть граф вида $\Sigma(X) \cup T$, где $T \in T(\Sigma)$. Следует отметить, что граф подводки учитывается только при геометрической реализации схемы. Функционирование схемы $\hat{\Sigma}(X)$ полностью определяет функционирование соответствующей схемы с подведением переменных $\hat{\Sigma}$.

Схема с подведением переменных $\Sigma(\hat{X}) = \Sigma(X) \cup T$ реализует систему функций \vec{F} , если схема $\Sigma(X)$ реализует эту систему функций. Например, если $\Sigma = \Sigma(x_1, \dots, x_n)$ — некоторая BDD с входными переменными $\{x_1, \dots, x_n\}$, $T \in T(\Sigma)$, а $\vec{F}(x_1, \dots, x_n)$ — система функций, реализуемая Σ , то граф $\hat{\Sigma}(x_1, \dots, x_n) = \Sigma(x_1, \dots, x_n) \cup T$ называется *BDD с подведением переменных*, построенной по BDD Σ , причём $\hat{\Sigma}(x_1, \dots, x_n)$ также реализует $\vec{F}(x_1, \dots, x_n)$.

Пусть теперь Σ — произвольная схема из такой модели, в которой каждому управляющему элементу сопоставляется ребро графа с пометкой из множества $X = \{x_1, \dots, x_n\}$ входных переменных Σ . *Графом подразделения* схемы Σ будем называть граф $G(\Sigma)$, который получается из Σ посредством подразделения каждого ребра (a, b) на цепь (a, c, b) длины 2 и переноса пометки с ребра (a, b) на новую вершину c .

Заметим, что в результате последовательного применения такой операции ко всем рёбрам Σ в полученном графе $\Sigma' = G(\Sigma)$ не останется ни одного помеченного ребра, а каждая помеченная вершина будет находиться в середине некоторой цепи длины 2. Таким образом, каждому управляющему элементу исходной схемы в графе $G(\Sigma)$ сопоставляется уже не ребро, а вершина, и, следовательно, введённое выше определение графа подводки для $G(\Sigma)$ применимо и в этой модели.

Итак, пусть $\Sigma(X)$ — схема с пометками из множества X на рёбрах. Тогда схемой с подведением переменных для $\Sigma(X)$ будем называть граф $\hat{\Sigma}(X) = G(\Sigma(X)) \cup T$, где $T \in T(G(\Sigma(X)))$.

Будем рассматривать геометрическую реализацию схем с подведением переменных, связанную с их гомеоморфным вложением в

единичный n -мерный куб (см, например, [2, 3]). Критерием сложности реализации схемы с подведением переменных $\hat{\Sigma}$ будет служить минимальная размерность $D(\hat{\Sigma})$ единичного куба, допускающего указанное вложение.

Под сложностью системы функций \vec{F} будем понимать минимальную сложность схемы с подведением переменных, реализующей \vec{F} . Введём функционалы $D^{BDD}(\vec{F})$ и $D^{KC}(\vec{F})$ для сложности реализации системы функций \vec{F} в классе BDD и контактных схем с подведением переменных соответственно.

Заметим, что указанная модель является модификацией из работ [2, 3], где исследовалось, в частности, поведение функции Шеннона для сложности BDD — $R^{BDD}(n)$, равной минимальной размерности единичного куба, допускающего для любой булевой функции $f(x_1, \dots, x_n)$ от n переменных вложение реализующей её BDD.

Напомним, что через \vec{Q}_n обозначается система всех элементарных конъюнкций ранга n от переменных x_1, \dots, x_n , а через \vec{L}_n — система из двух различных линейных функций порядка n , существенно зависящих от всех переменных x_1, \dots, x_n . Для этих систем функций были получены следующие оценки сложности их реализации в классах BDD и контактных схем с подведением переменных:

Теорема 1. $n + 1 \leq D^{BDD}(\vec{Q}_n) \leq n + 2$

Теорема 2. $\lceil \log n \rceil + 1 \leq D^{BDD}(\vec{L}_n) \leq \lceil \log n \rceil + 3$

Теорема 3. $n + 2 \leq D^{KC}(\vec{Q}_n) \leq n + 3$

Теорема 4. $\lceil \log(n - 1) \rceil + \lceil \log 6 \rceil \leq D^{KC}(\vec{L}_n) \leq \lceil \log n \rceil + 4$

Отметим, что верхние оценки получены конструктивно — для каждой системы функций \vec{L}_n и \vec{Q}_n построена соответствующая схема с подведением переменных. Нижние оценки были получены исходя из нижних оценок числа вершин в минимальных схемах, реализующих эти системы функций.

Работа выполнена при финансовой поддержке РФФИ (проект 09-01-00817).

Список литературы

1. Ложкин С. А. Лекции по основам кибернетики. — М.: Издательский отдел ф-та ВМиК МГУ, 2004.
2. Ложкин С. А., Седелев О. Б. О реализации функций алгебры логики BDD, вложенными в единичный куб // Вестник Московского ун-та. Серия 15.
3. Седелев О. Б. О реализации функций алгебры логики схема-

ми из некоторых классов, вложенными в гиперкубы. — Диссертация на соискание ученой степени кандидата физико-математических наук. — М., 2008.

О СЛОЖНОСТИ РЕАЛИЗАЦИИ ФУНКЦИЙ АЛГЕБРЫ ЛОГИКИ В ОДНОЙ МОДЕЛИ КЛЕТОЧНЫХ СХЕМ

А. Ю. Улесова (Москва)

Схема из клеточных элементов [1] представляет собой плоскую прямоугольную решетку, в каждой клетке которой расположен один из элементов базиса. Размеры всех элементов одинаковы и принимаются за единицу. Элементы могут быть как функциональными, то есть реализующими какую-то функцию от своих входов, так и коммутационными, которые служат для передачи сигнала к следующему элементу с возможным изменением направления.

В качестве входов и выходов схемы берутся входы и выходы элементов, расположенных на границе схемы. Функциональные элементы схемы соединяются между собой с помощью коммутационных так, чтобы полученная схема представляла собой схему из функциональных элементов (СФЭ). Считаем, что клеточная схема (КС) реализует такие же функции алгебры логики (ФАЛ), что и соответствующая ей СФЭ. Особенностью модели КС, исследуемой в данной работе, является то, что на входы схемы каждая переменная может подаваться неограниченное число раз.

Рассматриваемый в работе базис включает в себя три функциональных клеточных элемента: конъюнкция (имеет два входа на соседних сторонах клетки и два выхода, на которых реализуется конъюнкция входных переменных), дизъюнкция (аналогично), отрицание (имеет один вход и на противоположной стороне элемента один выход, на котором реализуется отрицание входной переменной). Из коммутационных элементов в базисе присутствуют проводник (один вход и один выход на противоположной стороне, куда передается неизменное значение входной переменной), пересечение (два входа и два выхода, значения входных переменных передаются на противоположные стороны элемента без изменения), два элемента поворота (один вход и один выход, элементы являются зеркальным отражением друг друга), изолятор (элемент без входов и выходов). Каждый

из элементов базиса может быть повернут в плоскости на угол, кратный 90 градусам.

Определим ряд функций Шеннона для площади схем в рассматриваемой модели. Обозначим высоту схемы Σ через $h(\Sigma)$, ее длину — через $\lambda(\Sigma)$, а площадь — через $A(\Sigma) = h(\Sigma)\lambda(\Sigma)$, и будем считать, что $h(\Sigma) \leq \lambda(\Sigma)$. Пусть $A(f)$ — наименьшая из площадей $A(\Sigma)$, где минимум берется по всем КС Σ , реализующим ФАЛ f , а $A(n)$ — максимальная из площадей $A(f)$, где максимум берется по всем ФАЛ f от n переменных. Наряду с этой стандартной функцией Шеннона определим аналогичные функции для КС фиксированной высоты. Напомним, что для любой ФАЛ f существует КС высоты два, реализующая эту функцию f . Следовательно, для любого $h, h \geq 2$, и любой ФАЛ f определена функция $A^{(h)}(f)$, равная наименьшей из площадей КС высоты h , реализующих f . При этом для любого $h, h \geq 2$, введем функцию Шеннона $A^{(h)}(n)$, равную максимальной из площадей $A^{(h)}(f)$, где максимум берется по всем ФАЛ $f(x_1, \dots, x_n)$. В работе [2] доказано, что функция $A^{(3)}(n)$ имеет порядок роста $\frac{2^n}{\log n}$. В данной работе исследуются функции Шеннона $A^{(h)}(n)$ для случая $h \geq 4$. Справедлива следующая теорема.

Теорема. $A^{(h)}(n) \sim \frac{h}{2} \frac{2^n}{\log n}$ при $h \geq 4$.¹

Следствие. $A(n) \lesssim \frac{2^{n+1}}{\log n}$.

Ниже приведено доказательство данной теоремы.

Нижняя оценка.

Лемма 1. $A^{(h)}(n) \gtrsim \frac{h}{2} \frac{2^n}{\log n}$ при $h \geq 2$.

Доказательство. Оценим сверху число КС высоты h и длины λ от переменных x_1, \dots, x_n , которые можно построить в рассматриваемой модели. Сначала заполним всю схему клеточными элементами, а потом расставим входы и выход на ее границе — в тех позициях, которые соответствуют входам (выходу) элементов базиса на границе схемы, где будут располагаться входы схемы, и те переменные, которые на них подаются. Заметим, что к каждому входу схемы можно подвести одну из n переменных. Таким образом, с учетом возможных поворотов базисных элементов, имеем 29 вариантов заполнения каждой клетки схемы и $(n+2)^{2\lambda+2h} \cdot 29^{h\lambda}$ ва-

¹Неравенство $a(n) \lesssim b(n)$ означает, что существует последовательность $\varepsilon(n) \rightarrow 0$ при $n \rightarrow \infty$ такая, что выполнено равенство $b(n) \geq a(n)(1 + \varepsilon(n))$. Асимптотическое равенство $a(n) \sim b(n)$ верно, если $a(n) \lesssim b(n)$ и $a(n) \gtrsim b(n)$.

риантов построения всей схемы. Из определения функции Шеннона $A^{(h)}(n) = h \cdot \lambda^{(h)}(n)$ и полученной верхней оценки числа схем вытекает следующее неравенство:

$$(n+2)^{2h} \cdot (n+2)^{2\lambda^{(h)}(n)} \cdot 29^{h\lambda^{(h)}(n)} \geq 2^{2^n}.$$

Решая это неравенство относительно $\lambda^{(h)}(n)$, получаем:

$$\left((n+2) \cdot 29^{\frac{h}{2}} \right)^{2\lambda^{(h)}(n)} \geq \frac{2^{2^n}}{(n+2)^{2h}},$$

$$2\lambda^{(h)}(n) \geq \frac{2^n - 2h \log_2(n+2)}{\log_2(29^{\frac{h}{2}}(n+2))} = \frac{2^n - 2h \log_2(n+2)}{\frac{h}{2} \log_2 29 + \log_2(n+2)} \sim \frac{2^n}{\log n},$$

и, следовательно,

$$A^{(h)}(n) = h \cdot \lambda^{(h)}(n) \gtrsim \frac{h}{2} \frac{2^n}{\log n}.$$

Лемма доказана.

Верхняя оценка.

Для получения верхней оценки используем результаты работы Лупанова О. Б. [3], в которой дается индуктивное определение специальных классов формул с поднятыми отрицаниями в базисе $\{\&, \vee, \neg\}$.

Базис индукции составляют классы $\mathcal{A}_\vee^0 = \mathcal{A}_{\&}^0$, которые состоят из формул

$$x_1, x_2, \dots, x_n, \dots, \bar{x}_1, \bar{x}_2, \dots, \bar{x}_n, \dots$$

Класс \mathcal{A}_\vee^k определяется следующим образом:

- 1) $\mathcal{A}_{\&}^{k-1} \subseteq \mathcal{A}_\vee^k$;
- 2) если $\mathcal{F}_1 \in \mathcal{A}_\vee^k, \mathcal{F}_2 \in \mathcal{A}_\vee^k$, то $(\mathcal{F}_1 \vee \mathcal{F}_2) \in \mathcal{A}_\vee^k$;
- 3) других формул в классе нет.

Класс $\mathcal{A}_{\&}^k$ определяется двойственным образом.

Из [3] следует, что для произвольной функции f существует ее реализация формулой \mathcal{F} из класса \mathcal{A}_\vee^3 , ранг $R(\mathcal{F})$ которой, т. е. число вхождений в нее символов переменных, асимптотически не больше $\frac{2^n}{\log n}$.

Лемма 2. $A^{(h)}(n) \lesssim \frac{h}{2} \frac{2^n}{\log n}$ при $h \geq 4$.

Доказательство. Покажем, что любую ФАЛ от n переменных можно реализовать схемой высоты 4, длина которой асимптотически не больше $\frac{2^{n-1}}{\log n}$.

Пусть f — произвольная ФАЛ от переменных x_1, \dots, x_n . Для этой функции строим формулу \mathcal{F} из \mathcal{A}_V^3 , как в [3]:

$$\mathcal{F} = \bigvee_{i=1}^{k_3} \mathcal{F}_i^{(3)}, \quad \mathcal{F}_i^{(3)} = \bigwedge_{j=1}^{k_{2,i}} \mathcal{F}_{ij}^{(2)}, \quad \mathcal{F}_{ij}^{(2)} = \bigvee_{l=1}^{k_{1,i,j}} \mathcal{F}_{ijl}^{(1)},$$

где $\mathcal{F}_{ijl}^{(1)}$ — либо переменная, либо отрицание переменной.

При этом выполнены следующие соотношения:

$$L(\mathcal{F}) = \sum_{ijl} L(\mathcal{F}_{ijl}^{(1)}) \sim \frac{2^n}{\log n},$$

$$\sum_{i=1}^{k_3} k_{2,i} = \bar{o}\left(\frac{2^n}{\log n}\right).$$

Построим схему Σ_f высоты 4, реализующую в клеточном варианте указанное выше представление произвольной ФАЛ f . Будем описывать эту схему по рядам сверху вниз, начиная с первого ряда и заканчивая четвертым.

Входные переменные подаются на горизонтальные границы схемы в первом и четвертом рядах. В этих рядах собираются все элементарные дизъюнкции $\mathcal{F}_{ij}^{(2)}$ на основе представления вида

$$\bar{x}_{i_1} \vee \bar{x}_{i_2} \vee \dots \vee \bar{x}_{i_k} \vee x_{i_{k+1}} \vee \dots \vee x_{i_m} = \overline{x_{i_1} x_{i_2} \dots x_{i_k}} \vee x_{i_{k+1}} \vee \dots \vee x_{i_m},$$

то есть первыми подаются переменные, входящие в дизъюнкцию с отрицанием.

Для каждой элементарной дизъюнкции $\mathcal{F}_{ij}^{(2)}$ выполняется следующая операция. Набор ее переменных делится на две группы, мощности которых не больше, чем $\left\lceil \frac{R(\mathcal{F}_{ij}^{(2)})}{2} \right\rceil$. Первая группа переменных подается на схему сверху, а вторая снизу. Сначала в четвертом ряду справа налево собирается дизъюнкция первой группы переменных (с использованием элементов конъюнкций и отрицания), затем

она передается на первый ряд, где к этой дизъюнкции добавляются переменные из второй группы (вторая половина дизъюнкции собирается слева направо). Далее полученная дизъюнкция передается на второй ряд схемы.

Во втором ряду схемы собираются конъюнкции, реализующие формулы $\mathcal{F}_i^{(3)}$, значение которых передается на третий ряд.

В третьем ряду собираются дизъюнкции построенных ранее конъюнкций. На выходе последнего элемента дизъюнкции в этом ряду и получим реализацию исходной функции f .

Таким образом, для длины построенной схемы справедливо соотношение

$$\lambda(\Sigma_f) \sim \frac{1}{2} \frac{2^n}{\log n}.$$

Любую функцию от n переменных можно реализовать аналогичной схемой высоты $h \geq 4$, имеющей площадь, асимптотически равную $h \frac{1}{2} \frac{2^n}{\log n}$. А значит, при $h \geq 4$ верно неравенство

$$A^{(h)}(n) \lesssim \frac{h}{2} \frac{2^n}{\log n}.$$

Тем самым доказана лемма 2.

Истинность утверждения теоремы непосредственно следует из доказанных лемм.

Для доказательства следствия из теоремы заметим, что

$$A(n) \lesssim 4 \cdot \frac{1}{2} \frac{2^n}{\log n} = \frac{2^{n+1}}{\log n}.$$

Работа выполнена при финансовой поддержке РФФИ (проект 09-01-00817).

Список литературы

1. Альбрехт А. О схемах из клеточных элементов // Проблемы кибернетики. Вып. 33. — М.: Наука, 1975. — С. 209–214.
2. Тиунчик А. А. О реализации функций алгебры логики клеточными схемами ограниченной ширины // Методы дискретного анализа в решении экстремальных задач. Вып. 50. — Новосибирск: Институт математики, 1990.
3. Лупанов О. Б. О реализации функций алгебры логики формулами из конечных классов (формулами ограниченной глубины) в базисе $\{\&, \vee, \neg\}$ // Проблемы кибернетики. Вып. 6. — М.: Наука, 1961.

О СЛОЖНОСТИ ВЫПОЛНИМОСТИ СИСТЕМЫ ФУНКЦИОНАЛЬНЫХ БУЛЕВЫХ УРАВНЕНИЙ

В. С. Федорова (Москва)

1. Введение

Один из часто используемых способов задания функций и множеств функций в математике — задание с помощью систем функциональных уравнений. Этот способ широко применяется в теории рекурсивных функций и теории автоматов и обладает важным достоинством — простотой и краткостью записи. При определении функциональных уравнений используются функциональные и индивидуальные переменные, а также различные функциональные и индивидуальные константы и, возможно, функционалы и операторы. Немало подобных функциональных уравнений можно найти и в теории функций многозначной логики, особенно в теории булевых функций [1, 2]. Так, с помощью функциональных уравнений можно определять множества монотонных, самодвойственных, линейных и многих других функций.

В настоящей работе рассматриваются функциональные булевы уравнения и проблема распознавания выполнимости для них, которая состоит в следующем: существуют ли булевы функции, удовлетворяющие данному функциональному уравнению. Во всех случаях разрешимых проблем выполнимости существует тривиальный алгоритм решения проблемы выполнимости, перебирающий все возможные значения входящих в формулу переменных и вычисляющий соответствующие значения данной формулы. Такой переборный алгоритм предоставляет достаточно грубую верхнюю оценку временной сложности решения проблемы распознавания выполнимости. Наиболее трудной задачей, как правило, является установление нетривиальной нижней оценки временной сложности решения упомянутой проблемы. Для получения нижних оценок используется моделирование абстрактных вычислительных устройств формулами рассматриваемого типа. Величина нижней оценки при этом может существенно зависеть как от выбранных вычислительных устройств, так и от способа моделирования вычислений на этих устройствах. Чаще всего в качестве абстрактного вычислительного устройства используются различные варианты машин Тьюринга (например, с ограничениями на время или зону работы), а моделирование состоит в описании с помощью формул процесса вычисления на этих машинах.

Целью данной работы является получение верхней и нижней оценок временной сложности решения проблемы распознавания выполнимости для функциональных булевых уравнений.

2. Основные понятия

Дадим необходимые определения. Пусть $E_2 = \{0, 1\}$, P_2 — множество всех функций на E_2 (множество булевых функций), $P_2^{(n)}$ — множество всех n -местных булевых функций.

В определении языка функциональных уравнений придерживаемся терминологии работы [3]. В качестве *функциональных констант* будем использовать булевы функции-константы 0 и 1.

Наряду с функциональными константами рассматриваем *функциональные булевы переменные* $\varphi_i^{(n)}$ с областью значений $P_2^{(n)}$ и обычные *индивидуальные переменные* x_1, x_2, \dots с областью значений E_2 .

