ИНСТИТУТ ПРИКЛАДНОЙ МАТЕМАТИКИ им. М. В. КЕЛДЫША
РОССИЙСКОЙ АКАДЕМИИ НАУК

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

МАТЕРИАЛЫ VII МОЛОДЕЖНОЙ НАУЧНОЙ ШКОЛЫ ПО ДИСКРЕТНОЙ МАТЕМАТИКЕ И ЕЕ ПРИЛОЖЕНИЯМ

(Москва, 18–23 мая 2009 г.)

ЧАСТЬ I

Москва 2009

МАТЕРИАЛЫ
VII МОЛОДЕЖНОЙ НАУЧНОЙ ШКОЛЫ
ПО ДИСКРЕТНОЙ МАТЕМАТИКЕ И ЕЕ ПРИЛОЖЕНИЯМ

(Москва, 18–23 мая 2009 г.)

ЧАСТЬ I

Москва 2009

М34
УДК 519.7

Издание осуществлено при поддержке Российского фонда фундаментальных исследований по проекту 09–01–06027

М34 Материалы VII молодежной научной школы по дискретной математике и ее приложениям (Москва, 18–23 мая 2009 г.). Часть I. Под редакцией А. В. Чашкина. 2009.— 54 с.

Сборник содержит материалы VII молодежной научной школы по дискретной математике и ее приложениям, проходившей в Москве с 18 по 23 мая 2009 г. при поддержке Российского фонда фундаментальных исследований (проект 09–01–06027). Для студентов, аспирантов и научных работников в области дискретной математики и математической кибернетики.

Научное издание

МАТЕРИАЛЫ
VII МОЛОДЕЖНОЙ НАУЧНОЙ ШКОЛЫ
ПО ДИСКРЕТНОЙ МАТЕМАТИКЕ И ЕЕ ПРИЛОЖЕНИЯМ
(Москва, 18–23 мая 2009 г.)

Под общей редакцией А. В. ЧАШКИНА

Ответственный за выпуск *А. Д. Яшунский*

СОДЕРЖАНИЕ

О ЧИСЛЕ «ХОРОШИХ» ФУНКЦИЙ $f(x_1,x_2,x_3,x_4)$

М. А. Алехина, Н. С. Спиридонов, О. Ю. Черепанова (Пенза)

Рассматривается реализация булевых функций схемами из ненадежных функциональных элементов в полном конечном базисе B [1]. Предполагается, что все функциональные элементы независимо друг от друга с вероятностью ε ($\varepsilon \in (0;1/2)$) подвержены инверсным неисправностям на выходах, когда функциональный элемент E с приписанной ему функцией e в неисправном состоянии реализует функцию $\bar{e}$. Считаем, что схема из ненадежных функциональных элементов реализует булеву функцию $f(\tilde{x})$ ($\tilde{x} = (x_1, x_2, ..., x_n)$), если при поступлении на входы схемы набора $\tilde{a}$ при отсутствии неисправностей в схеме на ее выходе появляется значение $f(\tilde{a})$.

Число $P(S) = \max\limits_{\tilde{a}} P_{\bar{f}(\tilde{a})}(S, \tilde{a})$ называется ненадежностью схемы S, где $P_{\bar{f}(\tilde{a})}(S, \tilde{a})$ — вероятность ошибки схемы S, реализующей функцию f, на входном наборе $\tilde{a}$. Схема A из ненадежных элементов, реализующая функцию f, называется асимптотически оптимальной по надежности, если $P(A) \sim P_\varepsilon(f)$ при $\varepsilon \to 0$, т. е. $\lim\limits_{\varepsilon\to 0} \frac{P_\varepsilon(f)}{P(A)} = 1$, где $P_\varepsilon(f) = \inf\limits_S P(S)$, инфимум берется по всем схемам S из ненадежных элементов, реализующим функцию $f(\tilde{x})$.

Впервые задачу синтеза надежных схем из ненадежных элементов рассматривал Дж. фон Нейман [2]. Он предполагал, что все элементы схемы независимо друг от друга с вероятностью ε подвержены инверсным неисправностям на выходах. Дж. фон Нейман предложил итерационный метод, позволяющий при $\varepsilon \in (0, 1/6)$ произвольную булеву функцию реализовать схемой, ненадежность которой не больше $\varepsilon + c_1\varepsilon^2$ (c_1 — некоторая положительная константа), при условии, что в рассматриваемом базисе содержится функция голосования $g(x_1, x_2, x_3) = x_1x_2 \vee x_1x_3 \vee x_2x_3$.

Поскольку любая схема S, содержащая хотя бы один элемент, имеет ненадежность $P(S) \geqslant \varepsilon$, схемы, предлагаемые Дж. фон Нейманом (и вообще, схемы, ненадежность которых не больше $\varepsilon+c_1\varepsilon^2$), являются асимптотически оптимальными по надежности для всех функций, кроме $x_1, x_2, ..., x_n$, которые можно реализовать абсолютно надежно, не используя функциональных элементов.

В [3] найдены и другие функции $h(x_1, x_2, x_3)$, наличие которых в базисе B гарантирует реализацию произвольной булевой функции схемой S, функционирующей с ненадежностью $P(S) \leqslant \varepsilon+c_2\varepsilon^2$, где $\varepsilon \in (0, d_2]$, c_2, d_2-

некоторые положительные константы. Функции $h(x_1, x_2, ..., x_k)$, обладающие таким свойством, будем называть «хорошими». Точнее, функция $h(x_1, x_2, ..., x_k)$, $k \geqslant 3$, называется хорошей, если ее наличие в базисе B гарантирует реализацию произвольной булевой функции асимптотически оптимальной схемой S, функционирующей с ненадежностью $P(S) \leqslant \varepsilon + c_3\varepsilon^2$, где $\varepsilon \in (0, d_3]$, c_3, d_3 — некоторые положительные константы.