Определим понятие *терма*. Всякая индивидуальная переменная и функциональная константа 0 или 1 есть терм. Если t_1, \dots, t_n — термы, $\varphi_i^{(n)}$ — функциональная переменная, то выражение $\varphi_i^{(n)}(t_1, \dots, t_n)$ есть терм.

Равенством или *функциональным булевым уравнением* называем любое выражение вида $t_1 = t_2$, где t_1, t_2 — термы.

Пусть $t_1 = t_2$ — функциональное булево уравнение и $\varphi_{i_1}^{(n_1)}, \dots, \varphi_{i_m}^{(n_m)}$ — все функциональные переменные, входящие в уравнение $t_1 = t_2$. *Решением уравнения* $t_1 = t_2$ называем систему булевых функций $\{f_{j_1}^{(n_1)}, \dots, f_{j_m}^{(n_m)}\}$, которая после замены каждой функциональной переменной $\varphi_{i_s}^{(n_s)}$ соответствующей функциональной константой $f_{j_s}^{(n_s)}$ превращает уравнение $t_1 = t_2$ в тождество (относительно всех входящих в уравнение индивидуальных переменных).

Пусть T — конечная система уравнений. *Решением системы уравнений* T называем систему булевых функций, которая является решением каждого уравнения, входящего в T . Будем говорить, что данные значения всех функциональных переменных, входящих в систему T , *выполняют* эту систему, если эти значения функциональных переменных принадлежат множеству решений данной системы. Конечная система уравнений T *выполнима*, если на множестве P_2 существуют значения всех функциональных переменных, которые выполняют систему T .

Для языка функциональных уравнений сформулируем следующую проблему: *по произвольной конечной системе уравнений T выяснить, является ли T выполнимой*. Данная работа посвящена оценкам сложности решения этой проблемы.

3. Верхняя оценка

Рассмотрим систему функциональных булевых уравнений с функциональными константами 0 и 1. Закодируем ее эффективно

и однозначно словом в алфавите $\{0, 1, \Lambda\}$. В дальнейшем, оценивая сложность проблемы выполнимости функциональных булевых уравнений, будем иметь в виду, что системы функциональных булевых уравнений задаются в этом коде, а сложность проблемы выполнимости оценивается через длину этого кода.

Пусть в системе функциональных булевых уравнений содержатся m различных функциональных переменных, зависящих соответственно от n_1, n_2, \dots, n_m аргументов. Пусть также $n = \max\{n_1, n_2, \dots, n_m\}$. Тогда для проверки выполнимости этой системы методом полного перебора необходимо проверить не более

$$2^{2^{n_1}} \cdot 2^{2^{n_2}} \cdot \dots \cdot 2^{2^{n_m}} \leq (2^{2^n})^m$$

вариантов.

Для величин m и n верны следующие оценки сверху через длину l кода системы функциональных булевых уравнений: m асимптотически не превосходит величины $l / \log_2 l$, а n — соответственно величины l . Тогда на основе вышеприведенного неравенства можно оценить сверху сложность алгоритма, решающего проблему выполнимости для систем функциональных булевых уравнений.

Поскольку в следующем разделе верхняя оценка будет получена с использованием недетерминированных вычислительных устройств, приведем сложность недетерминированного решения данной проблемы: в случае выполнимости системы уравнений проверка ее выполнимости может быть произведена за время, квадратичное относительно $l \cdot 2^l / \log_2 l$. Детерминизация описанной процедуры приводит, разумеется, к экспоненциальному увеличению времени.

4. Нижняя оценка

Для получения нижней оценки временной сложности решения поставленной проблемы используются конечные недетерминированные однородные структуры [4] (далее — ОС).

По произвольной конечной недетерминированной однородной структуре эффективно строится система функциональных булевых уравнений \mathcal{T} , которая выполнима в том и только том случае, когда ОС преобразует начальную конфигурацию в заключительную. Тем самым сложность проверки выполнимости системы уравнений \mathcal{T} оценивается снизу сложностью преобразования начальной конфигурации ОС в заключительную и (в меньшей степени) сложностью построения системы \mathcal{T} по ОС.

Введем необходимые понятия [5]. Пусть $A = (Q, g)$ — конечный недетерминированный автомат с множеством состояний $Q = \{q_0, q_1, \dots, q_{r-1}\}$, двумя входами и двумя выходами и функцией пе-

переходов $g : Q^3 \rightarrow 2^Q \setminus \{\emptyset\}$ (входным алфавитом автомата A является алфавит Q).

Для любого натурального числа m через M_m обозначим линейно упорядоченную последовательность из m копий A_1, A_2, \dots, A_m автомата A , в которой каждый автомат A_i , $1 < i < m$, связан с автоматами A_{i-1} и A_{i+1} . Автоматы A_1 и A_m связаны соответственно только с автоматами A_2 и A_{m-1} .

ОС M_m работает в дискретном времени $t = 1, 2, \dots$. В каждый момент времени $t + 1$ состояние автомата A_i , $1 < i < m$, определяется с помощью функции переходов g состояниями автоматов A_{i-1} , A_i , A_{i+1} в момент времени t . Будем считать, что при вычислении состояний автоматов A_1 и A_m вместо соответственно первого и третьего аргументов в функцию g всегда подставляются значения q_1 и q_2 из Q соответственно.

Согласно приведенным определениям функционирование ОС M_m происходит следующим образом. В начальный момент времени автоматы A_1, A_2, \dots, A_m устанавливаются в некоторые состояния $q_{i_1}, q_{i_2}, \dots, q_{i_m}$. Назовем этот набор состояний *инициальным*. В следующий момент времени вектор-состоянием (или *конфигурацией*) ОС M_m будет набор $(q_{j_1}, q_{j_2}, \dots, q_{j_m})$, где $q_{j_1} \in g(q_1, q_{i_1}, q_{i_2})$, $q_{j_2} \in g(q_{i_1}, q_{i_2}, q_{i_3})$, \dots , $q_{j_{m-1}} \in g(q_{i_{m-2}}, q_{i_{m-1}}, q_{i_m})$, $q_{j_m} \in g(q_{i_{m-1}}, q_{i_m}, q_2)$. Затем к полученным состояниям вновь "применяется" функция g и так далее.

Выделим состояние $q_0 \in Q$ и назовем его *заключительным*. Наложим ограничения на функцию переходов g : если хотя бы один из ее аргументов равен q_0 , то значение функции g также равно $\{q_0\}$. Таким образом, если все автоматы ОС M_m придут в заключительное состояние q_0 , то в дальнейшем с течением времени конфигурация ОС M_m не изменится. В этом случае будем считать, что ОС M_m закончила работу, а конфигурацию (q_0, q_0, \dots, q_0) назовем *заключительной*.

Будем говорить, что ОС M_m *допускает* конфигурацию $(q_{i_1}, q_{i_2}, \dots, q_{i_m})$, если M_m способна преобразовать конфигурацию $(q_{i_1}, q_{i_2}, \dots, q_{i_m})$ в заключительную конфигурацию (q_0, q_0, \dots, q_0) . Очевидно, что при этом число тактов преобразования не превосходит величины r^m . Множество всех конфигураций из Q^m , допускаемых ОС M_m , обозначим через $\mathbf{Rec}(M_m)$, пусть также

$$\mathbf{R}(A) = \bigcup_{m \geq 1} \mathbf{Rec}(M_m).$$

Теорема. *Существует алгоритм временной сложности*

$O(m \cdot \log_2 m)$, который для любого недетерминированного автомата A сводит проблему принадлежности конфигурации множеству $\mathbf{R}(A)$ к проблеме выполнимости некоторой системы функциональных булевых уравнений.

Следствие. Нижняя оценка временной сложности недетерминированного распознавания проблемы выполнимости системы функциональных булевых уравнений по порядку не меньше $d^{\frac{l}{\log_2 l}}$, где $d > 1$.

Работа выполнена при финансовой поддержке Российского фонда фундаментальных исследований (проект 09-01-00701).

Список литературы

1. Ekin O., Foldes S., Hammer P. L., Hellerstein L. Equational characterizations of Boolean function classes // Discrete Mathematics. — 2000. — V. 211. — P. 27–51.

2. Foldes S. Equational classes of Boolean functions via the HSP Theorem // Algebra Universalis. — 2000. — V. 44. — P. 309–324.

3. Марченков С. С., Федорова В. С. О решениях систем функциональных булевых уравнений // Дискретный анализ и исследование операций. — 2008. — Т. 15, № 6. — С. 48–57.

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

5. Марченков С. С. Итерация булевых (n, n) -операторов // Вестник МГУ. Серия 15. Вычислительная математика и кибернетика. — 2006. — № 4. — С. 36–41.

О ПРИБЛИЖЕННОМ ВЫЧИСЛЕНИИ МОНОТОННЫХ БУЛЕВЫХ ФУНКЦИЙ

А. В. Чашкин (Москва)

В работе рассматривается сложность приближенного вычисления монотонных булевых функций схемами из функциональных элементов в базисе из всех двухместных булевых функций. Сложностью вычисления n -местной булевой функции f с точностью $1 - \varepsilon$ называется $\min L(h)$, где минимум берется по всем таким функциям h , что $\sum_{x \in \{0,1\}^n} f(x) \oplus h(x) \leq \varepsilon 2^n$. Известно, что при $n \rightarrow \infty$ для почти всех n -местных булевых функций сложность их вычисления с точностью $1 - o(1)$ асимптотически совпадает со сложностью их точного вычисления и равна $\sim 2^n/n$ — сложности самой сложной n -местной булевой функции, т. е. для почти всех булевых функций невозможно

за счет редких неправильно вычисленных значений сколько-нибудь заметно уменьшить сложность вычислений. Далее будет показано, что для монотонных функций ситуация иная — поступившись точностью можно существенно уменьшить сложность вычислений.

Будем говорить, что монотонные булевы функции f_m и f_M вычисляют n -местную монотонную булеву функцию f с точностью $1 - \varepsilon$, если $f_m(x) \leq f(x) \leq f_M(x)$ для любого $x \in \{0, 1\}^n$ и $f_m(x) \neq f_M(x)$ не более чем на $\varepsilon 2^n$ наборах длины n . Сложностью вычисления n -местной монотонной булевой функции f с точностью $1 - \varepsilon$ назовем $\min L(f_m, f_M)$, где минимум берется по всем парам монотонных функций f_m, f_M , вычисляющих f с точностью $1 - \varepsilon$.

Известно, что при $n \rightarrow \infty$ сложность почти всех n -местных монотонных булевых функций асимптотически совпадает со сложностью самой сложной n -местной монотонной функции f , для которой справедливо равенство

$$L(f) = \frac{2^n}{n\sqrt{\pi n/2}}(1 + o(1)).$$

Сложность приближенного вычисления монотонных булевых функций оценивается в следующей теореме.

Теорема. *Существует такая постоянная c , что любая монотонная n -местная булева функция может быть вычислена с точностью $1 - o(1)$ и сложностью не превосходящей*

$$\frac{2^n}{n\sqrt{\pi n/2}} \cdot n^{-c \log_2 n}.$$

Доказательство. Напомним, что пара вершин n -мерного булева куба $\{0, 1\}^n$ называется ребром, если эти вершины различаются ровно в одном разряде. Пусть (x, y) и (u, v) — такие ребра n -мерного булева куба, что $y \preceq x$ и $v \preceq u$. Эти ребра назовем несравнимыми, если y несравнима с u или x несравнима с v . Последовательность вершин $\alpha = (x_0, \dots, x_n)$ такую, что $x_0 \prec \dots \prec x_n$, будем называть максимальной цепью n -мерного булева куба. Будем говорить, что цепь α проходит через ребро (u, v) , если вершины u и v принадлежат α .

Лемма 1. *Любое множество попарно несравнимых ребер n -мерного булева куба состоит не более чем из $n \binom{n-1}{\lfloor (n-1)/2 \rfloor}$ элементов.*

Доказательство. Пусть N — произвольное множество попарно несравнимых ребер n -мерного булева куба, а N_k — его подмножество, состоящее из всех тех ребер множества N , которые в булевом

кубе соединяют вершины k -го и $(k + 1)$ -го слоев. Если $(\alpha, \beta) \in N_k$, то через это ребро проходит ровно $k!(n - k - 1)!$ максимальных цепей. Так как каждая максимальная цепь проходит ровно через одно ребро множества N , то через все ребра множества N проходит ровно $\sum_{k=0}^{n-1} k!(n - k - 1)!|N_k|$ максимальных цепей. Так как в n -мерном булевом кубе существует только $n!$ различных максимальных цепей, то

$$\begin{aligned} n! &\geq \sum_{k=0}^{n-1} k!(n - k - 1)!|N_k| = (n - 1)! \sum_{k=0}^{n-1} |N_k| / \binom{n-1}{k} \geq \\ &\geq (n - 1)! \left(\sum_{k=0}^{n-1} |N_k| \right) / \binom{n-1}{\lfloor (n-1)/2 \rfloor} = (n - 1)! |N| / \binom{n-1}{\lfloor (n-1)/2 \rfloor}. \end{aligned}$$

Следовательно, $|N| \leq n \binom{n-1}{\lfloor (n-1)/2 \rfloor}$. Лемма доказана.

Пусть f — монотонная булева функция. Ребро (x, y) назовем непостоянным, если $f(x) \neq f(y)$. Так как любые два непостоянных ребра несравнимы, то из леммы 1 вытекает следующее утверждение.

Лемма 2. *У любой n -местной монотонной булевой функции число непостоянных ребер не превосходит $n \binom{n-1}{\lfloor (n-1)/2 \rfloor}$.*

Будем говорить, что ребро (x, y) проходит в i -м направлении, если наборы x и y различаются в i -м разряде.

Лемма 3. *Для любой n -местной монотонной булевой функции найдутся такие направления i_1, i_2, \dots, i_k , что число непостоянных ребер, проходящих в этих направлениях, не превосходит величины $k \binom{n-1}{\lfloor (n-1)/2 \rfloor}$.*

Доказательство. Допустим, что в любых k направлениях i_1, i_2, \dots, i_k проходит в совокупности больше чем $k \binom{n-1}{\lfloor (n-1)/2 \rfloor}$ непостоянных ребер. Тогда сумма S количества непостоянных ребер, взятых по всем k -элементным множествам направлений, больше $k \binom{n-1}{\lfloor (n-1)/2 \rfloor} \binom{n}{k}$. При этом непостоянные ребра каждого направления будут посчитаны ровно $\binom{n-1}{k-1}$ раз. Поэтому в силу леммы 2 сумма S не превосходит величины $n \binom{n-1}{\lfloor (n-1)/2 \rfloor} \binom{n-1}{k-1}$. Таким образом,

$$k \binom{n-1}{\lfloor (n-1)/2 \rfloor} \binom{n}{k} < S \leq n \binom{n-1}{k-1} \binom{n-1}{\lfloor (n-1)/2 \rfloor}.$$

Нетрудно видеть, что величины, стоящие в полученном неравенстве слева и справа от S равны, и, следовательно, сделанное предположение привело к противоречию. Лемма доказана.

Пусть далее $\mathbf{i} = (i_1, i_2, \dots, i_k)$ и $\alpha = (\alpha_1 \alpha_2 \dots \alpha_k)$. Символом $f_{\mathbf{i}}^{\alpha}(x)$ обозначим n -местную функцию с $(n-k)$ существенными переменными, получающуюся из n -местной булевой функции f подстановкой констант α_j вместо ее i_j -х аргументов, а символом $x_{\mathbf{i}}^{\alpha}$ — булев набор длины n , у которого i_j -е разряды равны величинам α_j .

Лемма 4. *Для любой n -местной монотонной булевой функции f найдется такой набор \mathbf{i} , что $f_{\mathbf{i}}^0(x) \neq f_{\mathbf{i}}^1(x)$ не более чем для $2^k \binom{n-1}{\lfloor (n-1)/2 \rfloor}$ различных наборов x длины n .*

Доказательство. Рассмотрим такие i_1, i_2, \dots, i_k , для которых у функции f в этих направлениях в совокупности проходит не более $k \binom{n-1}{\lfloor (n-1)/2 \rfloor}$ непостоянных ребер. Если $f_{\mathbf{i}}^1(x) \neq f_{\mathbf{i}}^0(x)$, то $f_{\mathbf{i}}^1(x) = 1$ и $f_{\mathbf{i}}^0(x) = 0$ и, следовательно, между наборами $x_{\mathbf{i}}^1$ и $x_{\mathbf{i}}^0$ будет не менее k непостоянных ребер. Поэтому каждому неравенству $f_{\mathbf{i}}^1(x) \neq f_{\mathbf{i}}^0(x)$ соответствует не менее k непостоянных ребер, проходящих в направлениях i_1, i_2, \dots, i_k . Так как в этих направлениях проходит не более $k \binom{n-1}{\lfloor (n-1)/2 \rfloor}$ непостоянных ребер, то очевидно, что число неравенств $f_{\mathbf{i}}^1(x) \neq f_{\mathbf{i}}^0(x)$ не превосходит $2^k \binom{n-1}{\lfloor (n-1)/2 \rfloor}$. Лемма доказана.

Функции $f_{\mathbf{i}}^0(x)$ и $f_{\mathbf{i}}^1(x)$ будем называть предками функции $f(x)$, а функцию $f(x)$ потомком этих функций. Каждый из предков f , в свою очередь, имеет по два предка — функции $f_{ij}^{00}(x)$, $f_{ij}^{01}(x)$ и $f_{it}^{10}(x)$, $f_{it}^{11}(x)$, которые будем называть предками второго поколения функции f . Аналогично определим предков f следующих, вплоть до m -го, поколений.

Пусть $f_{i_1 \dots i_s}^{\alpha_1 \dots \alpha_s}(x)$ — предок f s -го поколения, а $f_{i_1 \dots i_s i_{s+1}}^{\alpha_1 \dots \alpha_s 0}(x)$ и $f_{i_1 \dots i_s i_{s+1}}^{\alpha_1 \dots \alpha_s 1}(x)$ предки $f_{i_1 \dots i_s}^{\alpha_1 \dots \alpha_s}(x)$, и, следовательно, предки $(s+1)$ -го поколения f . Нетрудно видеть, что $f_{i_1 \dots i_s i_{s+1}}^{\alpha_1 \dots \alpha_s 0}(x)$ и $f_{i_1 \dots i_s i_{s+1}}^{\alpha_1 \dots \alpha_s 1}(x)$ можно использовать для приближенного вычисления их потомка — функции $f_{i_1 \dots i_s}^{\alpha_1 \dots \alpha_s}(x)$. Для этого достаточно вычислить их значения, и если вычисленные значения совпадут, то, очевидно, они будут равны значению $f_{i_1 \dots i_s}^{\alpha_1 \dots \alpha_s}(x)$. Из леммы 4 следует, что неравенство $f_{i_1 \dots i_s i_{s+1}}^{\alpha_1 \dots \alpha_s 0}(x) \neq f_{i_1 \dots i_s i_{s+1}}^{\alpha_1 \dots \alpha_s 1}(x)$ имеет место не более чем для $2^{k(s+1)} \binom{n-sk-1}{\lfloor (n-sk-1)/2 \rfloor}$ наборов x длины n .

Таким образом, для приближенного вычисления функции f мож-

но воспользоваться следующим алгоритмом. Сначала вычисляются значения всех 2^m предков m -го поколения функции f . Затем вычисляются дизъюнкция f_{\vee} и конъюнкция $f_{\&}$ всех вычисленных значений. Нетрудно видеть, что $f_{\&} \leq f \leq f_{\vee}$ и что если значения f_{\vee} и $f_{\&}$ совпали, то они равны значению f . Оценим величину N равную числу наборов, на которых данным алгоритмом нельзя вычислить значение f , т. е. таких наборов, для которых среди значений потомков m -го поколения будут встречаться как нули, так и единицы.

Допустим, что значения функции $f_{i_1 \dots i_s i_{s+1}}^{\alpha_1 \dots \alpha_s 0}(x)$ нельзя вычислить на множестве $A_{i_1 \dots i_s i_{s+1}}^{\alpha_1 \dots \alpha_s 0}$, а значения функции $f_{i_1 \dots i_s i_{s+1}}^{\alpha_1 \dots \alpha_s 1}(x)$ — на множестве $A_{i_1 \dots i_s i_{s+1}}^{\alpha_1 \dots \alpha_s 1}$. Тогда значение функции $f_{i_1 \dots i_s}(x)$ нельзя определить на множестве $A_{i_1 \dots i_s i_{s+1}}^{\alpha_1 \dots \alpha_s 0} \cup A_{i_1 \dots i_s i_{s+1}}^{\alpha_1 \dots \alpha_s 1}$ и еще не более чем на $2^{k+sk} \binom{n-sk-1}{\lfloor (n-sk-1)/2 \rfloor}$ наборах длины n , на которых не совпадают значения функций $f_{i_1 \dots i_s i_{s+1}}^{\alpha_1 \dots \alpha_s 0}(x)$ и $f_{i_1 \dots i_s i_{s+1}}^{\alpha_1 \dots \alpha_s 1}(x)$.

Пусть N_s — число наборов длины n , на которых нельзя определить значение предка s -го поколения функции f . Пусть $sk < n/2$. Тогда начиная с некоторого n

$$N_s \leq 2N_{s+1} + 2^{k(s+1)} \binom{n-sk-1}{\lfloor (n-sk-1)/2 \rfloor} \leq 2N_{s+1} + 2^k \binom{n}{\lfloor n/2 \rfloor}.$$

Так как $N_m = 0$, то

$$N \leq \sum_{s=1}^m 2^{k+s-1} \binom{n}{\lfloor n/2 \rfloor} \leq 2^{m+k} \binom{n}{\lfloor n/2 \rfloor}.$$

Положим $m = k = \frac{1}{4} \log_2 n - \log_2 \log_2 n$. В этом случае $N = o(2^n)$.

Каждая функция-предок m -го поколения имеет не более $n - mk$ существенных переменных. Следовательно, сложность вычисления всех 2^m предков m -го поколения функции f не превосходит

$$\frac{2^m \cdot 2^{n-km}}{(n-km)\sqrt{\pi(n-km)/2}} (1 + o(1)) = \frac{2^n}{n\sqrt{\pi n/2}} \cdot 2^{-km+m} (1 + o(1)).$$

Нетрудно видеть, что для выбранных значениях m и k найдется такое c , что

$$2^{-km+m} = n^{-c \log_2 n}.$$

Теорема доказана.

Работа выполнена при финансовой поддержке РФФИ (проект 08-01-00863) и программы поддержки ведущих научных школ РФ (проект НШ-4470.2008.1).

Список литературы

1. Забалуев Р. Н. О средней сложности монотонных функций // Дискретная математика. — 2006. — Т. 18, вып. 2. — С. 71–83.
2. Угольников А. Б. О реализации монотонных функций схемами из функциональных элементов // Проблемы кибернетики. — М.: Наука, — 1976. — Вып. 31. — С. 167–185.
3. Чашкин А. В. О сложности реализации булевых функций формулами // Дискретный анализ и исследование операций. — 2005. — Т. 12, вып. 2. — С. 56–72.
4. Pippenger N. Information theory and the complexity of boolean functions // Theory of Computing Systems. — 1976. — V. 10, № 1. — С. 129–167.

О СЛОЖНОСТИ РЕАЛИЗАЦИИ СИММЕТРИЧЕСКИХ ПОЛИНОМОВ

И. Ф. Чебурахин (Москва)

Трудоемкость решения задач анализа и синтеза булевых формул и схем из функциональных элементов известна [1]. Некоторые результаты в этом направлении для отдельных случаев приводятся в [2–4]. Эти случаи определяются естественной классификацией множества всех булевых функций. В качестве одного из таких классов в докладе рассматриваются симметрические булевы функции, представимые полиномами Жегалкина степени два и три, при реализации в базисе $\{\&, \oplus, 1\}$; и аналогично определяемые симметрические полиномы в классе монотонных функций при реализации в базисе $\{\&, \vee\}$ [2–4]. В докладе предлагаются различные методы реализации булевых функций указанного вида в классах формул и схем из функциональных элементов и получаемые при этом оценки показателей качества.

Работа выполнена при финансовой поддержке РФФИ, проект 09-01-90441 Укр Ф.

Список литературы

1. Яблонский С. В. Об алгоритмических трудностях синтеза минимальных контактных схем // Проблемы кибернетики. Вып. 2. — М.: Физматгиз, 1959. — С. 75–121.

2. Чебурахин И. Ф. Функциональные уравнения и сложность булевых функций в разных базисах // Труды VII Международной конференции «Дискретные модели в теории управляющих систем» (Покровское, 4–6 марта 2006 г.). — М.: МАКС Пресс, 2006. — С. 405–411.

3. Чебурахин И. Ф. Преобразования функциональных уравнений и показатели сложности булевых функций // Материалы IX Международного семинара «Дискретная математика и ее приложения», посвященного 75-летию со дня рождения академика О. Б. Лупанова (Москва, 18–23 июня 2007 г.). — М.: Изд-во механико-математического факультета МГУ, 2007. — С. 126–129.

4. Чебурахин И. Ф. Показатели сложности симметрических полиномов Жегалкина // Проблемы теоретической кибернетики. Тезисы докладов XIV Международной конференции (Казань, 2–7 июня 2008 г.). — Казань: Отечество, 2008. — С. 123.

ОБ ОДНОЙ ХАРАКТЕРИСТИКЕ ДЕРЕВЬЕВ, СВЯЗАННОЙ С ИНДИВИДУАЛЬНЫМ ТЕСТИРОВАНИЕМ БЕСПОВТОРНЫХ ФУНКЦИЙ

Д. В. Чистиков (Москва)

Задача тестирования относительно бесповторной альтернативы была поставлена А. А. Вороненко в работе [1]. В той же работе изучались связанные с бесповторными функциями комбинаторные объекты. Вводились *помеченно-раскрашенные* деревья — корневые деревья, внутренние вершины которого имеют не менее двух сыновей и раскрашены правильным образом в два цвета: 0 и 1, — а листьям приписаны попарно различные элементы множества вершин V . Рассматривалось также отображение φ , взаимно однозначно переводящее множество помеченно-раскрашенных деревьев с листьями V во множество ν -графов с вершинами V (см. определения и характеристические свойства в [1–4]).

Поставим, следуя [2, 3], задачу проверяющего тестирования для помеченно-раскрашенных деревьев. Пусть D — помеченно-раскрашенное дерево с листьями V . *Тест-графом* для D будем называть граф T на вершинах V такой, что для любого отличного от D дерева D' с тем же множеством листьев в T найдется ребро e , присутствующее ровно в одном из графов $\varphi(D)$ и $\varphi(D')$. Тест-граф будем

называть *тупиковым*, если при удалении любого ребра он перестает быть тест-графом.

В [2, 3] для данной комбинаторной постановки были получены следующие результаты. Для произвольного помеченно-раскрашенного дерева D были полностью описаны множества тест-графов и тупиковых тест-графов и установлено, что всякий тупиковый тест-граф содержит в точности

$$\nu(D) = \sum_{v \in \text{int } D} \left(-\binom{d(v)}{2} + (d(v) - 1) \sum_{v_i \in v\uparrow} d(v_i) \right)$$

ребер (здесь $\text{int } D$ — множество внутренних вершин дерева D , $v\uparrow$ — множество вершин — сыновей вершины v , $d(v)$ — их количество, причем для листьев полагается $d(v) = 1$). Было также продемонстрировано, что величина $\nu(D)$ характеризует сложность тестирования не только дерева D (в указанном выше смысле), но и ассоциированных с этим деревом неповторных функций в малых базисах. Так, для произвольной функции f , неповторной в базисе B_2 (базисе всех функций двух переменных), длина минимального теста не превосходит $4\nu(\ddot{D})$, где дерево \ddot{D} строится специальным образом из *канонического* дерева D для f [1]. В случае если f дополнительно неповторна в базисе $\{\oplus, \vee\}$ (является функцией *типа* Σ [4]), эта оценка понижается до $\nu(\ddot{D}) + n + 1$ (здесь \ddot{D} получается из D заменой всех пометок \oplus на 0 и \vee на 1). Если же задача тестирования рассматривается для базиса $\{\oplus, \vee\}$, то верхнюю оценку длины минимального теста дает само значение $\nu(\ddot{D})$.

Будем называть величину $\nu(D)$ *характеристикой* дерева D . Поскольку характеристика дерева не зависит от его раскраски, мы будем рассматривать множество всевозможных корневых деревьев, все внутренние вершины которых имеют не менее двух сыновей, — такие деревья будем для краткости называть *ветвящимися*. Дерево с единственной вершиной — корнем будем считать *вырожденным*, все остальные деревья (у них имеется не менее двух листьев) — *невырожденными*.

Докажем некоторые свойства характеристики $\nu(D)$. Вначале получим новый вид ее аналитического представления. Обозначим для этого символом $\text{Int } D$ множество всех *внутренних ребер* дерева D — ребер между внутренними вершинами — и введем величину $b(v) = d(v) - 1$, которую назовем *усеченным ветвлением* вершины v .

Теорема 1. Для ветвящегося дерева с $n \geq 2$ листьями

$$\begin{aligned} \nu(D) &= \sum_{(u,w) \in \text{Int } D} b(u)b(w) + \sum_{v \in \text{int } D} \binom{b(v)+1}{2} = \\ &= \sum_{(u,w) \in \text{Int } D} b(u)b(w) + \frac{1}{2} \sum_{v \in \text{int } D} b^2(v) + \frac{n-1}{2}. \end{aligned}$$

Доказательство. Каждая внутренняя вершина v дает вклад в характеристику, равный

$$- \frac{d(v)(d(v)-1)}{2} + (d(v)-1) \sum_{v_i \in v\uparrow} (d(v_i)-1) + (d(v)-1) \cdot |v\uparrow|.$$

Равенство $|v\uparrow| = d(v)$ позволяет сгруппировать первое и последнее слагаемые. Двойное суммирование по всевозможным $v \in \text{int } D$ и $v_i \in v\uparrow$ равносильно суммированию по всем ребрам (v, v_i) дерева D , причем, в силу того что для листьев $b(v_i) = 0$, невнутренние ребра можно из рассмотрения исключить. После смены обозначений с (v, v_i) на (u, w) и учета того, что сумма усеченных ветвлений всех внутренних вершин любого ветвящегося дерева с $n \geq 2$ листьями равна $n-1$, получим искомое. Отметим дополнительно, что первые слагаемые полученных представлений допускают ведение суммирования по всем ребрам $(u, w) \in E(D)$, а вторые — по всем вершинам $v \in V(D)$ дерева D .

Исследуем, как изменяется характеристика дерева под действием некоторых преобразований. Преобразование \mathcal{T} ветвящегося дерева D назовем ν -эквивалентным, если оно не изменяет его характеристики: $\nu(\mathcal{T}(D)) = \nu(D)$.

Пусть D — произвольное ветвящееся дерево с корнем v_0 . Рассмотрим две произвольные его вершины v_1, v_2 такие, что ни одна из них не лежит на пути из v_0 в другую. Пусть D_1 и D_2 — поддеревья D с корнями v_1 и v_2 ; u_1 и u_2 — родительские вершины для v_1 и v_2 . Поменяем местами поддеревья D_1 и D_2 , объявив родителем v_1 вершину u_2 , а родителем v_2 — вершину u_1 . Назовем такое преобразование *перестановкой поддеревьев D_1 и D_2* и обозначим символом \mathcal{C}^{v_1, v_2} . Выделим также специальный частный случай описанного преобразования. Пусть D_1 — невырожденное поддерево дерева D с корнем v_1 ; v_2 — лист D . Будем в этом случае обозначать преобразование дерева D в дерево $\mathcal{C}^{v_1, v_2}(D)$ символом $\mathcal{M}_{v_2}^{v_1}$ и говорить, что дерево $\mathcal{M}_{v_2}^{v_1}(D)$ получается из дерева D *перевешиванием поддерева D_1 в вершину v_2* (к вершине u_2).

Для заданного ветвящегося дерева D с корнем v_0 будем обозначать символом $U(D)$ некорневое дерево, получаемое из D присоединением к v_0 нового листа и снятием пометки корня. Нетрудно видеть, что для каждой внутренней вершины v получившегося дерева число $\deg v$ ее соседей на 2 больше значения величины $b(v)$ в дереве D . Это означает, что

$$\nu(D) = \sum_{(u,w) \in \text{Int } U(D)} (\deg u - 2)(\deg w - 2) + \frac{1}{2} \sum_{v \in \text{int } U(D)} (\deg v - 2)^2 + \frac{n-1}{2}$$

и приводит нас к следующему определению.

Пусть v — некоторая некорневая внутренняя вершина D , смежная с каким-либо листом w . Заменяем ребро (v, w) в $E(D)$ на ребро (v_0, w) и объявим корнем преобразованного дерева вершину v . Будем говорить, что получаемое таким образом дерево является результатом *переноса корня* дерева D в вершину v , и обозначать соответствующую операцию символом \mathcal{R}_v .

Пусть теперь v_1 и v_2 — смежные внутренние вершины ветвящегося дерева D , причем v_1 — родитель v_2 . Удалим из $E(D)$ все ребра, инцидентные v_1 и v_2 , и заменим в $V(D)$ вершины v_1 и v_2 на новую вершину v , сыновьями которой объявим всех сыновей вершин v_1 (кроме v_2) и v_2 : вершины $v_1^1, \dots, v_1^{b(v_1)}$ и $v_2^0, v_2^1, \dots, v_2^{b(v_2)}$ соответственно. Родителем v объявим родителя v_1 (если таковой имелся в исходном дереве; в противном случае назначим v корнем). Полученное дерево будем обозначать символом $\mathcal{J}^{v_1, v_2}(D)$ и называть результатом *склейки вершин* v_1 и v_2 в D . Обратное преобразование будем обозначать символом $\mathcal{S}_{v_2^0, v_2^1, \dots, v_2^{b(v_2)}}^v$ и называть *расклежкой вершины* v с подъемом вершин $v_2^0, v_2^1, \dots, v_2^{b(v_2)}$.

Теорема 2. *Следующие преобразования являются ν -эквивалентными:*

1. *Перестановка поддеревьев \mathcal{C}^{v_1, v_2} — тогда и только тогда, когда либо $b(v_1) = b(v_2)$, либо $b(u_1) = b(u_2)$ для родителей u_1 и u_2 вершин v_1 и v_2 .*
2. *Перевешивание поддерева $\mathcal{M}_{v_2}^{v_1}$ — тогда и только тогда, когда оно сохраняет усеченное ветвление родительской вершины корня перевешиваемого поддерева: $b(u_1) = b(u_2)$.*
3. *Перенос корня \mathcal{R}_v — всегда.*
4. *Склейка вершин \mathcal{J}^{v_1, v_2} (расклейка вершины \mathcal{S}_{\dots}^v) — тогда и только тогда, когда дерево не имеет внутренних вершин, отличных от v_1 и v_2 (когда v — единственная внутренняя вершина).*

Доказательство. Утверждения 1 и 2 выполняются в силу равенства $\nu(\mathcal{C}^{v_1, v_2}(D)) = \nu(D) - (b(v_2) - b(v_1))(b(u_2) - b(u_1))$, утверждение 3 — в силу изоморфизма графов $U(\mathcal{R}_v(D))$ и $U(D)$, а утверждение 4 — в силу соотношения

$$\nu(\mathcal{J}^{v_1, v_2}(D)) = \nu(D) + b(v_2) \sum_{i_1=1}^{b(v_1)} b(v_1^{i_1}) + b(v_1) \sum_{i_2=0}^{b(v_2)} b(v_2^{i_2}) + b(v_2) bp(v_1),$$

где $bp(v_1) = 0$, если v_1 — корень D и $bp(v_1) = b(u)$, если в D есть u — родитель v_1 .

Рассмотрим теперь вопрос об экстремальных свойствах характеристики $\nu(D)$. Для $q \geq 2$ будем называть ветвящееся дерево q -ичным, если каждая его внутренняя вершина имеет ровно q сыновей.

Теорема 3. *Характеристика произвольного q -ичного дерева D с k внутренними вершинами и $n = k(q - 1) + 1$ листом равна*

$$\nu(D) = n \cdot \left(\frac{3}{2}q - 1 \right) - \left(q^2 - \frac{q}{2} \right) = k \cdot \frac{(q - 1)(3q - 2)}{2} - (q - 1)^2.$$

Доказательство. Используем результат теоремы 1. Подграф $I(D) = (\text{int } D, \text{Int } D)$ дерева D , порожденный множеством вершин $\text{int } D$, сам является деревом, поэтому $|\text{Int } D| = k - 1$. Арифметические преобразования приводят к указанному результату.

Теорема 4. *Характеристика произвольного ветвящегося дерева D с $n \geq 2$ листьями удовлетворяет двойному неравенству $2n - 3 \leq \nu(D) \leq \binom{n}{2}$, нижняя граница в котором достигается лишь на бинарных (двоичных) деревьях и (в случае $n = 3$) трехлистной звезде Z_3 , а верхняя — на деревьях с одной и двумя внутренними вершинами, причем значения $\nu(D)$ для всевозможных D заполняют весь указанный отрезок.*

Доказательство. Искомое неравенство вытекает из того факта, что произвольное ветвящееся дерево с $n \geq 2$ листьями последовательной склейкой (расклейкой) вершин можно преобразовать в звезду Z_n (в некоторое бинарное дерево соответственно). Условия достижения экстремальных значений определяются утверждением 4 теоремы 2. Последнее же утверждение теоремы доказывается индукцией по n с дополнительным требованием наличия в графе $I(D)$ висячей вершины v_1 такой, что $b(v_1) = 1$ в дереве D . Базис индукции проверяется непосредственно. Присоединение к $v_1 \in V(I(D))$ новой висячей вершины увеличивает характеристику дерева D на 2.

Характеристика $(n+1)$ -листового дерева D_k^{n+1} с графом $I(D_k^{n+1})$ — цепью $v_1-v_2-v_3$ с $b(v_1) = 1$, $b(v_2) = k$, $b(v_3) = n-1-k$ равна $\binom{n}{2} + k + 1$, что для $1 \leq k \leq n-2$ дает отрезок $[\binom{n}{2} + 2; \binom{n+1}{2} - 1]$. Это завершает доказательство индукционного перехода; дополнительно отметим, что графы $I(D)$ для всех построенных нами деревьев являются простыми цепями.

Автор выражает признательность А. А. Вороненко за внимание к настоящей работе. Работа выполнена при финансовой поддержке РФФИ (проект 09-01-00817).

Список литературы

1. Вороненко А. А. О проверяющих тестах для неповторных функций // Математические вопросы кибернетики. Вып. 11. — М.: Физматлит, 2002. — С. 163–176.
2. Вороненко А. А. Некоторые вопросы тестирования: Препринт. — М.: МАКС Пресс, 2008.
3. Вороненко А. А., Чистиков Д. В. Индивидуальное тестирование неповторных функций // Ученые записки Казанского университета. Сер. Физико-математические науки. — 2009. — Т. 151, кн. 2. — С. 36–44.
4. Вороненко А. А. Об оценке длины проверяющего теста для некоторых неповторных функций // Прикладная математика и информатика. Т. 15. — М.: МАКС Пресс, 2003. — С. 85–97.

О СЛОЖНОСТИ НЕКОТОРЫХ ОПТИМАЛЬНЫХ ПО НАДЕЖНОСТИ СХЕМ

В. В. Чугунова (Пенза)

При решении некоторых практических задач возникает необходимость реализовать функции специального вида, например элементарную конъюнкцию $K_{\vec{\sigma}}^n = x_1^{\sigma_1} \& x_2^{\sigma_2} \& \dots \& x_n^{\sigma_n}$ ($\sigma_i \in \{0, 1\}$, $n \geq 2$, $\vec{\sigma} = (\sigma_1, \sigma_2, \dots, \sigma_n)$), схемами, оптимальными не только по сложности, но и оптимальными по надежности.