При инверсных неисправностях на выходах элементов при наличии хороших функций в базисе все булевы функции, кроме $x_1, x_2, ..., x_n$, можно реализовать асимптотически оптимальными схемами с ненадежностью ε при $\varepsilon \to 0$.

Опишем хорошие функции, найденные в [3].

Пусть $G_1 = \{x_1^{\sigma_1}x_2^{\sigma_2} \vee x_1^{\sigma_1}x_3^{\sigma_3} \vee x_2^{\sigma_2}x_3^{\sigma_3} | \sigma_i \in \{0,1\},\ i \in \{1,2,3\}\}$, G_2 — множество функций, зависящих от переменных x_1, x_2, x_3, и конгруэнтных функциям $x_1^{\sigma_1}x_2^{\sigma_2} \oplus x_3^{\sigma_3}$, G_3 — множество функций, зависящих от переменных x_1, x_2, x_3, конгруэнтных функциям $x_1^{\sigma_1}x_2^{\bar{\sigma}_2} \vee x_2^{\sigma_2}x_3^{\sigma_3}$, где $\sigma_1, \sigma_2, \sigma_3 \in \{0,1\}$. Полагаем $G = G_1 \cup G_2 \cup G_3$.

В [3] доказано, что функции множества G являются хорошими, и получен следующий результат: в полном конечном базисе B_3, содержащем функции не более чем трех переменных, почти все булевы функции можно реализовать асимптотически оптимальными схемами с ненадежностью ε (при $\varepsilon \to 0$) тогда и только тогда, когда $G \cap B_3 \neq \emptyset$.

Обозначим через T_4 множество всех функций $f(x_1, x_2, x_3, x_4)$, из которых при отождествлении некоторых двух переменных (с последующим переименованием переменных) можно получить функцию множества G. В этой работе с помощью ПЭВМ подсчитано число функций из множества T_4, и оказалось, что $|T_4| = 46672$. Поскольку число всех булевых функций $f(x_1, x_2, x_3, x_4)$ равно $2^{2^4} = 65536$, то $|T_4|/2^{2^4} = 0,7121582$. Очевидно, что функции множества T_4 являются хорошими.

В [4] рассматривалась и решалась следующая задача: найти хорошие функции $m(x_1, x_2, ..., x_k)$ и описать их свойства. Опишем найденные в [4] хорошие функции $m(x_1, x_2, ..., x_k)$.

Пусть $\tilde{\alpha}, \tilde{\beta}$ — некоторые двоичные наборы длины k. Через $\rho(\tilde{\alpha}, \tilde{\beta})$ обозначим расстояние Хэмминга между ними, равное

$$\rho(\tilde{\alpha}, \tilde{\beta}) = \sum_{i=1}^{k} |\alpha_i - \beta_i|.$$

Пусть булева функция $m(x_1, x_2, ..., x_k)$, $k \geqslant 3$, обладает следующим свойством.

Существуют наборы $\tilde{\alpha}, \tilde{\beta}$ длины k такие, что $3 \leqslant \rho(\tilde{\alpha}, \tilde{\beta}) = \rho \leqslant k$; для любого набора $\tilde{y} = (y_1, y_2, ..., y_k)$ такого, что $\rho(\tilde{\alpha}, \tilde{y}) \leqslant 1$, верно $m(\tilde{y}) = 0$; для любого набора $\tilde{y}$ такого, что $\rho(\tilde{\beta}, \tilde{y}) \leqslant 1$, верно $m(\tilde{y}) = 1$.

Такие наборы $\tilde{\alpha}, \tilde{\beta}$ будем называть характеристическими для функции $m(x_1, x_2, ..., x_k)$.

Обозначим через $M_k(\rho)$ класс функций $m(x_1, x_2, ..., x_k)$ с названным свойством. Полагаем

$$\tilde{M}_k = \bigcup_{\rho=3}^{k} M_k(\rho).$$

В работе [5] с помощью ПЭВМ найдено число $|\tilde{M}_4| = 3152$, а также $|\tilde{M}_4|/2^{2^4} = 0,0480957$.

Очевидно, что функции множества $T_4 \bigcup \tilde{M}_4$ являются хорошими. В этой работе с помощью ПЭВМ вычислено их количество, оно равно

$$|T_4 \bigcup \tilde{M}_4| = 46980.$$

Тогда $|T_4 \bigcup \tilde{M}_4|/2^{2^4} = 0,7168579$.

Поскольку $|T_4 \bigcup \tilde{M}_4| = |T_4| + |\tilde{M}_4| - |T_4 \bigcap \tilde{M}_4|$, то $|T_4 \bigcap \tilde{M}_4| = 2824$. Следовательно, из большей части функций (но не из всех) множества $\tilde{M}_4$ при отождествлении некоторых двух переменных получаются функции множества G.

Таким образом, количество хороших функций $f(x_1, x_2, x_3, x_4)$ не меньше, чем 46980.

Описать все хорошие функции $f(x_1, x_2, x_3, x_4)$ (а в будущем и все хорошие функции $f(x_1, x_2, ..., x_n),\ n > 4$) и подсчитать их количество — цель дальнейших исследований авторов.

Список литературы

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

2. von Neuman J. Probabilistic logics and the synthesis of reliable organisms from unreliable components // Automata studies, edited by Shannon C., Mc. Carthy J. — Princeton University Press, 1956. (Русский перевод: Автоматы. — М.: ИЛ, 1956. С. 68—139.)

3. Алехина М. А., Васин А. В. О надежности схем в базисах, содержащих функции не более чем трех переменных // Ученые записки Казанского государственного университета. Физико-математические науки. В печати.