Пусть функциональные элементы подвержены инверсным неисправностям на входах. Рассмотрим задачу реализации элементарной конъюнкции $K_{\vec{\sigma}}^n = x_1^{\sigma_1} \& x_2^{\sigma_2} \& \dots \& x_n^{\sigma_n}$ ($\sigma_i \in \{0, 1\}$) в базисе $\{x_1 \& x_2, x_1 \vee x_2, \bar{x}_1\}$ оптимальной по надежности схемой из ненадежных функциональных элементов, так, чтобы сложность этой схемы была минимальной.

Введем основные понятия.

Будем считать, что схема из функциональных элементов реализует булеву функцию $f(x_1, x_2, \dots, x_n) = f(\tilde{x})$, если при поступлении на входы схемы набора $\tilde{a} = (a_1, a_2, \dots, a_n)$ при отсутствии неисправностей на выходе схемы появляется значение $f(\tilde{a})$. Число входов функциональных элементов равно числу существенных переменных функций, приписанных этим элементам, то есть в рассматриваемом базисе каждый функциональный элемент имеет не более двух входов. Предполагается, что каждый вход элемента схемы независимо от всех других входов элементов с вероятностью ε ($0 < \varepsilon < 1/2$) подвержен инверсным неисправностям. Эти неисправности характеризуются тем, что поступающее на вход элемента значение a ($a \in \{0, 1\}$) с вероятностью ε может превратиться в значение \bar{a} . Заметим, что элементы, реализующие константы 0 и 1, являются абсолютно надежными при инверсных неисправностях на входах элементов.

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

Положим $P_\varepsilon(f) = \inf P(S)$, где S — схема из ненадежных элементов, реализующая булеву функцию f . Схему A из ненадежных элементов, реализующую булеву функцию f , назовем асимптотически оптимальной (наилучшей) по надежности, если $P(A) \sim P_\varepsilon(f)$ при $\varepsilon \rightarrow 0$.

Сложностью $L(S)$ схемы S будем считать число функциональных элементов в ней.

Известно (см., например [1]), что элементарную конъюнкцию $K_\sigma^n = x_1^{\sigma_1} \& x_2^{\sigma_2} \& \dots \& x_n^{\sigma_n}$ в базисе $\{x_1 \& x_2, x_1 \vee x_2, \bar{x}_1\}$ можно реализовать оптимальной по сложности схемой A , сложность которой равна:

$$L(A) = \begin{cases} n - 1, & \text{если } \|\tilde{\sigma}\| = n; \\ n, & \text{если } \|\tilde{\sigma}\| \neq n, \end{cases}$$

где

$$\|\tilde{\sigma}\| = \sum_{i=1}^n \sigma_i,$$

т. е. равно числу единиц в наборе $\tilde{\sigma} = (\sigma_1, \sigma_2, \dots, \sigma_n)$.

В работе [1] надежность схемы A не оценивается. Очевидно, что для схемы A : $P(A) \leq 2\varepsilon n$, где $P(A) < 1$ при $\varepsilon \in (0; 1/(2n))$.

С другой стороны, автором в работе [2] показано, что в базисе $\{x_1 \& x_2, x_1 \vee x_2, \bar{x}_1\}$ произвольную булеву функцию можно реализовать схемой C_1 или C_2 , для которых выполняются условия:

$$P(C_1) \leq 2\varepsilon + 46\varepsilon^2 \text{ при } \varepsilon \in (0; 1/1400] \text{ и } L(C_1) \lesssim 1008 \cdot \frac{2^n}{n},$$

$$P(C_2) \leq 2\varepsilon + 19\varepsilon^2 \text{ при } \varepsilon \in (0; 1/1400] \text{ и } L(C_2) \lesssim 3024 \cdot \frac{2^n}{n},$$

т. е. ненадежность схем C_1 и C_2 по порядку равна ненадежности оптимальной по надежности схемы, но сложность этих схем не является минимальной.

Выясним, можно ли построить схему, реализующую элементарную конъюнкцию $K_{\tilde{\sigma}}^n = x_1^{\sigma_1} \& x_2^{\sigma_2} \& \dots \& x_n^{\sigma_n}$ в базисе $\{x_1 \& x_2, x_1 \vee x_2, \bar{x}_1\}$ с ненадежностью, по порядку равной ненадежности оптимальной по надежности схемы, и минимальной по порядку сложности.

Утверждение о верхней оценке ненадежности схем, реализующих элементарную конъюнкцию $K_{\tilde{\sigma}}^n = x_1^{\sigma_1} \& x_2^{\sigma_2} \& \dots \& x_n^{\sigma_n}$ в базисе $\{x_1 \& x_2, x_1 \vee x_2, \bar{x}_1\}$, содержит теорема 1.

Теорема 1. *При $\varepsilon \in (0; 1/(130n^2)]$ элементарную конъюнкцию $K_{\tilde{\sigma}}^n = x_1^{\sigma_1} \& x_2^{\sigma_2} \& \dots \& x_n^{\sigma_n}$ в базисе $\{x_1 \& x_2, x_1 \vee x_2, \bar{x}_1\}$ можно реализовать схемой S , ненадежность которой $P(S) \leq 2\varepsilon + 19\varepsilon^2$, а сложность*

$$L(S) = \begin{cases} 16n - 1, & \text{если } \|\tilde{\sigma}\| = n; \\ 16n + 15, & \text{если } \|\tilde{\sigma}\| \neq n. \end{cases}$$

Для доказательства теоремы 1 воспользуемся леммой 1.

Построим схему $\varphi(S)$ следующим образом: выходы четырех экземпляров схемы S соединим с входами двух конъюнкторов, выходы которых затем соединим со входами дизъюнктора.

Лемма 1 [2]. *Пусть $\varepsilon \in (0; 1/150]$, f — произвольная функция, S — схема, реализующая функцию f с ненадежностью $P(S)$. Тогда можно построить схему $\varphi(S)$, реализующую функцию f с ненадежностью $P(\varphi(S)) \leq \max\{2\varepsilon + \varepsilon^2 + 4\varepsilon P(S) + 2P^2(S); 9\varepsilon^2 + 12\varepsilon P(S) + 4P^2(S)\}$.*

Доказательство теоремы 1. Пусть элементарная конъюнкция $K_{\tilde{\sigma}}^n = x_1^{\sigma_1} \& x_2^{\sigma_2} \& \dots \& x_n^{\sigma_n}$ в базисе $\{x_1 \& x_2, x_1 \vee x_2, \bar{x}_1\}$ реализована оптимальной по сложности схемой A , сложность которой:

$$L(A) = \begin{cases} n - 1, & \text{если } \|\tilde{\sigma}\| = n; \\ n, & \text{если } \|\tilde{\sigma}\| \neq n. \end{cases}$$

Очевидно, что ненадежность $P(A) \leq 2\varepsilon n$.

По схеме A построим схему $\varphi(A)$, реализующую элементарную конъюнкцию $K_{\tilde{\sigma}}^n = x_1^{\sigma_1} \& x_2^{\sigma_2} \& \dots \& x_n^{\sigma_n}$ и удовлетворяющую условиям леммы 1. Для этого возьмем четыре экземпляра схемы A , выходы которых соединим с входами двух конъюнкторов. Затем выходы конъюнкторов соединим с входами дизъюнктора. По лемме 1 при $0 < \varepsilon \leq \min\{1/(130n^2); 1/150\} = 1/(130n^2)$ и $n \geq 2$ ненадежность схемы $\varphi(A)$:

$$P(\varphi(A)) \leq \max\{2\varepsilon + \varepsilon^2 + 8\varepsilon^2 n + 8\varepsilon^2 n^2; 9\varepsilon^2 + 24\varepsilon^2 n + 16\varepsilon^2 n^2\} = \max\{2\varepsilon + \varepsilon^2(8n^2 + 8n + 1); \varepsilon^2(16n^2 + 24n + 9)\} \leq \max\{2\varepsilon + 13n^2\varepsilon^2; 31n^2\varepsilon^2\} \leq 2, 1\varepsilon.$$

Сложность схемы $\varphi(A)$:

$$L(\varphi(A)) = \begin{cases} 4(n-1) + 3 = 4n - 1, & \text{если } \|\tilde{\sigma}\| = n; \\ 4n + 3, & \text{если } \|\tilde{\sigma}\| \neq n. \end{cases}$$

По схеме $\varphi(A)$ построим схему $\varphi^2(A)$, реализующую элементарную конъюнкцию $K_{\tilde{\sigma}}^n = x_1^{\sigma_1} \& x_2^{\sigma_2} \& \dots \& x_n^{\sigma_n}$ и удовлетворяющую условиям леммы 1. Для этого возьмем четыре экземпляра схемы $\varphi(A)$, выходы которых соединим с входами двух конъюнкторов. Затем выходы конъюнкторов соединим с входами дизъюнктора. По лемме 1 при $\varepsilon \in (0; 1/(130n^2)]$ ненадежность схемы $\varphi^2(A)$:

$$P(\varphi^2(A)) \leq \max\{2\varepsilon + 19\varepsilon^2, 52\varepsilon^2\} = 2\varepsilon + 19\varepsilon^2.$$

Сложность схемы $\varphi^2(A)$:

$$L(\varphi^2(A)) = \begin{cases} 4(4n-1) + 3 = 16n - 1, & \text{если } \|\tilde{\sigma}\| = n; \\ 4(4n+3) + 3 = 16n + 15, & \text{если } \|\tilde{\sigma}\| \neq n. \end{cases}$$

Схема $\varphi^2(A)$ искомая, то есть $S = \varphi^2(A)$.

Теорема 1 доказана.

Пусть $K(n)$ — множество булевых функций $f(x_1, x_2, \dots, x_n)$ вида $f(\tilde{x}) = x_i^a$ (где $i = 1, 2, \dots, n, a \in \{0; 1\}$) и константы 1 и 0.

В работе [2] доказана теорема 2, содержащая утверждение о нижней оценке ненадежности схем, реализующих булевы функции $f(\tilde{x}) \notin K(n)$ в базисе $\{x_1 \& x_2, x_1 \vee x_2, \bar{x}_1\}$.

Теорема 2 [2]. Пусть $\varepsilon \in (0; 1/6]$, $f(\tilde{x})$ — булева функция, $f \notin K(n)$, и S — любая схема, реализующая f . Тогда $P(S) \geq 2\varepsilon - 2\varepsilon^2$.

Очевидно, что для элементарной конъюнкции $K_{\tilde{\sigma}}^n = x_1^{\sigma_1} \& x_2^{\sigma_2} \& \dots \& x_n^{\sigma_n}$ утверждение теоремы 2 справедливо.

Таким образом, из теорем 1 и 2 следует, что в базисе $\{x_1 \& x_2, x_1 \vee x_2, \bar{x}_1\}$ элементарную конъюнкцию $K_{\tilde{\sigma}}^n = x_1^{\sigma_1} \& x_2^{\sigma_2} \& \dots \& x_n^{\sigma_n}$ можно

реализовать асимптотически оптимальной по надежности схемой, функционирующей с ненадежностью, асимптотически равной 2ε , если ε стремится к 0 быстрее, чем $1/(130n^2)$ с ростом n . Сложность таких схем равна:

$$\begin{cases} 16n - 1, & \text{если } \|\tilde{\sigma}\| = n; \\ 16n + 15, & \text{если } \|\tilde{\sigma}\| \neq n, \end{cases}$$

т. е. по порядку равна сложности минимальных схем, построенных из абсолютно надежных элементов.

Из соображений двойственности в базисе $\{x_1 \& x_2, x_1 \vee x_2, \bar{x}_1\}$ утверждения, аналогичные теоремам 1 и 2, справедливы для элементарной дизъюнкции $D_{\tilde{\sigma}}^n = x_1^{\sigma_1} \vee x_2^{\sigma_2} \vee \dots \vee x_n^{\sigma_n}$. Таким образом, элементарную дизъюнкции $D_{\tilde{\sigma}}^n = x_1^{\sigma_1} \vee x_2^{\sigma_2} \vee \dots \vee x_n^{\sigma_n}$ также можно реализовать асимптотически оптимальной по надежности схемой, функционирующей с ненадежностью асимптотически равной 2ε , если ε стремится к 0 быстрее, чем $1/(130n^2)$ с ростом n . Сложность таких схем равна:

$$\begin{cases} 16n - 1, & \text{если } \|\tilde{\sigma}\| = n; \\ 16n + 15, & \text{если } \|\tilde{\sigma}\| \neq n, \end{cases}$$

т. е. по порядку равна сложности минимальных схем, построенных из абсолютно надежных элементов.

Работа выполнена при финансовой поддержке РГНФ (проекты 08-06-00503а, 09-06-28615а/В).

Список литературы

1. Кочергина Г. А. О сложности реализации элементарных конъюнкций и дизъюнкций схемами в некоторых полных базисах // Математические вопросы кибернетики. Вып. 11. — М.: Физматлит, 2002. — С. 219–243.
2. Чугунова В. В. Синтез асимптотически оптимальных по надежности схем при инверсных неисправностях на входах элементов // Дис. ... к. ф.-м. н. — Пенза, 2007.

РАСПРЕДЕЛЕННОЕ ПРЕДСТАВЛЕНИЕ ДИСКРЕТНЫХ ВЕРОЯТНОСТНЫХ АВТОМАТОВ, РЕАЛИЗУЮЩИХ МАРКОВСКИЕ ПОСЛЕДОВАТЕЛЬНОСТИ

С. В. Шалагин (Казань)

Определены модели дискретных вероятностных автоматов, реализующих марковские процессы, на основе систем полиномов от нескольких переменных над полем Галуа. Данные модели ориентированы на распределенную реализацию, допускающую распараллеливание вычислений и потоковую обработку данных, на базе однородных вычислительных структур. Модели стохастических процессов класса марковских [1, 2] представлены на базе полиномиальных функций (ПФ) над полем Галуа. Данный подход для однородных цепей Макова (ЦМ) и их функций представлен в ряде работ [3–5]. Реализация полиномиальных моделей неоднородных ЦМ (НЦМ) и их функций делает их привлекательными для реализации на базе однородных вычислительных структур. НЦМ задана как последовательность состояний вероятностного автомата (ВА) [2]

$$A_{NMCh} = (V, S, \mu(s'/s, v)), \quad (1)$$

где $\mu(s'/s, v)$ — функция переходов, задаваемая системой стохастических матриц (СМ) размерности $m \times m$ вида $\{P_{(s),i}, i = \overline{1, h}\}$, $V = \{v_1, v_2, \dots, v_h\}$ — входной алфавит, $S = \{s_1, s_2, \dots, s_m\}$ — множество состояний.

Замечание 1. В случае, когда для системы СМ вида $\{P_{(s),i}, i = \overline{1, h}\}$ значение $h = 1$, (1) описывает конечную однородную цепь Маркова [1].

Стохастическая функция НЦМ задана последовательностью букв выходного алфавита ВА общего вида [2]

$$A_{FNMCh} = (V, S, Z, \mu(s', z/s, v)), \quad (2)$$

где $Z = \{z_1, z_2, \dots, z_d\}$ — выходной алфавит, $\mu(s', z/s, v)$ задается двумя системами СМ: $\{P_{(s),i}, i = \overline{1, h}\}$ — $m \times m$ -матрицы, определенные аналогично & и $\{P_{(z),i}, i = \overline{1, h}\}$ $m \times d$ -матрицы, определяющие вероятностный закон последовательности выходных букв. На основе $\{P_{(s),i}, i = \overline{1, h}\}$ и $\{P_{(z),i}, i = \overline{1, h}\}$ образуем СМ $P_{(s,h)}$ и $P_{(z,h)}$ размерности $(h \cdot m) \times m$ и $(h \cdot m) \times d$ соответственно.

Замечание 2. В случае, когда для системы СМ вида $\{P_{(z),i}, i = \overline{1, h}\}$ значение $h = 1$, (2) описывает детерминированную функцию процесса, задаваемого ВА вида (1).

Замечание 3. В частном случае, когда $|Z| = 0$ (следовательно, $d = 0$ и матрицы $\{P_{(z),i}, i = \overline{1, h}\}$ — вырождаются), система (2) описывает процесс, определяемый ВА вида (1).

Для (2), согласно [3], определены разложения СМ вида $P_{(s,h)} = \sum_{i=1}^{l_s} p_i M_i$ и $P_{(z,h)} = \sum_{i=1}^{l_z} p_i M_i$, где M_i — простая матрица. Величины $p_i^{(s)}, p_i^{(z)} \in [0, 1]$, $\sum_{i=1}^{l_s} p_i^{(s)} = 1$ и $\sum_{i=1}^{l_z} p_i^{(z)} = 1$, $l_s \leq hm^2 - hm + 1$, $l_z \leq hmd - hm + 1$. На основе полученных систем простых матриц для каждого разложения строим конечные детерминированные автоматы (КДА) [6]. Согласно методике, приведенной в [5], полученные функции переходов КДА определяем на основе ПФ над полем Галуа вида $GF(2^n)$ от одной и двух переменных, которые обозначим как g и f соответственно. В [5] предложен и развит метод реализации произвольной дискретной детерминированной нелинейной функции (ДДНФ) $\psi(x_1, \dots, x_b)$ как суммы элементарных ПФ над $G = GF(2^n)$ вида

$$f(x_1, \dots, x_b) = \sum_{i_1=0}^r \dots \sum_{i_b=0}^r a_{i_1 \dots i_b} x_1^{i_1} \dots x_b^{i_b}, r = 2^n - 1, a_{i_1 \dots i_b}, x_1, \dots, x_b \in G. \quad (3)$$

Определим частный случай ПФ вида (3) от p переменных над G , которая представлена как сумма элементарных полиномов над $GF(2)$:

$$\varphi(t_1, \dots, t_p) = \sum_{i_1=0}^1 \dots \sum_{i_p=0}^1 b_{i_1 \dots i_p} t_1^{i_1} \dots t_p^{i_p}, b_{i_1 \dots i_p}, t_1, \dots, t_p \in GF(2). \quad (4)$$

ПФ вида (3) над G реализована на основе системы, включающей n многочленов вида (4) от $p \leq b \cdot n$ переменных [8].

Обозначим: $U(\psi(x_1, \dots, x_b))$ — множество всевозможных значений ДДНФ $\psi(x_1, \dots, x_b)$; $I(x_j)$ — множество всевозможных значений переменной x_j , $j = \overline{1, b}$, на входе ДДНФ $\psi(x_1, \dots, x_b)$. Следствием введения различного рода ограничений на $U(\psi(x_1, \dots, x_b))$ и $I(x_j)$ является снижение оценок сложности вычисления ПФ вида (3), реализующей $\psi(x_1, \dots, x_b)$ [8].

Определение 1. ПФ вида (3) принадлежит к классам $A(k)$, $k = \overline{1, n}$, если для реализуемой ей ДДНФ $|U(\psi(x_1, \dots, x_b))| \in (2^{k-1}, 2^k)$.

Определение 2 [8]. ПФ вида G принадлежит к классу $B(d_1; d_2; \dots; d_b)$, $d_j \in [1, n]$, $j = \overline{1, b}$, если для реализуемой ей ДД-

НФ $|I(x_1)| \in (2^{d_1-1}, 2^{d_1}), |I(x_2)| \in (2^{d_2-1}, 2^{d_2}), \dots, |I(x_b)| \in (2^{d_b-1}, 2^{d_b})$.