4. Алехина М. А., Аксенов С. И., Васин А. В. О функциях и схемах, применяемых для повышения надежности схем // Известия высших учебных

заведений. Поволжский регион. Физико-математические науки. — 2008. — № 3. — С. 30—38.

5. Алехина М. А., Заваровский К. Ю., Спиридонов Н. С. О числе функций, используемых для повышения надежности схем // Труды международного симпозиума «Надёжность и качество, 2008». — Пенза: Информ.-издат. центр ПГУ, 2008. — Том 1. — С. 363.

СИНТЕЗ ЛЕГКОТЕСТИРУЕМЫХ СХЕМ ДЛЯ СИСТЕМ ФУНКЦИЙ ИЗ НЕКОТОРЫХ КЛАССОВ

Ю. В. Бородина (Москва)

Будем рассматривать схемы из функциональных элементов [1,2].

Пусть S — некоторая схема из функциональных элементов, реализующая систему (упорядоченный набор) из m булевых функций $f_1(\tilde{x}), f_2(\tilde{x}), \ldots, f_m(\tilde{x})$, $\tilde{x} = (x_1, x_2, \ldots, x_n)$.

Определение. Функции, реализуемые на выходах схемы при наличии в схеме неисправных элементов, называются *функциями неисправности.*

Набор функций неисправности $(g_1(\tilde{x}), \ldots, g_m(\tilde{x}))$ будем называть *нетривиальным*, если хотя бы одна какая-нибудь функция $g_i(\tilde{x})$, $i \in \{1, \ldots, m\}$, отлична от соответствующей ей функции $f_i(\tilde{x})$, т.е. $g_i(\tilde{x}) \not\equiv f_i(\tilde{x})$.

Определение. Множество T входных наборов схемы S называется *полным проверяющим тестом для этой схемы*, если для любого нетривиального набора функций неисправности $(g_1(\tilde{x}), \ldots, g_m(\tilde{x}))$ в T найдется хотя бы один такой набор $\tilde{\sigma}$, что $(f_1(\tilde{\sigma}), \ldots, f_m(\tilde{\sigma})) \neq (g_1(\tilde{\sigma}), \ldots, g_m(\tilde{\sigma}))$ (здесь равенство булевых наборов покомпонентное, т.е. $(\alpha_1, \ldots, \alpha_m) = (\beta_1, \ldots, \beta_m)$ означает $\alpha_1 = \beta_1, \ldots, \alpha_m = \beta_m$). Число наборов, составляющих этот тест, называется *длиной теста* [3].

В качестве тривиального теста всегда можно взять тест, содержащий все 2^n наборов значений переменных булевой функции от n переменных.

В данной работе рассматривается задача построения легкотестируемых схем из функциональных элементов в базисе $\{\&, \vee, {}^-\}$ для систем булевых функций из различных классов. В качестве неисправностей предполагаются константные неисправности типа «1» на выходах элементов.

Пусть $\mathcal{F}_{n,m}$ — система из m булевых функций $f_1(\tilde{x}), f_2(\tilde{x}), \ldots, f_m(\tilde{x})$, где $\tilde{x} = (x_1, x_2, \ldots, x_n)$; у функций из $\mathcal{F}_{n,m}$ могут быть фиктивные переменные из числа $x_1, x_2, \ldots, x_n$.

Согласно теореме 2 из работы [4], каждую из функций $f_1, \ldots, f_m$ можно реализовать схемой, допускающей полный проверяющий тест длины не более 2. Таким образом, систему $\mathcal{F}_{n,m}$ можно реализовать схемой, допускающей полный проверяющий тест длины не более $2m$. Эту очевидную оценку можно уменьшить, используя детали доказательства указанной теоремы.

Теорема 1. *Любую систему $\mathcal{F}_{n,m}$ из m булевых функций, отличных от констант, можно реализовать схемой из функциональных элементов, допускающей полный проверяющий тест длины не более $1+q$, где $q \leqslant m$ — число функций из $\mathcal{F}_{n,m}$, сохраняющих единицу (m. е. равных 1 на наборе $(1, \ldots, 1)$).*

Значение $1+q$ в этой оценке длины теста в общем случае нельзя заменить ни на какое число, меньшее q.

Следствие 1. *Любую систему $\mathcal{F}_{n,m}$ из m монотонных булевых функций, отличных от констант, можно реализовать схемой из функциональных элементов, допускающей полный проверяющий тест длины 2.*

Следствие 2. *Пусть $\mathcal{F}_{n,m}$ — система из m булевых функций, отличных от констант, каждая из которых монотонна по каждой из l переменных $x_1, x_2, \ldots, x_l$ и антимонотонна по каждой из k переменных $x_{l+1}, \ldots, x_{l+k}$. Тогда систему $\mathcal{F}_{n,m}$ можно реализовать схемой из функциональных элементов, допускающей полный проверяющий тест, длина которого не превосходит $1+2^{n-k-l}$.*

Теорема 2. *Любую систему $\mathcal{F}_{n,m}$ из m монотонных булевых функций, отличных от констант, можно реализовать схемой из функциональных элементов в базисе $\{\&, \vee\}$, допускающей полный проверяющий тест длины, не превосходящей $\min\{m, n\}$.*

Теорема 3. *Пусть $\mathcal{F}_{n,m}$ — система из m булевых функций, отличных от констант, каждая из которых монотонна по каждой из l переменных $x_1, x_2, \ldots, x_l$, $l > 0$, и антимонотонна по каждой из $n-l$ переменных $x_{l+1}, \ldots, x_n$. Тогда систему $\mathcal{F}_{n,m}$ можно реализовать схемой из функциональных элементов, допускающей полный проверяющий тест, длина которого не превосходит $\min\{m, l\}$. При этом указанная схема содержит ровно $n-l$ инверторов, и на входы этих инверторов подаются значения переменных $x_{l+1}, \ldots, x_n$.*

Последние две теоремы получены в [5].