На основе оценок, полученных в [7], сформулирована

Теорема 1 [8]. *Оценки временной и емкостной сложности вычисления полинома вида (3), принадлежащего к классам $A(k), k = \overline{1, n}$, и $B(d_1; d_2; \dots; d_b), d_j \in [1, n], j = \overline{1, b}$, на основе системы ПФ (4), равны, соответственно,*

$$T(A(k), B(d_1; d_2; \dots; d_b)) = \left\lceil \log_2 \sum_{j=1}^b d_j \right\rceil, \quad (5)$$

$$Q(A(k), B(d_1; d_2; \dots; d_b)) = k \left(\sum_{j=1}^b d_j - 1 \right). \quad (6)$$

Модель стохастической функции НЦМ вида (2) реализуема двумя КДА и двумя генераторами дискретной случайной (либо псевдослучайной) величины (ДСВ) [3, 4]. Функция переходов первого КДА определяется ДДНФ вида $f_A(L_s, M)$, где $|L_s| = \min(2^{n_s}) \geq l_s$, $|M| = \min(2^{n_m}) \geq m$, а мощность ее выхода равна $|M|$. Функция переходов второго КДА задана как ДДНФ $f_B(L_z, M)$, где $|L_z| = \min(2^{n_z}) \geq l_z$, а мощность ее выхода равна $|Z| = \min(2^{n_d}) \geq d$.

Лемма. *ДДНФ $f_A(L_s, M)$ принадлежит к классам $A(n_m)$, и $B(n_s; n_m)$, а ДДНФ $f_B(L_z, M)$ — к классам $A(n_d)$ и $B(n_z; n_m)$.*

Генератор ДСВ l_s с законом, определяемым на основе значения величины V , представим генератором равномерно распределенной случайно (псевдослучайной) величины (РРСВ) и ДДНФ от двух переменных вида $f_G(L_v, W)$. С выхода $f_G(L_v, W)$ снимается l_s , $|L_v| = \min(2^{n_h}) \geq h$, а W — n_w -разрядная РРСВ на диапазоне $[0, 2^{n_w} - 1]$. Генератор ДСВ l_z с заданным законом представим генератором $n_{w'}$ -разрядной РРСВ W' , определенной в диапазоне $[0, 2^{n_{w'}} - 1]$, и ДДНФ от одной переменной — $f'_G(W')$. На основе теоремы 3 и леммы 2 при условии, что оценки временной сложности для ПФ $f_G(L_v, W)$ и $f'_G(W')$ будут не более, чем для ПФ $f_A(L_s, M)$ и $f_B(L_z, M)$, определена

Теорема 2. *Оценки временной и емкостной сложности генерирования элементов последовательности, определяемой стохастической функцией неоднородной цепи Маркова, заданной согласно*

(2), на основе ДДНФ вида $f_A(L_s, M)$ и $f_B(L_z, M)$ при использовании системы многочленов вида (4) над $GF(2)$ составляют:

$$T(f_A + f_B) =]\log(n_s + n_m)[+]\log(n_z + n_m)[;$$

$$Q(f_A + f_B) = n_m(n_s + n_m - 1) + n_d(n_z + n_m - 1).$$

Справедливы следствия из теоремы 2.

Следствие 1. При конвейерной реализации процесса генерирования элементов последовательности, определяемой стохастической функцией неоднородной цепи Маркова, заданной согласно (2), на основе ДДНФ вида $f_A(L_s, M)$ и $f_B(L_z, M)$ при использовании системы многочленов вида (4) над $GF(2)$, оценка временной сложности вычисления ее элементов, при сохранении той же оценки емкостной сложности и задействовании $|M|$ D -триггеров будет равна $T(f_A, f_B) = \max(]\log(n_s + n_m)[+]\log(n_z + n_m)[)$.

Следствие 2. Оценки временной и емкостной сложности реализации процесса генерирования элементов последовательности, определяемой неоднородной цепью Маркова, заданной согласно (1), на базе ДДНФ $f_A(L_s, M)$ при использовании системы многочленов вида (4) над $GF(2)$, равны: $T(f_A) =]\log(n_s + n_m)[$ и $Q(f_A) = n_m(n_s + n_m - 1)$.

Если две ДДНФ — $f_G(L_v, W)$ и $f_B(L_z, M)$, заданы ДДНФ от трех переменных вида $f_{GA}(L_v, W, M)$, на выходе которой определены значения из множества S , а две ДДНФ $f'_G(W')$ и $f_B(L_z, M)$ — ДДНФ от двух переменных $f_{GB}(W', M)$, на выходе которой определены значения из Z , то основе теоремы 1 и леммы сформулирована

Теорема 3. Оценки временной и емкостной сложности генерирования элементов последовательности, определяемой стохастической функцией неоднородной цепи Маркова, заданной согласно (2), на основе ДДНФ вида $f_{GA}(L_v, W, M)$ и $f_{GB}(W', M)$ при использовании системы многочленов вида (5) над $GF(2)$ составляют:

$$T(f_{GA}, f_{GB}) = \max(]\log(n_h + n_w + n_m)[+]\log(n'_w + n_m)[);$$

$$Q(f_{GA} + f_{GB}) = n_m(n_h + n_w + n_m - 1) + n_d(n'_w + n_m - 1).$$

Методика реализации генератора (2) на основе систем многочленов вида (4), включает четыре этапа.

Этап 1. Определение множеств $|L_s| = \min(2^{n_s}) \geq l_s$, $|L_z| = \min(2^{n_z}) \geq l_z$, $|L_v| = \min(2^{n_h}) \geq h$. и $|M| = \min(2^{n_m}) \geq m$ и рядности n_w и $n_{w'}$ либо $f_{GA}(L_v, W, M)$ и $f_{GB}(W', M)$.

Этап 2. Используя множества, определенные на этапе 1, получи ДДНФ $f_A(L_s, M)$ и $f_B(L_z, M)$ либо $f_{GA}(L_v, W, M)$ и $f_{GB}(W', M)$.

Этап 3. Определяем согласно [6], вида (3), реализующие ДДНФ $f_A(L_s, M)$ и $f_B(L_z, M)$, $f_{GA}(L_v, W, M)$ и $f_{GB}(W', M)$.

Этап 4. Представление ПФ вида (3), согласно [8], определенных на этапе 3, системами многочленов над $GF(2)$ вида (4).

Для частных случаев, определенных в замечаниях 1–3, предложенная методика также является приемлемой.

Список литературы

1. Кемени Дж., Снелл Дж. Конечные цепи Маркова. — М.: Наука, 1970.
2. Бухараев Р. Г. Основы теории вероятностных автоматов. — М.: Наука, 1985.
3. Захаров В. М., Нурутдинов Ш. Р., Шалагин С. В. Реализация полиномиальных моделей над полем $GF(2^n)$ неоднородных цепей Маркова и их функций в базисе ПЛИС/FPGA // Тезисы докл. науч. конф. — Казань: Центр инновационных технологий, 2006. — С. 62–66.
4. Захаров В. М., Нурутдинов Ш. Р., Соколов С. Ю., Шалагин С. В. Полиномиальное представление конечноавтоматных случайных последовательностей над полем Галуа // Вестник КГТУ им. А. Н. Туполева. — 2003. — № 2. — С. 24–28.
5. Нурутдинов Ш. Р. Основы теории полиномиальных моделей автоматных преобразований над полем Галуа. — Казань: Изд-во КГУ, 2005.
6. Поспелов Д. А. Вероятностные автоматы. — М.: Энергия, 1970.
7. Шалагин С. В. Умножение элементов расширений полей Галуа в базисе ПЛИС/FPGA // Инф. технологии. — 2007. — № 12. — С. 22–27.
8. Шалагин С. В. О представлении нелинейных полиномов над конечным полем распределенной вычислительной системой // Нелинейный мир. — 2009. — № 5. — С. 376–379.

АНАЛИЗ ПРИЗНАКОВ, ИДЕНТИФИЦИРУЮЩИХ АВТОМАТНЫЕ МАРКОВСКИЕ МОДЕЛИ ПО ГЕНЕРИРУЕМЫМ ИМИ ПОСЛЕДОВАТЕЛЬНОСТЯМ

С. В. Шалагин, А. Р. Нурутдинова (Казань)

Автоматные марковские модели используются для решения задач анализа, управления и контроля объектов различной природы в сложных системах и системах управления. В частности, автоматные марковские модели (АММ) позволяют моделировать широкий класс устройств [1, 2]. Актуальными являются задачи синтеза и анализа автоматных марковских моделей [3]. Задача анализа цепей Маркова (ЦМ) имеет важное прикладное значение, связанное с исследованием частотного распределения символов текстов по m -граммам, $m = 2, 3, \dots$ (биграммам, триграммам и т. д.) [4].

Предложена методика идентификации АММ, определяемых на основе эргодических стохастических матриц (ЭСМ) [5] из априори заданных подклассов. Исследованы три группы признаков, отображающих характеристики последовательностей, заданной длины, генерируемых АММ: элементы биграммы (M), частотные признаки (F) и функционалы на основе биграммы (V). Также исследуется вопрос повышения информативности рабочего множества признаков, позволяющих идентифицировать подклассы ЭСМ — P , которые определяют АММ(P), по реализациям ЦМ [5]. Под идентификацией будем понимать отнесение АММ(P) по реализации ЦМ к определенному подклассу ЭСМ с априори заданной вероятностью. Информативность признаков каждой из групп — V , F и M , то есть способность каждой группы признаков идентифицировать АММ(P), по генерируемой ей ЦМ заданной длины N . Определена вероятность идентификации принадлежности АММ к определенному подклассу на основе генерируемой ей ЦМ заданной длины N .

Пусть задана простая конечная однородная ЦМ задана в виде [5]

$$(S, P, \pi_0), \quad (1)$$

где $S = \{i_s\}$, $i = \overline{0, n-1}$ — множество состояний ЦМ, P — ЭСМ вида $P = (p_{ij})$, $i, j = \overline{0, n-1}$, а π_0 — вектор длины n начального распределения вероятности появления каждого состояния ЦМ.

Автономным вероятностным автоматом будем называть систему

$$(\bar{U}, S, \delta(u, s)), \quad (2)$$

где \bar{U} — дискретная случайная величина, принимающая на входе значения u_1, u_2, \dots, u_l с распределением $\bar{p} = (p_1, p_2, \dots, p_l)$, $\sum_{i=1}^n p_i =$

1, $0 \leq p_i \leq 1$, $\delta(u, s)$ — функция переходов, ставящая в соответствие паре (u, s) однозначно новое состояние $s' \in S$.

В качестве АММ(P), порождающей ЦМ, будем рассматривать автомат (2), заданный на основе (1) по алгоритму разложения матрицы P [1]. На АММ(P) накладывается следующее ограничение: значения положительных элементов P в (1) кратны определенной величине D , которая представляет собой дискретность положительных элементов ЭСМ. Данная задача решена в рамках представления АММ в виде системы, включающей конечный детерминированный автомат и генератор дискретной случайной величины [1]. Исследуемые марковские последовательности, являются реализациями простых конечных однородных ЦМ. Они определяются АММ(P), где P принадлежит одному из подклассов ЭСМ: квазитреугольные (T) и блочнообобщающиеся (B) [6].

$$v_g = \begin{cases} 1 : P \in X(g); \\ 0 : \text{иначе} \end{cases}, g = \overline{1, 4}, \quad (3)$$

где $X(1)=T_n$, $X(2)=T_v$, $X(3)=B_l$ и $X(4)=B_p$. Принадлежность к подклассу $X(g)$, $g = \overline{1, 4}$, определена априори. Признаки v_g , определенные согласно (3), являются теоретическими оценками величин \tilde{v}_g вычисление которых производится путем подсчета частот по биграмме $\tilde{P} = (\tilde{p}_{ij})_{n \times n}$, построенной на основе ЦМ определенной длины:

$$\tilde{v}_g = \begin{cases} 1 : \forall \tilde{p}_{ij} : ((\tilde{p}_{ij} \geq 0) \wedge (p_{ij} > 0)) \wedge (\tilde{p}_{ij} = 0) \wedge (p_{ij} = 0) \\ \wedge (P \in X(g)) \\ 0 : \text{иначе} \end{cases}, \quad (4)$$

где $i, j = \overline{0, n-1}$, $g = \overline{1, 4}$, значение $X(g)$ определено по аналогии с (3), $\tilde{p}_{ij} = \frac{1}{N-1} \sum_{z=1}^{N-1} (s(z) = i) \& (s(z+1) = j)$, $s(z)$ — состояние ЦМ в дискретный момент времени z .

Признаки $F = \{\tilde{f}_k\}$, $k = \overline{1-n, n-1}$, характеризуют частоту перехода ЦМ из состояния s_i в состояние s_j для случая, когда $i - j = k$, где $s_i, s_j \in S$, $i, j = \overline{1, n}$. Теоретические значения F равны:

$$f_k = n^{-1} \cdot \sum_{i=1}^{n-|k|} t(i, k), \quad (5)$$

где $t(i, k) = p_{i(i-k)}$ для $k = \overline{1-n, 0}$ и $t(i, k) = p_{(i+k)i}$ для $k = \overline{1, n-1}$.

В группу $M = \{m_r\}$, где $r = \overline{1, n^2}$, включены все элементы ЭСМ P . Данная группа несет полную информацию о структуре P [4].

Пусть множество эмпирических значений для признаков — \tilde{h} : $\tilde{h} \in \{ \tilde{v}_g \ \tilde{m}_r \ \tilde{f}_k \}$, $k = \overline{1-n, n-1}$, $g = \overline{1, 4}$, $r = \overline{1, n^2}$ а h — как теоретическое значение для \tilde{h} . Верхняя оценка длины подпоследовательности N' , на основе которой вычисляются значения признаков, достаточной для идентификации АММ(P_1) и АММ(P_2), где P_1 и P_2 принадлежат различным подклассам ЭСМ с доверительной вероятностью α , определяется согласно формуле:

$$N' = \frac{\tilde{h} (1 - \tilde{h})}{|h - \tilde{h}|^2} t_\alpha^2 \leq \max_{\tilde{h}} \left(\frac{\tilde{h} (1 - \tilde{h})}{\varepsilon^2} t_\alpha^2 \right) = \frac{1}{4\varepsilon^2} t_\alpha^2, \quad (6)$$

где ε — отклонение h и \tilde{h} , t_α — величина, определяющая для закона распределения Гаусса количество среднеквадратических отклонений, которое нужно отложить относительно центра рассеивания, чтобы вероятность попадания в полученный интервал была равна α , $N' = N - 1$ для $\tilde{h} \in \{ \tilde{v}_g \ \tilde{f}_k \}$, $N' = N$ для $\tilde{h} = \tilde{m}_r$.

С целью исследования эффективности решения получены четыре ЭСМ, задающих АММ(P), с максимальным значением энтропии, по одной для каждого из четырех подклассов ЭСМ размерности $n = 6$. Для данных ЭСМ реализовано по 100 ЦМ длины N . Для объектов дискриминации, 400 ЦМ, при использовании специализированной прикладной программы вычислены признаки F , M и V . Минимальная длина, необходимая для идентификации, определяется как достаточная длина для статистического анализа $N = 12$, а максимальная длина — как длина, достаточная для решения задачи при использовании групп признаков V , так как N минимально для V когда ЭСМ имеет размерность $n > 5$. Максимальная длина ЦМ $n = 700$.

Получены факторные решения для ЦМ, сгенерированных на основе АММ(P), где P имеет размерность $n = 5, 6$ (длина генерируемых ЦМ равна 700 и 120 соответственно). Данные решения позволяют сгруппировать (по факторам) признаки из множеств V , F и M , поместив в каждую из групп те из них, которые сильно коррелированы между собой. На основе признаков из данных множеств сгенерированы две таблицы «Объект-признак» [1] — Т5 и Т6. Индекс в наименовании таблиц определен размерностью эргодических стохастических матриц (ЭСМ) — $n = 5, 6$. Т5 и Т6 содержат

200 строк. Т5, содержит 38, а Т6 — 51 столбцов, количество которых определено на основе мощностей множеств V , F и M соответственно. Об информативности данных множеств следует судить по тому, какая доля признаков, в них входящих, объясняется факторным решением. Информативность признаков из множеств V и F в плане решения задачи идентификации АММ(P), достигает 100%. Для элементов ЭСМ (для множества M), в Т5 информативными (при решении задачи ФА) являются только 20 признаков из 25, а в Т6 — только 21 признак из 36. На основании результатов полученных факторных решений следует, что использование функционалов из V и частотных признаков F является перспективным в плане повышения информативности объединенного множества признаков, используемого для идентификации АММ(P).

С целью дискриминации объектов — ЦМ, генерируемых АММ, используются признаки, заданные на базе биграмм, и рассчитываемые на основе ЦМ. Для выделения ЦМ, генерируемой АММ, заданной на базе заданного подкласса ЭСМ, определена своя лингвистическая переменная. Для признаков на базе биграмм лингвистическая переменная определяется по формуле [7]:

$$(v_g, T^* = T \bigcup G(T) = \tilde{p}_{ij} \bigcup \{(P), P \in X(v_g)\}, U = [0, 1], G, M), \quad (7)$$

где T^* — расширение терм-множества лингвистической переменной v_g , T — базовое терм-множество ЛП, $G(T)$ — синтаксическая процедура (правило), описывающая процесс образования из множества T осмысленных для данной задачи значений ЛП. Синтаксическое правило $G(T)$ определено как:

$$p(v_g) = p((P), P \in X(v_g)) = \begin{cases} 0 : & \tilde{Z}(X(v_g)) > 0 \\ \alpha : & \tilde{Z}(X(v_g)) = 0 \end{cases} \quad (8)$$

Функционал $X(v_g)$ принимает значения (Тн, Тв, Бп, Бл), $g = \overline{1, 4}$. $\tilde{Z}(X(v_g))$ — сумма элементов биграммы, которые принимают нулевые значения в случае, когда $P \in X(v_g)$. Доверительная вероятность α определена следующим образом: $\frac{1+\alpha}{2} = F^*(t_\alpha)$, где F^* — функция распределения Гаусса, t_α — величина, определяющая для распределения Гаусса число среднеквадратических отклонений, которое нужно отложить относительно центра рассеивания, чтобы получить интервал, вероятность попадания в который была равна α . t_α для ЛП из

множества V определена согласно формуле вида:

$$t_\alpha = \sqrt{\frac{p_{\max} \cdot N}{1 - p_{\max}}}, \quad (9)$$

где p_{\max} есть максимальное отклонение величины $\tilde{Z}(X(v_g))$ от ее теоретического значения — $Z(X(v_g))$, $g = \overline{1, 4}$. М для (10) определено как следующее высказывание: "последовательность, порождаемая АММ(P), $P \in X(v_g)$, с вероятностью $p(v_g)$, $g = \overline{1, 4}$ ". Таким образом, задано множество ЛП $V = \{v_g\}$, $g = \overline{1, 4}$, которое позволяют определить вероятность принадлежности ЦМ, порождаемой АММ(P), к заданному подклассу ЭСМ.

Список литературы

1. Поспелов Д. А. Вероятностные автоматы. — М.: Энергия, 1970.
2. Бухараев Р. Г. Основы теории вероятностных автоматов. — М.: Наука, 1985.
3. Захаров В. М., Нурмеев Н. Н., Салимов Ф. И., Соколов С. Ю., Шалагин С. В. К задаче дискриминантного анализа автоматных марковских моделей // Вестник Казанского государственного технического университета им. А. Н. Туполева. — 2001. — № 3. — С. 37–39.
4. Friedman W. F., Callimahos D. Military cryptanalysis. Part I. V. Z. — Laguna Hills: Aegean Park Press, 1985.
5. Кемени Дж., Снелл Дж. Конечные цепи Маркова. — М.: Наука, 1970.
6. Сабитова А. Р., Шалагин С. В. Дискриминантный анализ вероятностных моделей марковского типа // Всероссийская конф. молодых ученых "Наука. Технологии. Инновации". Ч. 1. — Новосибирск: Изд-во НГТУ, 2007. — С. 90–92.
7. Заде Л. А. Понятие лингвистической переменной и его применение к принятию приближенных решений. — М.: Мир, 1976.

ТРЕХМЕРНАЯ ВИЗУАЛИЗАЦИЯ НА ОСНОВЕ СИНТАКСИЧЕСКОГО АНАЛИЗА

Т. И. Шарапудинов (Махачкала)

Рассматривается задача ввода редактируемого математического текста на стадии выполнения приложения с последующим построением поверхности

$$x = x(u, v), y = y(u, v), z = z(u, v), \quad (1)$$

где справа от знака равенства располагаются “тексты формул”.

Предлагаются два подхода к решению.

1. Суть первого подхода заключается в следующем. В тексте программы *A.pas* размещена директива, предписывающая компилятору вставить текст из вспомогательного файла с заданным именем. Далее в *A.pas* предусматривается построение поверхности (1) в предположении, что ее описание размещается во вспомогательном файле.

В программе *B* предлагается ввести тексты формул (1) с клавиатуры, после чего в соответствии с правилами выбранного языка программирования подготавливаются тексты описания соответствующих паскалевых функций, которые затем сохраняются в ранее упоминавшемся вспомогательном файле. Затем с помощью одной из предусмотренных в Delphi процедур запуска исполняемых файлов (*WinExec*, *FileExecute* и др.) запускается автономный компилятор, которому в качестве параметра передается имя файла *A.pas*; в результате на диске формируется исполняемый файл *A.exe*. Повторным вызовом той же процедуры программа *A.exe* запускается из программы *B*.

2. Суть второго подхода заключается в совмещении синтаксического анализа древовидной структуры вычислительной схемы для выражения [1] с объектно-ориентированным подходом, позволившим выполнить компиляцию динамически задаваемого выражения. Для повышения качества визуализации привлечена графическая библиотека OpenGL [2–3].

В среде Delphi нами разработано приложение, позволяющее строить параметрические поверхности, масштабировать, выполнять вращение вокруг произвольного вектора, менять цвета и стиль отображения, передвигать, выделять область, сохранять в файле и выводить на печатающее устройство.

3. Отметим, что решение с использованием современных сред программирования встречается в развитых пакетах компьютерной математики, относящихся, скорее, к разряду интерпретируемых,

что замедляет скорость, значительно облегчая при этом принципиальное решение задач рассматриваемого типа.

Работа выполнена при финансовой поддержке гранта 09–01–96504–р_юг_а и гранта РФФИ 07-01-00143-а.

Список литературы

1. Новиков Ф. А. Дискретная математика для программистов. — СПб.: “Питер”, 2001.
2. Краснов М. OpenGL. Графика в проектах Delphi. — СПб.: “БХВ-Петербург”, 2002.
3. Тюкачев Н., Свиридов Ю. Delphi 5. Создание мультимедийных приложений. — СПб.: “Питер”, 2000.

О СЛОЖНОСТИ ТЕСТИРОВАНИЯ ЗАМЫКАНИЙ В ФОРМУЛАХ БУЛЕВЫХ ФУНКЦИЙ

В. И. Шевченко (Нижний Новгород)

В работе рассматриваются формулы булевых функций, в каждой из которых возможны ” \wedge ” замыкания или ” \vee ” замыкания некоторых переменных формулы с другими ее переменными. При этом предполагается, что в любой формуле могут быть или только ” \wedge ” замыкания, или только ” \vee ” замыкания. Для обнаружения этих замыканий используются деревья решений (условные тесты) [1, 2]. В работе изучается временная сложность деревьев решений. Для формул булевых функций в различных базисах получены верхние и нижние оценки минимальной глубины деревьев решений в зависимости от числа переменных в формуле в худшем случае. Данная работа является продолжением работы [3].

Определения

Пусть B произвольное конечное множество булевых функций, которое в дальнейшем иногда будем называть *базисом*. Пусть $A(x_1, \dots, x_n)$ — некоторая формула в базисе B [4], реализующая функцию от переменных x_1, \dots, x_n , а последовательность переменных $J = x_{j_1}, x_{j_2}, \dots, x_{j_t}$ есть все переменные, которые в таком порядке входят в формулу $A(x_1, \dots, x_n)$. Тогда множество формул $U(A)$ определим следующим образом: 1) формула A принадлежит множеству $U(A)$; 2) пусть $x_{p_1}, x_{p_2}, \dots, x_{p_s}$ — некоторая подпоследовательность последовательности переменных J , X_1, X_2, \dots, X_s — произвольные подмножества множества переменных $\{x_1, \dots, x_n\}$, а $C_1(x_{p_1}, X_1), C_2(x_{p_2}, X_2),$

$\dots, C_s(x_{p_s}, X_s)$ — конъюнкции, если имеет место "∧" замыкание, или дизъюнкции, если имеет место "∨" замыкание, переменных из $\{x_{p_1}, X_1\}, \{x_{p_2}, X_2\} \dots, \{x_{p_s}, X_s\}$ соответственно. Тогда формула, полученная из A подстановкой вместо переменных $x_{p_1}, x_{p_2} \dots, x_{p_s}$ соответственно $C_1(x_{p_1}, X_1), C_2(x_{p_2}, X_2) \dots, C_s(x_{p_s}, X_s)$, также принадлежит $U(A)$. Каждая формула, которая может быть получена из A описанным выше способом, принадлежит $U(A)$. Никаких других формул множество $U(A)$ не содержит.

Обозначим через $F(A)$ множество различных функций, реализуемых формулами из $U(A)$. Пусть $F(A) = \{f_1, \dots, f_m\}$, где f_1 — функция, реализуемая формулой A . Тогда множество $U(A)$ разобьем на два подмножества $U_1(A)$ и $U_2(A)$ такие, что все формулы из $U_1(A)$ реализуют функцию f_1 , а формулы из подмножества $U_2(A)$ реализуют функции из множества $F(A) \setminus \{f_1\}$.

Задача контроля. Известно, что формула $A' \in U(A)$. Требуется определить к какому из подмножеств $U_1(A)$ или $U_2(A)$ принадлежит A' .

Для решения этой задачи используются деревья решений.

Дерево решений Y для множества формул $U(A)$ представляет собой конечное ориентированное корневое дерево, которое состоит из двух последовательностей вершин v_0, \dots, v_k и w_1, \dots, w_k , где $k \geq 1$. Вершина v_0 — корневая. Из каждой вершины v_i , где $i = 0, \dots, k-1$, исходят ровно две дуги, одна из которых входит в вершину v_{i+1} , а другая — в вершину w_{i+1} . Из вершин w_1, \dots, w_k и вершины v_k не исходит ни одна дуга. Для $i = 0, \dots, k-1$ вершине v_i приписан двоичный набор $\alpha_i \in \{0, 1\}^n$, дуге, исходящей из v_i и входящей в v_{i+1} , приписано число $\delta_{i+1} \in \{0, 1\}$, а дуге, исходящей из v_i и входящей в w_{i+1} , приписано число $\bar{\delta}_{i+1} \in \{0, 1\}$. При этом функция f_1 — единственная в множестве $F(A)$, которая на наборах $\alpha_0, \dots, \alpha_{k-1}$ принимает значения $\delta_1, \dots, \delta_k$ соответственно и для любой функции f_p из $F(A) \setminus \{f_1\}$ найдется вершина w_{i+1} такая, что, если $i = 0$, то $f_p(\alpha_0) = \bar{\delta}_1$, если $i > 0$, то на наборах $\alpha_0, \dots, \alpha_{i-1}$ функция f_p принимает значения $\delta_1 \dots, \delta_i$, а на наборе α_i — значение $\bar{\delta}_{i+1}$. Каждой вершине w_1, \dots, w_k приписано число 2, а вершине v_k — число 1.

Длина пути дерева решений Y от корня конечной вершины, которой приписано число 1, называется глубиной дерева решений Y и обозначается через $h(Y)$. Величина $h(A) = \min h(Y)$, где минимум берется по всем деревьям решений для формулы A , называется *минимальной глубиной деревьев решений* для A .

Множество различных функций G из $F(A) \setminus \{f_1\}$ будем называть

Π -множеством для формулы A , если для любого набора α из $\{0, 1\}^n$ найдется не более одной функции g из G такой, что $g(\alpha) \neq f(\alpha)$.

Формулу A , реализующую функцию от n переменных, иногда будем обозначать через A_n , а число всех переменных, которые в нее входят, иногда будем называть *длиной формулы* и обозначать через $l(A)$.

Результаты

Утверждения сформулируем для "∧" замыканий, утверждения для случая "∨" замыканий формулируются двойственным образом.

Теорема 1. 1) Если базис $B \equiv \{x \vee y\}$, то для любых $n \geq 2$ и формулы A_n в базисе B справедливо равенство

$$h(A_n) = n.$$

2) Если базис $B \in \{\{x \vee y, x \cdot y\}, \{x \vee y \cdot z\}, \{x \cdot (y \vee z)\}, x \cdot y \vee y \cdot z \vee x \cdot z\}$, то для $n \geq 3$ в базисе B найдется формула A_n такая, что $l(A_n) = O(n)$ и справедливы неравенства

$$2^{\lfloor n/2 \rfloor - 1} \leq h(A_n) \leq \binom{n}{\lfloor n/2 \rfloor}.$$

Теорема 2. Если базис $B \in \{\{x \cdot \bar{y}\}, \{\bar{x} \cdot \bar{y}\}, \{x \vee \bar{y}\}, \{\bar{x} \vee \bar{y}\}, \{x \vee y \cdot \bar{z}\}, \{x \cdot (y \vee \bar{z})\}, \{x \cdot y \vee y \cdot \bar{z} \vee x \cdot \bar{z}\}, \{x \cdot \bar{y} \vee \bar{y} \cdot \bar{z} \vee x \cdot \bar{z}\}\}$ то для $n \geq 3$ в базисе B найдется формула A_n такая, что $l(A_n) = O(n)$ и справедливы неравенства

$$2^{n-2} - 2 \leq h(A_n) \leq 2^n.$$

Утверждения теорем 1 и 2 основываются на следующих вспомогательных утверждениях.

Лемма 1. Пусть G — произвольное Π -множество для формулы A . Тогда $h(A) \geq |G|$.

Лемма 2. Пусть B — базис, все функции которого реализуют монотонные булевы функции, A — формула в этом базисе, реализующая функцию f , и $N_1(f)$ — множество нижних единиц f . Тогда $h(A) \leq |N_1(f)|$.

Лемма 3. Если базис $B \equiv \{x \vee y, x \cdot y\}$, то для $n \geq 3$ в базисе B найдется формула A_n такая, что $l(A_n) = 2n - 1$ и справедливы неравенства

$$2^{\lfloor n/2 \rfloor - 1} \leq h(A_n) \leq \binom{n}{\lfloor n/2 \rfloor}.$$

Лемма 4. Если базис $B \equiv \{x \cdot \bar{y}\}$, то для $n \geq 3$ в базисе B найдется формула A_n такая, что $l(A_n) = n$ и справедливы неравенства

$$2^{n-1} - 2 \leq h(A_n) \leq 2^n.$$

Список литературы

1. Мошков М. Ю. Деревья решений. Теория и приложения. — Нижний Новгород: Изд-во ННГУ, 1994.

2. Чегис И. А., Яблонский С. В. Логические способы контроля работы электрических схем // Тр. Матем. ин-та АН СССР. — 1958. — Т. 51. — С. 270–360.

3. Шевченко В. И. О сложности контроля и диагностики "И" ("ИЛИ") замыканий в формулах монотонных булевых функций // Материалы XIV Международной конференции "Проблемы теоретической конференции" (23–28 мая 2005 г., Пенза).

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

ПРЯМОЕ ДОКАЗАТЕЛЬСТВО ОБОБЩЕННОГО ПРАВИЛА СЛОЖЕНИЯ ЭНТРОПИЙ ДЛЯ ЧАСТИЧНО ОПРЕДЕЛЕННЫХ ДАННЫХ

Л. А. Шоломов (Москва)

В случае недоопределенных данных вместо обычного правила сложения энтропий $H(X) + H(Y|X) = H(XY)$ возникает более сложное соотношение — обобщенное правило [1]. Входящие в него величины заданы неявно как минимумы некоторых выражений, в связи с чем его доказательство в общем виде требует громоздких выкладок (эскиз доказательства имеется в [1]). Но в содержательно важном случае — для частично определенных данных, когда используются лишь полностью определенные и полностью неопределенные символы, эти величины представимы в явном виде, что позволяет дать для этого случая более простое прямое доказательство.

Введем соответствующие понятия. Пусть $M = \{0, 1, \dots, m-1\}$ и каждому непустому подмножеству $T \subseteq M$ сопоставлен символ a_T . Алфавит символов a_T обозначим через A , а его подалфавит $\{a_0, a_1, \dots, a_{m-1}\}$ — через A_0 . Символы из A_0 будем называть *основными*, из A — *недоопределенными*. Доопределением символа $a_T \in A$ назовем всякий основной символ a_i , $i \in T$. Символ a_M , допускающий любое доопределение, назовем *неопределенным* и обозначим $*$.

Будем рассматривать источник X , порождающий символы $a_T \in A$ независимо с вероятностями $p(a_T) \geq 0$. Такой источник будем называть *недоопределенным*, при выполнении условия $p(a_T) = 0$ для $a_T \notin A_0 \cup \{*\}$ — *частично определенным*, а в случае $p(a_T) = 0$ для $a_T \notin A_0$ — *полностью определенным*. Доопределением источника X называется полностью определенный источник X' , задаваемый набором переходных вероятностей $p(a'_i|a_T)$, $i \in T$, $\sum_{i \in T} p(a'_i|a_T) = 1$, и порождающий символы a'_i с вероятностями $p(a'_i) = \sum_T p(a_T)p(a'_i|a_T)$. (Чтобы различать символы a_i источников X и X' , символы из X' обозначаем a'_i .)

Энтропией источника X называется величина

$$\mathcal{H}(X) = \min_Q \left\{ - \sum_{T \subseteq M} p(a_T) \log \sum_{i \in T} q_i \right\}, \quad (1)$$

где минимум берется по наборам $Q = (q_i, i \in M)$, $q_i \geq 0$, $\sum_{i \in M} q_i = 1$ (логарифмы всюду двоичные). Если набор \hat{Q} минимизирует правую часть, будем говорить, что на нем достигается энтропия.

Утверждение 1 [1]. 1. Для любого доопределения X' источника X справедливо неравенство $I(X', X) \geq \mathcal{H}(X)$, где

$$I(X, X') = \sum_{i, T} p(a_T)p(a'_i|a_T) \log \frac{p(a'_i|a_T)}{\sum_S p(a_S)p(a'_i|a_S)}$$

— величина взаимной информации [2].

2. Равенство $I(\hat{X}, X) = \mathcal{H}(X)$ имеет место тогда и только тогда, когда доопределение \hat{X} задается переходными вероятностями $p(\hat{a}_i|a_T) = \frac{\hat{q}_i}{\sum_{j \in T} \hat{q}_j}$, где $\hat{Q} = (\hat{q}_i, i \in M)$ — произвольный набор, на котором достигается энтропия $\mathcal{H}(X)$.

Доопределение \hat{X} из утверждения 1 назовем *лучшим*. Будем считать, что оно единственно (это имеет место при достаточно слабых условиях [1]).

Введем понятие условной энтропии $\mathcal{H}(Y|X)$. Пусть произведение XU недоопределенных источников X и U с алфавитами $A = \{a_T, T \subseteq M\}$ и $B = \{b_U, U \subseteq L\}$, $L = \{0, 1, \dots, l-1\}$, задано совместным распределением $(p(a_T, b_U), T \subseteq M, U \subseteq L)$. Если источник X полностью определен (произведению XU соответствует совместное распределение $(p(a_i, b_U), i \in M, U \subseteq L)$), то при каждом $i \in M$ найдем энтропию $\mathcal{H}(Y|a_i)$ источника U при условии

исхода a_i , используя в (1) вместо вероятностей условные вероятности $p(b_U|a_i) = p(a_i, b_U)/p(a_i)$, где $p(a_i) = \sum_U p(a_i, b_U)$, и положим $\mathcal{H}(Y|X) = \sum_i p(a_i)\mathcal{H}(Y|a_i)$. Если источник X недоопределен, возьмем его лучшее доопределение \hat{X} , найдем совместное распределение $p(\hat{a}_i, b_U) = p(a_T, b_U)p(\hat{a}_i|a_T)$ пар (\hat{a}_i, b_U) в произведении $\hat{X}Y$, используя переходные вероятности из утверждения 1, вычислим $\mathcal{H}(Y|\hat{X})$ и положим $\mathcal{H}(Y|X) = \mathcal{H}(Y|\hat{X})$.

Продолжением доопределения \hat{X} на XY называется полностью определенный источник $\hat{X}Y'$, построенный по $XY\hat{X}$ применением некоторого набора переходных вероятностей $p(b'_j|a_T, b_U, \hat{a}_i)$ и порождающий пары (\hat{a}_i, b'_j) с вероятностями

$$p(\hat{a}_i, b'_j) = \sum_{T,U} p(a_T, b_U, \hat{a}_i)p(b'_j|a_T, b_U, \hat{a}_i).$$

Величину

$$\hat{\mathcal{H}}(XY) = \min_{\hat{X}Y'} I(XY, \hat{X}Y'),$$

где $I(\cdot, \cdot)$ — взаимная информация и минимум берется по всем продолжениям лучшего доопределения \hat{X} , будем называть *энтропией произведения XY при лучшем доопределении источника X* .

Теорема [1]. *Имеет место следующее обобщенное правило сложения энтропий*

$$\mathcal{H}(X) + \mathcal{H}(Y|X) = \hat{\mathcal{H}}(XY).$$

Докажем его для случая частично определенных источников X и Y с алфавитами $\{a_0, \dots, a_{m-1}, *\}$ и $\{b_0, \dots, b_{l-1}, *\}$. Пусть произведение XY задано совместным распределением $p(a_i, b_j) = p_{ij}$, $p(*, b_j) = p_{*j}$, $p(a_i, *) = p_{i*}$ и $p(*, *) = p_{**}$. Тогда $p(a_i) = \sum_j p_{ij} = p_i$, $p(*) = \sum_j p_{*j} = p_*$. Энтропия $\mathcal{H}(X)$ достигается на единственном наборе [3] $\hat{Q} = (\hat{q}_i, i \in M)$, $\hat{q}_i = p_i/(1 - p_*)$ и

$$\mathcal{H}(X) = - \sum_i p_i \log q_i = (1 - p_*) \log(1 - p_*) - \sum_i p_i \log p_i. \quad (2)$$

Лучшее доопределение \hat{X} задается переходными вероятностями $p(\hat{a}_i|a_i) = 1$, $p(\hat{a}_i|*) = \hat{q}_i$, и произведению $\hat{X}Y$ соответствует совместное распределение $p(\hat{a}_i, b_j) = p_{ij} + \hat{q}_i p_{*j} = \pi_{ij}$, $p(\hat{a}_i, *) = p_{i*} + \hat{q}_i p_{**} = \pi_{i*}$.

С учетом того, что $p(b_j|\hat{a}_i) = \pi_{ij}/\hat{q}_i$ и источник $Y|\hat{a}_i$ частично определен, можно согласно [3] найти явное выражение для $\mathcal{H}(Y|\hat{a}_i)$ и затем для $\mathcal{H}(Y|X) = \mathcal{H}(Y|\hat{X}) = \sum_i \hat{q}_i \mathcal{H}(Y|\hat{a}_i)$. Проведем соответствующие выкладки, получаем

$$\mathcal{H}(Y|X) = - \sum_{i,j} \pi_{ij} \log \frac{\pi_{ij}}{\sum_v \pi_{iv}}. \quad (3)$$

Для вычисления $\hat{\mathcal{H}}(XY)$ понадобится утверждение, которое возникает как более сложное проявление эффекта Нечипорука, рассмотренного в [4]. Оно справедливо для недоопределенных источников общего вида. Пусть в произведении XY пара $(*, *)$ встречается с вероятностью $p(*, *) > 0$. Рассмотрим произведение X^0Y^0 , в котором $p^0(*, *) = 0$ и $p^0(a_T, b_U) = p(a_T, b_U)/(1 - p(*, *))$.