Из теоремы 3 и следствия 2 вытекает

Следствие 3. *Пусть $\mathcal{F}_{n,m}$ — система из m булевых функций, отличных от констант, каждая из которых монотонна по каждой из l*

переменных $x_1, x_2, \ldots, x_l$, $l > 0$, *и антимонотонна по каждой из* $n - l$ *переменных* $x_{l+1}, \ldots, x_n$. *Тогда систему* $\mathcal{F}_{n,m}$ *можно реализовать схемой из функциональных элементов, допускающей полный проверяющий тест, длина которого не превосходит* $\min\{2, l\}$.

Теорема 4. *Пусть* $\mathcal{F}_{n,m}$ — *система из* m *булевых функций, отличных от констант, каждая из которых монотонна по каждой из* l *переменных* $x_2, x_3, \ldots, x_{l+1}$, $l > 0$, *и антимонотонна по каждой из* $n - l - 1$ *переменных* $x_{l+2}, \ldots, x_n$. *Тогда систему* $\mathcal{F}_{n,m}$ *можно реализовать схемой из функциональных элементов, допускающей полный проверяющий тест, длина которого не превосходящей* $\min\{m, l\}$. *При этом указанная схема содержит ровно* $n - l$ *инверторов, и на входы этих инверторов подаются значения переменных* $x_1, x_{l+2}, \ldots, x_n$.

Из теоремы 4 и следствия 2 вытекает

Следствие 4. *Пусть* $\mathcal{F}_{n,m}$ — *система из* m *булевых функций, отличных от констант, каждая из которых монотонна по каждой из* l *переменных* $x_2, x_3, \ldots, x_{l+1}$, $l > 0$, *и антимонотонна по каждой из* $n - l$ *переменных* $x_{l+2}, \ldots, x_n$. *Тогда систему* $\mathcal{F}_{n,m}$ *можно реализовать схемой из функциональных элементов, допускающей полный проверяющий тест, длина которого не превосходит* $\min\{3, l\}$.

Работа выполнена при финансовой поддержке РФФИ (проект 08-01-00863), программы «Ведущие научные школы РФ» (проект НШ-4470.2008.1).

Список литературы

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

2. Яблонский С. В. Введение в дискретную математику. — М.: Высшая школа, 2002.

3. Редькин Н. П. О схемах, допускающих короткие тесты // Вестн. Моск. ун-та. Матем. Механ. — 1988. — N 2.—С. 17—21.

4. Бородина Ю. В. Синтез легкотестируемых схем в базисе $\{\&, \vee, {}^-\}$ при однотипных константных неисправностях на выходах элементов // Вестн. Моск. ун-та. Сер. 15, Вычислительная математика и кибернетика. — 2008. — 1. —С. 40—44.

5. Бородина Ю. В. Синтез легкотестируемых схем в базисе $\{\&, \vee, {}^-\}$ для систем функций из некоторых классов // Вестн. Моск. ун-та. Сер. 1, Математика. Механика. — 2006. — 4. — С. 68—72.

О 2-СМЕЖНОСТНЫХ МНОГОГРАННИКАХ

А. Г. Бродский (Ярославль)

1. Введение

Как известно, вычислительную сложность задач комбинаторной оптимизации отражают некоторые свойства графов многогранников, порождаемых этими задачами. В частности, заметную роль играет *плотность* (т. е. максимальное количество попарно смежных вершин) *графов многогранников*, которая служит нижней границей временной трудоемкости алгоритмов из широкого класса, включающего большинство известных комбинаторных методов. Оценки плотности полиэдральных графов большого количества комбинаторных задач показали, что эта характеристика экспоненциальна по размерности многогранников для труднорешаемых задач и полиномиальна для полиномиально разрешимых.

Более того, полиэдральные графы задач о максимальном разрезе, о покрытии матрицы, о клике (вершинное покрытие, независимое множество) являются полными. Напомним, что многогранники, у которых любые две вершины смежны, называются 2-*смежностными* [4,6,9].

Существование уже в $\mathbb{R}^4$ 2-смежностных многогранников со сколь угодно большим числом вершин установил К. Каратеодори [7] в 1907 году. В 1956 г. этот факт был «переоткрыт» в работе Д. Гейла [8], который предложил конструкцию, позволяющую, в частности, по некоторым системам n точек на сфере S_{m-1} в $\mathbb{R}^m$, где $n \geqslant m+2$, строить 2-смежностные многогранники в $\mathbb{R}^d$, где $d = n - m - 1$. Получаемые с помощью конструкции Гейла 2-смежностные многогранники имеют некоторый специальный вид (в предлагаемой нами терминологии это *строго* 2-*смежностные многогранники*). По сравнению с определениями 2-смежностного и строго 2-смежностного многогранников условия, накладываемые на исходную систему n точек на сфере S_{m-1}, являются более прозрачными и удобными с точки зрения построения таких систем. Например, оказывается интуитивно ясным, что вероятность их выполнения при выборе точек на S_{m-1} наугад велика. Это побудило Гейла к формулировке следующей гипотезы:

(G) вероятность получения (строго) 2-смежностного многогранника при случайном выборе n его вершин в $\mathbb{R}^d$ быстро возрастает с увеличением числа измерений d.

Представляют интерес и редуцированные варианты этой гипотезы [1–3]:

(G1) вероятность того, что при случайном выборе n точек $a_1, \ldots, a_n$ на сфере S_{d-1} выпуклый многогранник $\mathrm{conv}(a_1, \ldots, a_n)$ является 2-смежностным, быстро возрастает с увеличением d;

(G2) вероятность того, что при случайном выборе n точек $a_1, \ldots, a_n$ из множества вершин единичного куба $I_d = \{0,1\}^d \subseteq S_{d-1}$ выпуклый многогранник $\mathrm{conv}(a_1, \ldots, a_n)$ является 2-смежностным, быстро возрастает с увеличением d.

Обсуждению гипотезы (G2) посвящена часть 2. Что касается гипотезы (G), то возможным подходом к ее доказательству Гейл считает сведение к гипотезе

(G3) вероятность получения (строго) 2-смежностного многогранника в $\mathbb{R}^d$ с помощью конструкции Гейла (при случайном выборе n точек на сфере S_{m-1}) быстро возрастает с увеличением d.

В части 3 приведены результаты детального исследования конструкции Гейла, а в части 4 — формулировка теоремы, подтверждающей справедливость гипотезы (G3).

2. О гипотезе (G2)

Обозначим через $P_{n,d}$ вероятность того, что при случайном выборе без возвращения n вершин единичного d-мерного куба их выпуклая оболочка является 2-смежностным многогранником.

Теорема 1 (В. А. Бондаренко, А. Г. Бродский [2]). *Для любого натурального d, $d > 1$, и для любого натурального n, $n \leqslant 2^d$ выполняется неравенство*

$$P_{n,d} \geqslant 1 - \frac{n(n-1)(n-2)(n-3)}{8} \cdot \frac{2 \cdot 5^d - 11 \cdot 3^d + 14 \cdot 2^d - 5}{(2^d-1)(2^d-2)(2^d-3)}.$$

Иллюстрацией к теореме 1 служит такой числовой пример: случайно выбранные 25000 точек 100-мерного куба образуют 2-смежностный многогранник с вероятностью, превышающей 0,999.

Следствие 1. *Если $n(d) = O(2^{cd})$, где $c = \mathrm{const}$ удовлетворяет неравенствам*

$$0 < c < \frac{1}{4}(3 - \log_2 5), \tag{1}$$

то

$$P_{n(d),d} \longrightarrow 1$$

при $d \to \infty$.

Замечание 1. Неравенства (1) выполняются при $c = 1/6$. Поэтому

$$P_{n(d),d} \to 1$$

при $d \to \infty$ в предположении, что $n(d) = O(2^{d/6})$.

Замечание 2. Поскольку при достаточно больших d выполняется условие $2^{d/6} \gg d$, то установлена справедливость гипотезы (G2).

3. О конструкции Гейла

Систему $a = (a_1, \ldots, a_n)$ точек из $\mathbb{R}^m$ будем называть *положительно линейно зависимой*, если $\alpha_1 a_1 + \ldots + \alpha_n a_n = 0$ для некоторых $\alpha_1, \ldots, \alpha_n > 0$. Систему $a = (a_1, \ldots, a_n)$ точек из $\mathbb{R}^m$ будем называть *аффинно вполне m-мерной*, если при удалении из нее любой точки получается подсистема аффинного ранга m. Систему $a = (a_1, \ldots, a_n)$ точек из $\mathbb{R}^m$ будем называть *подходящей для построения строго 2-смежностных многогранников*, если каждое открытое полупространство в $\mathbb{R}^m$, ограниченное проходящей через точку 0 гиперплоскостью, содержит не менее трех точек системы a. Если a — система n точек из S_{m-1}, то это означает, что каждая открытая полусфера сферы S_{m-1} содержит не менее трех точек системы a. Систему $a = (a_1, \ldots, a_n)$ точек из $\mathbb{R}^m$ будем называть *строго 2-смежностной*, если у каждого ненулевого решения $(\lambda_1, \ldots, \lambda_n) \in \mathbb{R}^n$ системы уравнений

$$\begin{cases} \lambda_1 + \ldots + \lambda_n = 0, \\ \lambda_1 a_1 + \ldots + \lambda_n a_n = 0 \end{cases}$$

хотя бы три его компоненты положительны. Выпуклый многогранник P в $\mathbb{R}^m$ будем называть *строго 2-смежностным*, если система его вершин является строго 2-смежностной. Известно [8], что если $a = (a_1, \ldots, a_n)$ — строго 2-смежностная система точек из $\mathbb{R}^d$, то $\operatorname{conv} a$ является 2-смежностным многогранником с вершинами $a_1, \ldots, a_n$.

Теорема 2 (А.Г.Бродский [5]). *Пусть $m, n \in \mathbb{N}$ и $m < n - 1$. Существуют отношение эквивалентности θ на множестве $U_{m,n}$ положительно линейно зависимых и имеющих ранг m систем n точек из S_{m-1} и отношение эквивалентности ρ на множестве $V_{m,n}$ аффинно вполне $(n-m-1)$-мерных систем n точек из $\mathbb{R}^{n-m-1}$ такие, что конструкция Гейла определяет взаимно однозначное соответствие между фактормножествами $U_{m,n}/\theta$ и $V_{m,n}/\rho$. Оно индуцирует взаимно однозначное соответствие между классами θ-эквивалентности подходящих для построения строго 2-смежностных многогранников систем n точек из S_{m-1} и классами ρ-эквивалентности аффинно вполне $(n-m-1)$-мерных строго 2-смежностных систем n точек из $\mathbb{R}^{n-m-1}$.*

Отметим, что в применении конструкции Гейла к системе n точек на сфере S_{m-1} имеется некоторый произвол. При желании этот произвол