Утверждение 2. *Имеют место равенства*

$$\begin{aligned} \mathcal{H}(X) &= (1 - p(*, *))\mathcal{H}(X^0), & \mathcal{H}(Y|X) &= (1 - p(*, *))\mathcal{H}(Y^0|X^0), \\ \hat{\mathcal{H}}(XY) &= (1 - p(*, *))\hat{\mathcal{H}}(X^0Y^0). \end{aligned}$$

В силу этих соотношений, при доказательстве обобщенного правила сложения энтропий можно ограничиться случаем, когда недоопределенных пар $(*, *)$ нет. Вернемся к частично определенным источникам и будем считать, что $p_{**} = 0$.

Рассмотрим продолжение $\hat{X}Y'$ лучшего доопределения \hat{X} на XY . Пусть оно соответствует переходным вероятностям $p(b'_j|a_i, *, \hat{a}_i) = x_{i,j}$. Тогда $p(a_i, b_j, \hat{a}_i, b'_j) = p_{ij}$, $p(a_i, *, \hat{a}_i, b'_j) = p_{i*}x_{i,j}$, $p(*, b_j, \hat{a}_i, b'_j) = \hat{q}_i p_{*j}$, $p(\hat{a}_i, b'_j) = p_{ij} + p_{i*}x_{i,j} + \hat{q}_i p_{*j} = \pi_{ij} + p_{i*}x_{i,j}$. Отметим, что $\sum_{j \in J} x_{i,j} = 1$.

Вычислим

$$\begin{aligned} I(XY, \hat{X}Y') &= \sum_{i,j} \left(p(a_i, b_j, \hat{a}_i, b'_j) \log \frac{p(a_i, b_j, \hat{a}_i, b'_j)}{p(a_i, b_j)p(\hat{a}_i, b'_j)} + \right. \\ &+ \left. p(*, b_j, \hat{a}_i, b'_j) \log \frac{p(*, b_j, \hat{a}_i, b'_j)}{p(*, b_j)p(\hat{a}_i, b'_j)} + p(a_i, *, \hat{a}_i, b'_j) \log \frac{p(a_i, *, \hat{a}_i, b'_j)}{p(a_i, *)p(\hat{a}_i, b'_j)} \right). \end{aligned}$$

Подставив указанные значения и осуществив сокращения, получаем

$I(XY, \hat{X}Y') = \sum_i F_i$, где

$$F_i = \sum_j \left(p_{ij} \log \frac{1}{\pi_{ij} + p_{i*}x_{i,j}} + p_{i*}x_{i,j} \log \frac{x_{i,j}}{\pi_{ij} + p_{i*}x_{i,j}} + \hat{q}_i p_{*j} \log \frac{\hat{q}_i}{\pi_{ij} + p_{i*}x_{i,j}} \right) =$$

$$= \sum_j \left(-(\pi_{ij} + p_{i*}x_{i,j}) \log(\pi_{ij} + p_{i*}x_{i,j}) + p_{i*}x_{i,j} \log x_{i,j} \right) + \hat{q}_i p_{*j} \log \hat{q}_i.$$

Для разных i функции F_i зависят от разных переменных, поэтому минимум $I(XY, \hat{X}Y')$ достигается минимизацией каждой из функций F_i . Отметим, что декомпозиция задачи стала возможной благодаря сведению к случаю $p_{**} = 0$ применением утверждения 2.

Легко проверить, что функция $f(x) = -(a + bx) \log(a + bx) + bx \log x$, $a, b \geq 0$, вогнута вниз при $x \geq 0$. Следовательно, функция F_i от переменных $x_{i,j}$, $j \in J$, также вогнута вниз. Осуществив ее дифференцирование и выполнив ряд преобразований, находим

$$\frac{\partial F_i}{\partial x_{i,j}} = p_{i*} \log \frac{x_{i,j}}{\pi_{ij} + p_{i*}x_{i,j}}.$$

Вычислим $\frac{\partial F_i(\alpha^{(i)})}{\partial x_{i,j}}$ в точке $\alpha^{(i)} = (\alpha_{ij}, j \in J)$, где $\alpha_{ij} = \frac{\pi_{ij}}{\sum_v \pi_{iv}}$.

Имеем после некоторых преобразований

$$\frac{\partial F_i(\alpha^{(i)})}{\partial x_{i,j}} = -p_{i*} \log \left(\sum_v \pi_{iv} + p_{i*} \right).$$

Это значение не зависит от j ; обозначим его через λ_i . Поскольку $\sum_v \pi_{iv} + p_{i*} = \hat{q}_i < 1$, выполнено $\lambda_i > 0$. Отсюда в силу теоремы 4.4.1 из [2] заключаем, что минимум вогнутой вниз функции F_i на множестве векторов вероятностей $(x_{i,j}, j \in J)$ достигается в точке $\alpha^{(i)}$. Учитывая, что в этой точке

$$\pi_{ij} + p_{i*}x_{i,j} = \frac{\pi_{ij}}{\sum_v \pi_{iv}} \left(\sum_v \pi_{iv} + p_{i*} \right) = \hat{q}_i \frac{\pi_{ij}}{\sum_v \pi_{iv}},$$

после некоторых преобразований приводим $F_i(\alpha^{(i)})$ к виду

$$F_i(\alpha^{(i)}) = \sum_j \left(-\hat{q}_i \frac{\pi_{ij}}{\sum_v \pi_{iv}} + \hat{q}_i p_{*j} \right) \log \hat{q}_i - \sum_j \pi_{ij} \log \frac{\pi_{ij}}{\sum_v \pi_{iv}}.$$

Преобразовав первую сумму к $-(\hat{q}_i - \hat{q}_i \sum_j p_{*j}) \log \hat{q}_i = -p_i \log \hat{q}_i$, получаем $F_i(\alpha^{(i)}) = -p_i \log \hat{q}_i - \sum_j \pi_{ij} \log \frac{\pi_{ij}}{\sum_v \pi_{iv}}$. Это в силу (2) и (3) дает $\hat{\mathcal{H}}(XY) = \sum_i F_i(\alpha^{(i)}) = \mathcal{H}(X) + \mathcal{H}(Y|X)$.

Работа выполнена при финансовой поддержке ОНИТ РАН по программе фундаментальных исследований.

Список литературы

1. Шоломов Л. А. Обобщенное правило сложения энтропий для недоопределенных данных // Доклады Академии наук. — 2009. — Т. 427, № 1. — С. 28–31.
2. Галлагер Р. Теория информации и надежная связь. — М.: Советское радио, 1974.
3. Шоломов Л. А. Информационные свойства недоопределенных данных // Дискретная математика и ее приложения: Сборник лекций молодежных научных школ. Вып. IV. — М.: ИПМ РАН, 2007. — С. 26–50.
4. Шоломов Л. А. Распространение эффекта Нечипорука на кодирование с заданным критерием верности // Дискретные модели в теории управляющих систем: VIII Международная конференция. — М.: МАКС Пресс, 2009. — С. 370–374.

О СИНТЕЗЕ ПРЕДИКАТНЫХ СХЕМ НА ОСНОВЕ РАЗЛОЖЕНИЙ ПО ОБОБЩЕННЫМ ПЕРЕМЕННЫМ

М. С. Шуплецов (Москва)

В данной работе рассматривается задача синтеза [3, 7]) для модели схем из предикатных элементов [5, 6]. Рассматриваемая модель обобщает многие классы схем как преобразующего типа, например, схемы из функциональных элементов (СФЭ) и СФЭ с неопределенностями на выходах [1], так и схем проводящего типа, например, контактные и итеративно-контактные схемы [3, 4]. Кроме того, представленный класс схем достаточно близок к модели неявных и параметрических представлений булевых функций [2].

Предикатная схема представляет собой двудольный граф, у которого все вершины одной доли помечены предикатными символами соответствующих предикатных элементов, а вершины другой доли - символами внутренних и внешних переменных. Функционирование

предикатного элемента с k полюсами задается его характеристической функцией от k переменных, связанных с этими полюсами (считается, что элемент находится в допустимом состоянии, если его характеристическая функция равна 1). Схема находится в допустимом состоянии на некотором наборе значений входных переменных тогда и только тогда, когда существует набор значений внутренних переменных такой, что все предикатные элементы схемы будут находиться в допустимом состоянии. Соответствующий набор значений входных переменных будем называть допустимым.

Подмножество M , состоящее из r , $r \geq 2$, переменных предиката $\pi(x_1, \dots, x_n)$, назовем его обобщенной существенной переменной (ОП), если существует такой набор β значений остальных переменных предиката, подстановка которого вместо указанных переменных даст предикат, допустимый только на двух противоположных наборах α и $\bar{\alpha}$ значений переменных из M . При этом набор β будем называть *определяющим*, а наборы α и $\bar{\alpha}$ — *основными* наборами ОП M предиката π . Если один из полюсов предиката π , связанный с переменной из M , выбрать в качестве выходного полюса и считать, что предикат π моделирует некоторый функциональный элемент с неопределенностями на выходе, то определение ОП совпадает с определением обобщенной существенной переменной из работы [1].

Рассмотрим произвольный базис $\mathfrak{B} = \{\pi_i\}_{i=1}^r$, где каждому предикату π_i , $i = \overline{1, r}$, с k_i полюсами сопоставлено положительное число L_i , которое задает “вес” этого предиката. Кроме того, пусть у предиката π_i , $i = \overline{1, r}$ есть m_i минимальных по включению и, возможно, пересекающихся ОП. Тогда приведенным весом $\rho_{\mathfrak{B}}$ базиса \mathfrak{B} назовем следующую величину:

$$\rho_{\mathfrak{B}} = \min_{i: 1 \leq i \leq r, k_i \geq 2, m_i \geq 1} \left\{ \frac{L_i}{\min\{k_i - 1, m_i\}} \right\}.$$

Переменную x_i предиката $\varphi(x_1, \dots, x_n)$ назовем *дизъюнктивной*, если существуют такие булевские константы α_j , $j \neq i$, $i = \overline{1, n}$, что $\chi_{\varphi}(\alpha_1, \dots, \alpha_{i-1}, x_i, \alpha_{i+1}, \dots, \alpha_n) \equiv 1$. Предикат, имеющий хотя бы одну дизъюнктивную переменную, будем называть *дизъюнктивным*. Базис \mathfrak{B} будем называть *обобщенно-дизъюнктивным*, если его приведенный вес достигается на дизъюнктивном предикате π' с k' полюсами (не ограничивая общность рассуждений, будем считать, что у дизъюнктивного предиката первая переменная всегда является дизъюнктивной), который содержит m' различных минимальных по включению ОП, содержащих первую переменную предиката π' и не имеющих пересечений по другим переменным этого предиката.

Пусть $\mathcal{U}_{\mathfrak{B}}$ — класс предикатных схем, построенных в базисе \mathfrak{B} , а $\Pi_2(n)$ — множество всех булевских предикатов от n переменных. Под сложностью $L_{\mathfrak{B}}(\Sigma)$ предикатной схемы Σ , $\Sigma \in \mathcal{U}_{\mathfrak{B}}$, понимается сумма весов её предикатов, а под сложностью $L_{\mathfrak{B}}(\phi)$ предиката ϕ — минимальная из сложностей реализующих его схем. Введем обычным образом функцию Шеннона

$$L_{\mathfrak{B}}(n) = \max_{\phi \in \Pi_2(n)} L_{\mathfrak{B}}(\phi)$$

для класса $\mathcal{U}_{\mathfrak{B}}$ предикатных схем в базисе \mathfrak{B} относительно функционала сложности L .

В работе [5] была получена асимптотика функции Шеннона для сложности предикатных схем в достаточно широком классе базисов, а в работе [6] — оценки высокой степени точности для некоторых базисов специального вида. Основным результатом этой работы является следующее утверждение.

Теорема. *Если \mathfrak{B} — обобщенно-дизъюнктивный базис, то для функции Шеннона $L_{\mathfrak{B}}(n)$ справедлива следующая оценка*

$$L_{\mathfrak{B}}(n) \leq \rho_{\mathfrak{B}} \frac{2^n}{n} \left(1 + O\left(\frac{\log_2 n}{n}\right) \right).$$

Для доказательства теоремы построим аналог обобщенного разложения [3] в случае схем из предикатных элементов на основе специальной системы ОП.

Лемма 1. *Пусть a и N , $N \geq 2^a$, — натуральные числа, и дизъюнктивный предикат $\Phi(z_0, \dots, z_N)$ содержит N различных минимальных по включению ОП M_1, \dots, M_N , содержащих дизъюнктивную переменную z_0 . Пусть, кроме того, каждая переменная x_k , $i = 1, \dots, 2^a$, входит хотя бы в одну из ОП M_l , $l = 1, \dots, 2^a$. Тогда существуют такие предикаты $\psi_i(y_i, x_1, \dots, x_a, w_{i_1}, \dots, w_{i_{t_i}})$, $1 \leq i \leq N$, где i_j , $j = 1, \dots, t_i$, — номера ОП, содержащих переменную x_i , и верно равенство*

$$\begin{aligned} (\exists y_1) \dots (\exists y_N) \Phi(z_0, y_1, \dots, y_N) \bigwedge_{i=1}^N \psi_i(y_i, \hat{x}, w_{i_1}, \dots, w_{i_{t_i}}) = \\ = \bigvee_{\sigma=(\sigma_1, \dots, \sigma_a)} x_1^{\sigma_1} \cdot \dots \cdot x_a^{\sigma_a} \cdot w_{\nu(\sigma)+1} \sim z_0, \end{aligned} \quad (1)$$

где $\hat{x} = (x_1, \dots, x_a)$, а $\nu(\sigma)$ — номер набора σ .

Доказательство. Зафиксируем произвольный набор γ значений переменных из множества \hat{x} и рассмотрим левую часть равенства (1). Так как для ОП $M_{\nu(\alpha)+1}$ предиката Φ существует определяющий

набор β значений всех остальных переменных, которые не входят в $M_{\nu(\alpha)+1}$, и основной набор α значений переменных, которые входят в $M_{\nu(\alpha)+1}$, то предикаты ψ_i , $i = 1, \dots, N$, можно задать следующим образом:

$$\psi_i(y_i, \gamma, w_{i_1}, \dots, w_{i_{t_i}}) = \begin{cases} y_i \sim \beta_i, & \text{если } x_i \notin M_{\nu(\alpha)+1}, \\ y_i \sim w_{\nu(\alpha)+1} \oplus \alpha_i, & \text{иначе.} \end{cases}$$

В таком случае, при фиксированных значениях переменных \hat{x} , существует единственный допустимый набор значений переменных $\hat{y} = (y_1, \dots, y_N)$. Подставив набор γ и допустимые значения для переменных \hat{y} , получаем, что по определению ОП $M_{\nu(\alpha)+1}$ левая часть равенства (1) переходит в $z_0 \sim w_{\nu(\alpha)+1}$, и при этом в правой части получается аналогичное выражение.

Лемма доказана.

Лемма 2. Если $\mathfrak{B} = \{\pi_i\}_{i=1}^r$ — обобщенно-дизъюнктивный базис, то для любого предиката $\phi(x_1, \dots, x_n)$, $\phi \in \Pi_2(n)$, существует реализующая его предикатная схема Σ_ϕ , $\Sigma_\phi \in \mathcal{U}_{\mathfrak{B}}$, такая, что

$$L_{\mathfrak{B}}(\Sigma_\phi) \leq \rho_{\mathfrak{B}} \frac{2^n}{n} \left(1 + O\left(\frac{\log_2 n}{n}\right) \right).$$

Доказательство. Пусть k и u , $u \leq (n-k)$, — натуральные параметры. Рассмотрим такое разбиение $\Delta = (\delta_1, \dots, \delta_p)$ наборов булева куба B^n , что любой суффикс набора из B^n длины k встречается только в одной компоненте δ_i , $i = 1, \dots, p$, и при этом среди наборов каждой компоненты δ_i можно выделить ровно s различных суффиксов. Нетрудно видеть, что $p \leq \frac{2^k}{s} + 1$. Если $f_i(x_1, \dots, x_n)$, $i = 1, \dots, p$, — функции, которые на наборах из δ_i , $i = 1, \dots, p$, совпадают с характеристической функцией χ_ϕ предиката ϕ , то верно следующее представление

$$\phi(x_1, \dots, x_n) = (\exists Y) \left(\bigvee_{i=1}^p \bigvee_{\tilde{\sigma}=(\sigma_1, \dots, \sigma_u)} x_1^{\sigma_1} \cdot \dots \cdot x_u^{\sigma_u} \cdot y_{i, \tilde{\sigma}} \right) \cdot \bigwedge_{i=1}^p \bigwedge_{\tilde{\sigma}=(\sigma_1, \dots, \sigma_u)} (f_{i, \tilde{\sigma}}(x_{u+1}, \dots, x_n) \sim y_{i, \tilde{\sigma}}), \quad (2)$$

где $f_{i, \tilde{\sigma}}(x_{u+1}, \dots, x_n) = f_i(\tilde{\sigma}, x_{u+1}, \dots, x_n)$ и Y — список переменных $y_{i, \tilde{\sigma}}$, $i = 1, \dots, p$, $\tilde{\sigma} \in B^u$. Построим схему Σ_ϕ на основе разложения (2). Получим предикат Φ с $l \cdot m'$ ОП при помощи следующей процедуры: возьмем l копий предиката $\pi_{\mathfrak{B}}$ и отождествим первые переменные этих предикатов. Пусть $2^{n-k-u} \leq l \cdot m'$, тогда предикаты $\pi_{f_{i, \tilde{\sigma}}} = f_{i, \tilde{\sigma}}(x_{u+1}, \dots, x_n) \sim y_{i, \tilde{\sigma}}$ можно разложить по переменным

x_{u+1}, \dots, x_{u-k} , используя лемму 1. Из структуры предиката Φ вытекает, что вспомогательные предикаты ψ_i , которые возникают в разложении (1), зависят от не более, чем $(n - k - u + 1)$ переменной. Используя построения работы [1], для предикатов $\pi_{f_i, \tilde{\sigma}}$ и ψ_i можно построить предикатную схему со сложностью, не превосходящей $c'(2^{n-k-u}(2^{n-k-u} + p2^s + 1) + ps2^s + 2^k)$, где c' — константа, зависящая от базиса \mathfrak{B} . Предикаты Φ можно реализовать со сложностью, не превосходящей $p2^{ul} \cdot L'$. Остальная часть разложения (2) требует не более, чем $c'2^u(p + 1)$ предикатных элементов. Выбирая значения параметров: $k = \lfloor 2 \log_2 n \rfloor$, $s = \lceil n - 4 \log_2 n \rceil$, $u = \lfloor n - 3 \log_2 n \rfloor$, получаем, что сложность схемы Σ_ϕ можно оценить следующим образом:

$$L(\Sigma_\phi) \leq \frac{L'}{m'} \cdot \frac{2^n}{n - 4 \log_2 n} + O\left(\frac{2^n}{n^2}\right) = \rho_{\mathfrak{B}} \frac{2^n}{n} \left(1 + O\left(\frac{\log_2 n}{n}\right)\right).$$

Лемма доказана.

Из леммы 2 вытекает справедливость основной теоремы данной работы.

Работа выполнена при финансовой поддержке РФФИ (проект 09-01-00817-а).

Список литературы

1. Долгополова А. В. Задача синтеза и проблемы полноты для одного класса схем из функциональных элементов, связанных с электронными схемами. — Диссертация на соискание ученой степени кандидата физико-математических наук. — М., 2003.
2. Касим-Заде О. М. О сложности параметрических представлений булевых функций // Математические вопросы кибернетики. Вып. 7. — М.: Наука. Физматлит, 1998. — С. 85–160.
3. Лупанов О. Б. Асимптотические оценки сложности управляющих систем. — М.: Изд-во МГУ, 1984.
4. Ложкин С. А. Оценки высокой степени точности для сложности управляющих систем из некоторых классов // Математические вопросы кибернетики. Вып. 6. — М.: Наука. Физматлит, 1996. — С. 189–214.
5. Шуплецов М. С. Асимптотика функции Шеннона в некоторых базисах с элементами блочного типа // Материалы XVII Международной школы-семинара “Синтез и сложность управляющих систем” имени академика О. Б. Лупанова (Новосибирск, 27 октября – 1 ноября 2008 г.). — Новосибирск: Изд-во института математики, 2008. — С. 196–201.
6. Шуплецов М. С. Оценки высокой степени точности для сложности предикатных схем в некоторых базисах // Ученые записки

Казанского университета. Сер. Физико-математические науки. — 2009. — Т. 151, кн. 2. — С. 173–184.