можно было бы устранить. Однако даже это не избавило бы конструкцию Гейла от одной ее существенной особенности: определяемое ею соответствие между системами n точек на сфере S_{m-1} и системами n точек в $\mathbb{R}^d$ (выпуклая оболочка которых дает интересующий нас многогранник) не является взаимно однозначным. В ходе доказательства теоремы 2 выясняется, что рассматриваемые свойства систем точек согласованы с отношениями эквивалентности θ и ρ. Если дополнить конструкцию Гейла простой матричной конструкцией, позволяющей по одному представителю класса эквивалентности ρ получать все остальные, то можно сказать следующее. При применении конструкции Гейла необходимым и достаточным условием получения класса эквивалентности, состоящего из строго 2-смежностных многогранников, является свойство исходной системы точек быть подходящей для построения строго 2-смежностных многогранников. Применяя конструкцию Гейла к подходящим для построения строго 2-смежностных многогранников системам n точек на сфере S_{m-1}, можно получить все строго 2-смежностные многогранники из $V_{m,n}$. Это дает повод для следующего уточнения формулировки гипотезы (G3):

(G3′) вероятность того, что случайно выбранные n точек на сфере S_{m-1} образуют систему, подходящую для построения строго 2-смежностных многогранников в $\mathbb{R}^d$, быстро возрастает с увеличением d.

4. О гипотезе (G3)

Пусть $m, d \in \mathbb{N}$ и $n = m + 1 + d$. Обозначим через $Q_{m,d}$ вероятность того, что случайно выбранные n точек на сфере S_{m-1} образуют систему, подходящую для построения строго 2-смежностных многогранников в $\mathbb{R}^d$.

Теорема 3 (А. Г. Бродский [5]). *Для любых $m, d \in \mathbb{N}$ и $n = m + 1 + d$ выполняется неравенство*

$$Q_{m,d} \geqslant 1 - \frac{f(n)}{a^n},$$

где

$$f(n) = k + \frac{k(2k-3)}{2(k-1)^2}n + \frac{k}{2(k-1)^2}n^2, \qquad a = \frac{k}{k-1}, \qquad k = 2^m.$$

Иллюстрацией к теореме 3 служит такой числовой пример: случайно выбранные 19 точек на сфере $S_0 = \{-1, 1\}$ образуют систему, подходящую для построения строго 2-смежностных многогранников в $\mathbb{R}^{17}$ с вероятностью, превышающей 0,999.

Следствие 2. *При фиксированном* m, $m \in \mathbb{N}$,

$$Q_{m,d} \longrightarrow 1$$

при $d \to \infty$.

Замечание 3. Таким образом, гипотеза (G3′) справедлива. Вопрос о сведении гипотезы (G) к гипотезе (G3′) остается открытым.

Список литературы

1. Бондаренко В. А. Полиэдральные графы и сложность в комбинаторной оптимизации. — Ярославль: ЯрГУ, 1995.

2. Бондаренко В. А., Бродский А. Г. О случайных 2-смежностных 0/1-многогранниках // Дискретная математика. — 2008. — Т. 20, №1. — С. 64–69.

3. Бондаренко В. А., Максименко А. Н. Геометрические конструкции и сложность в комбинаторной оптимизации. — М.: Изд-во ЛКИ, 2008.

4. Брёнстед А. Введение в теорию выпуклых многогранников. — М.: Мир, 1988.

5. Бродский А. Г. О 2-смежностных многогранниках и конструкции Гейла // Моделирование и анализ информационных систем (принята к опубликованию).

6. Емеличев В. А., Ковалев М. М., Кравцов М. К. Многогранники, графы, оптимизация (комбинаторная теория многогранников). — М.: Наука, 1981.

7. Caratheodory C. Ueber den Variabilitatsbereich der Koeffizienten von Potenzreihen, die gegebene Werte nicht annehmen // Math. Ann. — 1907. — V. 64. — P. 12–17.

8. Gale D. Neighboring vertices on a convex polyhedron // Linear inequalities and related systems / H. W. Kuhn, A. W. Tucker, Eds. — Princeton, New Jersey: Princeton University Press, 1956. (Русский перевод: Гейл Д. Соседние вершины на выпуклом многограннике // Линейные неравенства и смежные вопросы / Под ред. Г. У. Куна и А. У. Таккера. — М.: ИЛ, 1959. — С. 355–362.)

9. Ziegler G. M. Lectures on polytopes. — N.Y.: Springer, 1995.

ОБ АСИМПТОТИЧЕСКИ ОПТИМАЛЬНЫХ СХЕМАХ В БАЗИСЕ $\{x_1\&x_2,\ x_1\vee x_2,\ \overline{x}_1\}$ ПРИ ИНВЕРСНЫХ НЕИСПРАВНОСТЯХ НА ВЫХОДАХ ЭЛЕМЕНТОВ

А. В. Васин (Пенза)

Рассматривается реализация булевых функций схемами из ненадежных функциональных элементов (ФЭ) в базисе $\{x_1\&x_2, x_1 \vee x_2, \bar{x}_1\}$. Предполагается, что все ФЭ независимо друг от друга с вероятностью ε ($\varepsilon \in (0; 1/2)$) подвержены инверсным неисправностям на выходах. Считаем, что схема из ненадежных ФЭ реализует булеву функцию $f(\tilde{x})$ ($\tilde{x} = (x_1, x_2, ..., x_n)$), если при поступлении на входы схемы набора $\tilde{a}$ при отсутствии неисправностей на ее выходе появляется значение $f(\tilde{a})$. Число $P(S) = \max\limits_{\tilde{a}} P_{\bar{f}(\tilde{a})}(S, \tilde{a})$ назовем ненадежностью схемы S, где $P_{\bar{f}(\tilde{a})}(S, \tilde{a})$ — вероятность ошибки схемы S на входном наборе $\tilde{a}$. Схема A из ненадежных элементов, реализующая функцию f, называется асимптотически оптимальной по надежности, если $P(A) \sim P_\varepsilon(f)$ при $\varepsilon \to 0$, т. е. $\lim\limits_{\varepsilon\to 0} \frac{P_\varepsilon(f)}{P(A)} = 1$, где $P_\varepsilon(f) = \inf\limits_S P(S)$, инфимум берется по всем схемам S из ненадежных элементов, реализующим функцию $f(\tilde{x})$.

Введем функцию Шеннона $L_{p,\varepsilon}(n) = \max\limits_f \min\limits_S L(S)$, характеризующую сложность схем, реализующих функции от n переменных в базисе B, где минимум берется по всем схемам S из ненадежных элементов, реализующим функцию $f(x_1, x_2, ..., x_n)$ с ненадежностью $P(S) \leqslant p$, а максимум — по всем булевым функциям f от n переменных.

Пусть $\rho = \min\limits_{E_i}(v(E_i)/(n(E_i) - 1))$, где минимум берется по всем элементам E_i базиса B, для которых $n(E_i) > 1$, $n(E_i)$ — число существенных переменных функции e_i, реализуемой элементом E_i, а $\nu(E_i)$ — вес функционального элемента E_i, $i = 1, ..., m$.

О. Б. Лупанов [1] показал, что для схем, реализующих булевы функции от n переменных и состоящих только из надежных элементов (т. е. при $\varepsilon = 0$ и $p = 0$), выполняется соотношение $L_{0,0}(n) \sim \rho \cdot 2^n/n$.

С. И. Ортюков [2] для инверсных неисправностей на выходах элементов получил следующий результат: пусть $0 < \varepsilon < \varepsilon_0$, $p > q(\varepsilon)L_g$, где L_g — минимальное число надежных элементов, необходимое для реализации функции голосования $g(x_1, x_2, x_3) = x_1x_2 \vee x_1x_3 \vee x_2x_3$ в рассматриваемом базисе, $q(\varepsilon)$ — некоторая функция такая, что $q(\varepsilon) = \varepsilon + 3\varepsilon^2 + o(\varepsilon^2)$

при $\varepsilon \to 0$. Тогда существует такая функция $\rho(\varepsilon) \to \rho$ при $\varepsilon \to 0$, что $L_{p,\varepsilon}(n) \lesssim \rho(\varepsilon) \cdot 2^n/n$.

Д. Улиг [3] для инверсных неисправностей на выходах элементов с вероятностью ошибки ε доказал, что для любых, сколь угодно малых чисел c и b $(c, b > 0)$ существует число $\varepsilon\prime(\varepsilon\prime \in (0, 1/2))$ такое, что при любом ε $(\varepsilon \in (0, \varepsilon\prime))$, и любом p, удовлетворяющем условию $p \geqslant (1 + b)\varepsilon L_g$ (точнее $p \geqslant q(\varepsilon)L_g$), справедливо соотношение $L_{p,\varepsilon}(n) \lesssim (1 + c)\rho \cdot 2^n/n$.

Таким образом, в результатах С. И. Ортюкова и Д. Улига асимптотика функции Шеннона сохраняется с точностью до множителя, сколь угодно близкого к единице (при этом вероятность сбоя ε ограничена константой), т. е. найденные ими методы синтеза позволяют строить асимптотически оптимальные по сложности схемы, функционирующие с некоторым уровнем надежности.

Задача построения асимптотически оптимальных по надежности схем решена М. А. Алехиной [4] для однотипных константных неисправностей только на входах или только на выходах элементов и В. В. Чугуновой [5] для инверсных неисправностей на входах элементов в полных неприводимых базисах из двухвходовых элементов, а также в базисе $\{x\&y, x \vee y, \bar{x}\}$.

Чтобы сформулировать полученные в [4] и [5] результаты, введем необходимые определения.

Если неисправность такова, что элемент (реализующий в исправном состоянии приписанную ему булеву функцию) в неисправном состоянии, в которое переходит с вероятностью ε, где $\varepsilon \in (0; 1/2)$, реализует константу 0, то она называется неисправностью типа 0 на выходе элемента. Если же элемент в неисправном состоянии реализует константу 1, то такая неисправность называется неисправностью типа 1 на выходе элемента.

Если неисправность элемента такова, что поступающий на его вход нуль не искажается, а поступающая на его вход единица с вероятностью ε, где $\varepsilon \in (0; 1/2)$, может превратиться в нуль, то она называется неисправностью типа 0 на входе элемента. Если же неисправность элемента такова, что поступающая на его вход единица не искажается, а нуль с вероятностью ε может превратиться в единицу, то она называется неисправностью типа 1 на входе элемента.

Инверсные неисправности на входах элементов характеризуются тем, что поступающее на вход элемента значение a, $a \in \{0, 1\}$, с вероятностью ε может превратиться в значение $\bar{a}$.

Ненадежность $P(S)$ схемы S, а также асимптотически оптимальная схема определяются также как для инверсных неисправностей на выходах элементов.

М. А. Алехиной [4] доказано, что в базисе $\{x\&y, x \vee y, \bar{x}\}$ при однотип-

ных константных неисправностях на выходах элементов почти все булевы функции можно реализовать асимптотически оптимальными по надежности схемами, функционирующими с ненадежностью асимптотически равной ε при $\varepsilon \to 0$. Доказано [4] также, что в базисе $\{x\&y, x \vee y, \bar{x}\}$ при однотипных константных неисправностях на входах элементов почти все булевы функции можно реализовать асимптотически оптимальными по надежности схемами, функционирующими с ненадежностью, асимптотически равной ε^2 при $\varepsilon \to 0$. Сложность таких схем (здесь и далее сложность схемы — число функциональных элементов в ней) в обоих случаях по порядку равна сложности минимальных схем, построенных только из надежных элементов, причем мультипликативные константы равны 40 и 504 соответственно.