7. Shannon C. E. The synthethis of two-terminal switching circuits // Bell Syst. Techn. J. — 1949. — V. 28, № 1. — P. 59–98.

О ПРЕДЕЛЬНЫХ ВЕРОЯТНОСТЯХ ЗНАЧЕНИЙ СЛУЧАЙНЫХ ВЫРАЖЕНИЙ В КВАЗИГРУППАХ

А. Д. Яшунский (Москва)

Конечное множество Q с определённой на нём бинарной операцией умножения \cdot будем называть *квазигруппой*, если для любых $a, b \in Q$ уравнения $a \cdot x = b$ и $y \cdot a = b$ всегда разрешимы относительно x и y , причём однозначно [1]. Эта однозначность равносильна тому, что на множестве Q также могут быть определены бинарные операции \backslash и $/$ (левое и правое деление, соответственно) такие, что $x = a \backslash b$ и $y = b/a$. Для удобства далее будем обозначать элементы квазигруппы через $1, 2, 3, \dots, q$.

Определим понятие *бесповторной формулы* в квазигруппе Q по индукции. Во-первых, любая переменная является бесповторной формулой. Во-вторых, если $\hat{\Phi}$ и $\hat{\Psi}$ — бесповторные формулы, и множества их переменных не пересекаются, то $(\hat{\Phi} \cdot \hat{\Psi})$ есть также бесповторная формула. Далее будем отождествлять бесповторные формулы, различающиеся лишь наименованием переменных. *Сложностью* бесповторной формулы будем называть число вхождений в неё символа \cdot (операции умножения).

Выражением в квазигруппе Q будем называть строку, получающуюся в результате подстановки констант из Q вместо всех переменных некоторой бесповторной формулы. Для каждого выражения однозначно (с точностью до наименования переменных) определена бесповторная формула, порождающая это выражение. Сложностью выражения Φ будем называть сложность порождающей формулы и обозначать $|\Phi|$.

Введём вероятностную меру на множестве всех выражений сложности n в квазигруппе Q . Обозначим через s_n число бесповторных формул сложности n ($s_n = \frac{1}{n+1} \binom{2n}{n}$). Определим на выражениях в квазигруппе функцию π следующим образом. Для выражений, состоящих из одного символа $i \in Q$, положим $\pi(i) = p_i$, где все $p_i \geq 0$ и $\sum_{i \in Q} p_i = 1$. Для выражения $(\Phi \cdot \Psi)$ положим $\pi((\Phi \cdot \Psi)) = \pi(\Phi)\pi(\Psi)$.

Вероятность $\mathcal{P}(\Phi)$ выражения Φ положим равной $\pi(\Phi)/s_n$. Легко проверить, что при таком определении, действительно, выражения сложности n образуют вероятностное пространство.

Содержательно такое распределение вероятностей соответствует случайному равновероятному выбору порождающей бесповторной формулы для выражения среди всех бесповторных формул сложности n , и независимой случайной подстановке символов вместо переменных формулы. При этом вероятность подстановки символа $i \in Q$ вместо переменной равна r_i .

Каждое выражение Φ принимает некоторое значение $i \in Q$. Будем записывать это как $\Phi = i$. Рассмотрим в вероятностном пространстве выражений сложности n вероятности событий $\{\Phi = i\}$: $P_{i,n} = \mathcal{P}\{\Phi = i\}$. Следующая теорема показывает, что при достаточно общих условиях величины $P_{i,n}$ имеют предел при $n \rightarrow \infty$.

Теорема. Пусть Q — квазигруппа из q элементов, с определённым выше распределением вероятностей на множестве выражений сложности n , и пусть все $r_i > 0$. Тогда для всех $i \in Q$ существует предел $P_i = \lim_{n \rightarrow \infty} P_{i,n} = 1/q$.

Отметим, что если квазигруппа Q является группой, соответствующее утверждение является, фактически, фольклорным (подробнее о случайных блужданиях на группах см. [4]). Принципиальным отличием групп является наличие ассоциативности у операции умножения, позволяющей свести рассмотрение случайных выражений в группе к рассмотрению цепей Маркова.

Для доказательства теоремы введём производящие функции:

$$T_i(z) = \sum_n s_n P_{i,n} z^n \text{ и } S(z) = \sum_n s_n z^n.$$

Эти функции можно рассматривать как формальные степенные ряды, для которых сложение, умножение на константы и перемножение определяются обычным образом. Будем использовать обозначение $[z^n]F(z)$ для n -го коэффициента в степенном ряде F .

В силу равенства $\sum_{i \in Q} T_i(z) = S(z)$ выполнено

$$P_{i,n} = \frac{[z^n]T_i}{[z^n]S} = \frac{[z^n]T_i}{[z^n](T_1 + \dots + T_k)}.$$

Таким образом, для нахождения предела P_i достаточно исследовать асимптотику коэффициентов $[z^n]T_i$ при $n \rightarrow \infty$.

Воспользовавшись подходом Шютценберге в применении к формальной грамматике, описывающей выражения в квазигруппе, или же путём непосредственной проверки, можно получить, что производящие функции $T_i(z)$, $i \in Q$ удовлетворяют уравнениям:

$$T_i(z) = p_i + z \sum_{j \cdot k = i} T_j(z) T_k(z). \quad (1)$$

Для анализа асимптотического поведения коэффициентов производящих функций $T_i(z)$ будет использоваться теорема Дрмота—Лэлли—Вудса (подробнее см. [3]). Возможность её применения обусловлена наличием у системы уравнений (1) следующих дополнительных свойств:

- 1) *нелинейность*: система нелинейна по функциям $T_i(z)$;
- 2) *положительность*: все коэффициенты в правых частях уравнений (1) неотрицательны;
- 3) *корректность* (система задаёт сжимающее отображение в пространстве векторов из формальных степенных рядов с метрикой $d(\vec{T}, \vec{T}') = 2^{-\text{val}(T_j - T'_j)}$, где $\text{val}(F) = \beta$, если $F = \sum_{n \geq \beta} f_n z^n$ и $f_\beta \neq 0$): проверяется для системы (1) непосредственно;
- 4) *неразложимость*² (в ориентированном графе зависимостей между переменными T_i , где из k -ой в j -ю вершину проводится дуга, если k -е уравнение содержит T_j , любые две вершины соединены ориентированным путём): для системы (1) следует из того, что каждое уравнение содержит все переменные T_i ;
- 5) *апериодичность* (формальный степенной ряд F называется периодическим, если существуют натуральные $r, d \in \mathbb{N}$, $r > 1$, такие что $F = \sum_{n \geq 0} f_{rn+d} z^{rn+d}$ и апериодическим в противном случае; система уравнений апериодическая, если все компоненты её решения апериодические): следует из положительности $[z^n]T_i$ при всех n и i , которая в свою очередь вытекает непосредственно из неравенств $p_i > 0$.

²Ранее использовался термин *несводимость*, однако, по аналогии с терминологией для цепей Маркова, по-видимому, следует использовать термин *неразложимость*.

Благодаря наличию всех вышеперечисленных свойств, система удовлетворяет условиям теоремы Дрмота—Лэлли—Вудса, а также следствия 2 из работы [3]. По указанному следствию, все функции $T_i(z)$ (как функции комплексного переменного) имеют общую особую точку $\omega \in \mathbb{R}^+$, ряды $T_i(z)$ сходятся внутри круга радиуса ω , и асимптотическое поведение коэффициентов $[z^n]T_i$ определяется разложением функций $T_i(z)$ в ряды Пуизо в окрестности точки ω :

$$T_i(z) = \tau_i + C_i\sqrt{\omega - z} + o(\sqrt{\omega - z}). \quad (2)$$

А именно, имеет место асимптотическое равенство

$$[z^n]T_i(z) \sim -\frac{1}{2\sqrt{\pi}}\omega^{-n+1/2}n^{-3/2}C_i.$$

Следовательно, для интересующих нас величин P_i выполнены соотношения:

$$P_i = \frac{C_i}{C_1 + C_2 + \dots + C_q}. \quad (3)$$

Так как коэффициенты рядов $T_i(z)$ положительны, точка ω является особой и для их суммы $S(z)$. Складывая все уравнения системы (1), получаем, что $S(z)$ удовлетворяет уравнению $S = 1 + zS^2$. Обозначив $S(\omega)$ через σ , по теореме о неявной функции [2] получим, что ω и σ удовлетворяют уравнению $1 = 2\omega\sigma$.

Отметим также, что имеет место соотношение:

$$\sigma = \tau_1 + \tau_2 + \dots + \tau_q. \quad (4)$$

Подставляя разложения (2) в систему уравнений (1) и приравнявая коэффициенты в правой и левой частях уравнений при $\sqrt{\omega - z}$, получаем, что коэффициенты C_i удовлетворяют уравнениям:

$$C_i = \omega \sum_{j \cdot k = i} C_j \tau_k + \omega \sum_{j \cdot k = i} \tau_j C_k,$$

которые можно переписать в виде:

$$C_i = \omega \sum_j (\tau_{j \setminus i} + \tau_{i/j}) C_j.$$

Эти уравнения (в силу соотношения (4)) линейно зависимы и определяют значения C_i лишь с точностью до общего множителя, однако,

принимая во внимание равенства (3), несложно заметить, что для P_i выполнены аналогичные соотношения:

$$P_i = \omega \sum_j (\tau_{j \setminus i} + \tau_{i/j}) P_j, \quad (5)$$

которые, очевидно, дополняются уравнением $P_1 + P_2 + \dots + P_q = 1$.

Покажем, что $P_i = 1/q$ удовлетворяют системе уравнений (5). Подставляя $P_i = 1/q$ в правую часть уравнения, получим:

$$\frac{1}{q} \omega \sum_j (\tau_{j \setminus i} + \tau_{i/j}). \quad (6)$$

В силу свойств операций \setminus и $/$ в квазигруппе, имеют место соотношения:

$$\sum_j \tau_{j \setminus i} = \sum_j \tau_{i/j} = \sum_j \tau_j.$$

Из уравнения (4) вытекает, что выражения (6) при всех i равны $2\omega\sigma/q$, что, в силу $1 = 2\omega\sigma$, равно $1/q$. Таким образом, $P_i = 1/q$ действительно удовлетворяют уравнениям (5), что доказывает теорему.

Автор выражает благодарность О. М. Касим-Заде за полезные обсуждения и внимание к работе.

Работа выполнена при финансовой поддержке РФФИ (проект 08-01-00863), программы поддержки ведущих научных школ РФ (проект НШ-4470.2008.1) и программы фундаментальных исследований ОМН РАН «Алгебраические и комбинаторные методы математической кибернетики и информационные системы нового поколения» (проект «Задачи оптимального синтеза управляющих систем»).

Список литературы

1. Белоусов В. Д. Основы теории квазигрупп и луп. — М.: Наука, 1967.
2. Евграфов М. А. Аналитические функции. — М.: Наука, 1968.
3. Яшунский А. Д. Об асимптотике вероятности значений случайных булевых выражений // Дискретный анализ и исследование операций. — 2006. — Т. 13, № 2. — С. 59–99.
4. Saloff-Coste L. Random walks on finite groups. Probability on discrete structures. Encyclopaedia Math. Sci., 110, ed. Kesten H. — Berlin: Springer, 2004. — P. 263–346.

ИНФОРМАЦИЯ

Серия школ-семинаров «Синтез и сложность управляющих систем» основана академиком Олегом Борисовичем Лупановым и проводилась под его руководством начиная с 1988 года. Первая школа-семинар этого цикла была организована во Львове (1988), последующие школы-семинары проходили в Новосибирске (1989, 2004, 2008), Ташкенте (1990), Нижнем Новгороде (1992, 1994, 1996, 1998, 2000, 2003), Минске (1993, 1995, 1999), Пензе (2001, 2003, 2009), Санкт-Петербурге (2006). С 2006 г. серии школ-семинаров «Синтез и сложность управляющих систем» присвоено имя академика О. Б. Лупанова.

XVIII Международная школа-семинар «Синтез и сложность управляющих систем» имени академика О. Б. Лупанова, материалы которой публикуются в данном сборнике, прошла в Пензе с 28 сентября по 3 октября 2009 г. Эта школа-семинар была организована механико-математическим факультетом Московского государственного университета имени М. В. Ломоносова, Институтом прикладной математики имени М. В. Келдыша РАН и Пензенским государственным университетом.

В работе школы-семинара приняли участие более 40 математиков из Москвы, Санкт-Петербурга, Казани, Нижнего Новгорода, Пензы, Иркутска, Ярославля и Махачкалы. Было заслушено 35 докладов, большинство из которых представлены в настоящем сборнике. Полный список докладов приводится ниже:

Д. А. Алекберли (Махачкала). Условия оптимизации частного случая расписания из 2-нагрузок.

М. А. Алехина, С. М. Грабовская (Пенза). Об асимптотически оптимальных по надежности неветвящихся программах в полном конечном базисе с функциями $x_1 \oplus x_2, x_1 \& x_2$.

М. А. Алехина, П. Г. Пичугина (Пенза). О надежности двойственных схем в произвольном полном конечном базисе.

Л. Н. Бондаренко (Пенза). Многочлены Эйлера и их связь с перманентами и гафнианами.

А. В. Васин (Пенза). Оценки ненадежности оптимальных схем в базисе $\{x_1 \& x_2, \bar{x}_1\}$ при инверсных неисправностях на выходах элементов.

С. Ф. Винокуров, А. С. Францева (Иркутск). Сложность булевых функций в некоторых классах обратимых схем.

А. А. Вороненко (Москва). О сложности распознавания свойств не всюду определенных дискретных функций.

М. А. Герасимов (Санкт-Петербург). О битовой длине разбиений

входного потока алгоритма Хаффмана при реализации на машинах Тьюринга с почти линейным временем.

А. А. Груздов (Ярославль). Сравнительный анализ динамической информационной модели DIM и ORM систем.

Д. А. Дагаев (Москва). Об одном классе псевдолинейных функций.

А. Б. Дайняк, Д. С. Романов, М. С. Шуплецов (Москва). О реализации булевых функций контактными схемами со структурными ограничениями.

О. С. Дудакова (Москва). О конечной порожденности предполных классов монотонных функций девятизначной логики.

Л. П. Жильцова, А. А. Рызаев (Нижний Новгород). О свойствах матрицы первых моментов и деревьев вывода для разложимой стохастической КС-грамматики в критическом случае.

А. С. Казимиров (Иркутск). Преобразования булевых функций, сохраняющие сложность полиномов.

Р. М. Колпаков (Москва), М. Раффино (Париж), М. Рао (Бордо). О числе слов Дежан над алфавитом из 5, 6 и 7 букв.

В. В. Кочергин (Москва). О сложности вентильных схем с кратным числом путей.

В. Б. Ларионов (Москва). О надструктуре некоторых семейств замкнутых классов монотонных k -значных функций.

А. М. Магомедов (Махачкала). Применение теоремы о разбиении гиперграфа к задаче оптимизации расписания.

Т. А. Магомедов (Махачкала). Непрерывное 3-тестирование.

П. П. Макарычев (Пенза). Модели многокомпонентных систем на основе маркированных графов.

Р. Г. Мубаракзянов (Казань). Определение конечности множества состояний функции цепи Маркова.

В. И. Пантелеев (Иркутск). Мульти- и ультраклоны на двухэлементном множестве.

О. А. Садовников (Москва). О реализации некоторых функций схемами с подведением переменных, вложенными в единичный куб.

А. Ю. Улесова (Москва). О сложности реализации функций алгебры логики в одной модели клеточных схем.

В. С. Федорова (Москва). О сложности выполнимости системы функциональных булевых уравнений.

А. В. Чашкин (Москва). О приближенном вычислении монотонных булевых функций.

И. Ф. Чебурахин (Москва). О сложности реализации элементарных симметрических полиномов.

Д. В. Чистиков (Москва). Об одной характеристике деревьев, связанной с индивидуальным тестированием бесповторных функций.

В. В. Чугунова (Пенза). О сложности некоторых оптимальных по надежности схем.

С. В. Шалагин (Казань). Распределенное представление дискретных вероятностных автоматов, реализующих марковские процессы.

С. В. Шалагин, А. Р. Нурутдинова (Казань). Анализ признаков, идентифицирующих автоматные марковские модели по генерируемым ими последовательностям.

Т. И. Шарапудинов (Махачкала). Трехмерная визуализация на основе синтаксического анализа.

В. И. Шевченко (Нижний Новгород). О сложности тестирования замыканий в формулах булевых функций.

Л. А. Шоломов (Москва). Прямое доказательство обобщенного правила сложения энтропий для частично определенных данных.

М. С. Шуплецов (Москва). О синтезе предикатных схем на основе разложений по обобщенным переменным.

А. Д. Ящунский (Москва). О предельных вероятностях значений случайных выражений в квазигруппах.

Информация о предыдущих школах-семинарах и их материалы опубликованы в следующих изданиях:

1. Віст. АН УРСР [Вестник АН УССР, на укр. языке]. — 1989. — № 3. — С. 104–105.

2. Методы дискретного анализа в изучении булевых функций и графов. Вып. 48. — Новосибирск, 1989. — С. 95–103.

3. Сибирский журнал исследования операций. — 1994. — Т. 1, № 1. — С. 75–84.

4. Дискретный анализ и исследование операций. — 1995. — Т. 2, № 1. — С. 68–81.

5. Материалы VII Межгосударственной школы-семинара «Синтез и сложность управляющих систем» (Минск, 13–16/XI 1995.). — М.: Изд-во механико-математического факультета МГУ, 1996. — 30 с.

6. Материалы IX Межгосударственной школы-семинара «Синтез и сложность управляющих систем» (Нижний Новгород, 16–19 декабря 1998 г.). — М.: Изд-во механико-математического факультета МГУ, 1999. — 100 с.

7. Материалы X Межгосударственной школы-семинара «Синтез и сложность управляющих систем» (Минск, 29 ноября – 3 декабря

1999 г.). — М.: Изд-во центра прикладных исследований при механико-математическом факультете МГУ, 2000. — 31 с.

8. Материалы XI Международной школы-семинара «Синтез и сложность управляющих систем» (Нижний Новгород, 20–25 ноября 2000 г.). Части I, II. — М.: Изд-во центра прикладных исследований при механико-математическом факультете МГУ, 2001. — 264 с.

9. Материалы XII Межгосударственной школы-семинара «Синтез и сложность управляющих систем» (Пенза, 15–21 октября 2001 г.). Части I, II. — М.: Изд-во центра прикладных исследований при механико-математическом факультете МГУ, 2001. — 263 с.

10. Материалы XIII Международной школы-семинара «Синтез и сложность управляющих систем» (Пенза, 14–20 октября 2002 г.). Части I, II. — М.: Изд-во центра прикладных исследований при механико-математическом факультете МГУ, 2002. — 216 с.

11. Материалы XIV Международной школы-семинара «Синтез и сложность управляющих систем» (Нижний Новгород, 27 октября – 1 ноября 2003 г.). — Нижний Новгород: Изд-во Нижегородского государственного педагогического университета, 2003. — 132 с.

12. Материалы XV Международной школы-семинара «Синтез и сложность управляющих систем» (Новосибирск, 18–23 октября 2004 г.). — Новосибирск: Изд-во Института математики, 2004. — 118 с.

13. Материалы XVI Международной школы-семинара «Синтез и сложность управляющих систем» (Санкт-Петербург, 26–30 июня 2006 г.). М.: Изд-во механико-математического факультета МГУ, 2006. — 159 с.

14. Материалы XVII Международной школы-семинара «Синтез и сложность управляющих систем» имени академика О. Б. Лупанова (Новосибирск, 27 октября — 1 ноября 2008 г.). — Новосибирск: Изд-во Института математики, 2008. — 202 с.