В. В. Чугуновой [5] доказано, что в базисе $\{x_1\&x_2, x_1 \vee x_2, \bar{x}_1\}$ при инверсных неисправностях на входах элементов почти все булевы функции можно реализовать асимптотически оптимальными по надежности схемами, функционирующими с ненадежностью асимптотически равной 2ε при $\varepsilon \to 0$. Сложность предлагаемых схем по порядку также равна сложности минимальных схем, построенных только из надежных элементов, причем мультипликативная константа равна 336.

Возникает вопрос, какой максимальной надежности можно добиться при использовании ненадежных элементов, подверженных инверсным неисправностям на выходах, в базисе $\{x_1\&x_2, x_1 \vee x_2, \bar{x}_1\}$. Ответ на него получен в работе [6], сопровождается полными подробными доказательствами. Приведем полученные результаты.

Теорема 1 [6]. *При $\varepsilon \in (0, 1/128]$ любую булеву функцию можно реализовать такой схемой S, что $P(S) \leqslant 3\varepsilon + 32\varepsilon^2$.*

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

Теорема 2 [6]. *Пусть $\varepsilon \in (0, 1/6]$, функция $f(\tilde{x}) \in K(n)$, и пусть S — любая схема, реализующая функцию f. Тогда $P(S) \geqslant 3\varepsilon - 6\varepsilon^2 + 4\varepsilon^3$.*

Из теоремы 2 следует, что при $\varepsilon \in (0, 1/128]$ 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 3ε при $\varepsilon \to 0$.

Далее получен ответ на вопрос о сложности асимптотически оптимальных схем. Пусть веса всех базисных элементов равны 1, тогда сложность схемы — число элементов в ней.

Из результатов М. А. Алехиной и С. И. Аксенова [7] следует теорема:

Теорема 3. *Для любого $b > 0$ существуют константы ε_1, $\varepsilon_1 \in (0, 1/2)$, и d такие, что при любых $\varepsilon \in (0, \varepsilon_1)$, любую булеву функцию $f(x_1, ..., x_n)$ можно реализовать схемой S, для которой*

$$P(S) \leqslant 3\varepsilon + d\varepsilon^2, \quad L(S) \lesssim 3(1+b) \cdot 2^n/n.$$

Для сравнения этого результата с результатами С. И. Ортюкова и Д. Улига нужно знать величину L_g — минимальное число надежных элементов, необходимое для реализации в базисе $\{x_1 \& x_2, x_1 \vee x_2, \bar{x}_1\}$ функции голосования $g(x_1, x_2, x_3) = x_1x_2 \vee x_1x_3 \vee x_2x_3$.

Известно, что $g(x_1, x_2, x_3) = x_1(x_2 \vee x_3) \vee x_2x_3$, т. е. $L_g \leqslant 4$. С другой стороны, $g \in K(n)$, а при доказательстве теоремы 2 все возможные схемы из трех элементов рассмотрены, и ни одна из них не реализует функцию g. Значит, L_g=4.

Таким образом, схемы из результатов С. И. Ортюкова и Д. Улига имеют асимптотически оптимальную сложность, но функционируют с ненадежностью не больше p, где $p > L_g\varepsilon$, $L_g = 4$. Нет оснований считать эти схемы асимптотически оптимальными по надежности.

Таким образом, при инверсных неисправностях на выходах элементов в базисе $\{x_1 \& x_2, x_1 \vee x_2, \bar{x}_1\}$ для почти всех булевых функций можно строить асимптотически оптимальные по надежности схемы, сложность которых превышает сложность минимальных схем, построенных только из надежных элементов, не более чем в 3 раза.

Список литературы

1. Лупанов О. Б. Об одном методе синтеза схем. // Изв. ВУЗов, Радиофизика, — 1958. — Т. 1, N 1. — С. 120—140.

2. Ортюков С. И. Об избыточности реализации булевых функций схемами из ненадежных элементов. // Труды семинара по дискретной математике и ее приложениям (Москва, 27 – 29 января 1987 г.). — М.: Изд-во Моск. ун-та, — 1989. — С. 166–168.

3. Uhlig D. Reliable networks from unreliable gates with almost minimal comlexity // Fundamentals of Computation Theory. Intern. conf. FCT'87 (Kazan, June 1987). Proc. Berlin: Springer-Verl., — 1987. — P. 462 –469. (Lecture Notes in Comput. Sci.; V. 278). (Русский перевод: Автоматы. — М.: ИЛ, — 1956. — С. 68—139).

4. Алехина М. А. Синтез асимптотически оптимальных по надежности схем из ненадежных элементов. // Пенза: Информационно–издательский центр ПГУ, — 2006.

5. Чугунова В. В. Синтез асимптотически оптимальных по надежности схем при инверсных неисправностях на входах элементов // Дисс. ... канд. физико-математических наук. — Пенза, — 2007.

6. Васин А. В. Об асимптотически оптимальных схемах в базисе $\{x_1 \& x_2, x_1 \vee x_2, \bar{x}_1\}$ при инверсных неисправностях на выходах элементов // Известия высших учебных заведений. Поволжский регион. Физико-математические науки. — №4(8), — 2008. — С. 2–16.

7. Алехина М. А., Аксенов С. И. О сложности надежных схем при инверсных неисправностях на выходах элементов // Материалы IX Международного семинара «Дискретная математика и ее приложения», посвященного 75-летию со дня рождения академика О. Б. Лупанова (Москва, 18–23 июня 2007г.). — М.: изд-во мех.-мат. фак-та МГУ, — 2007. — С. 56–59.

О ПРОГРАММЕ ПОСТРОЕНИЯ ПОЛИНОМОВ ЖЕГАЛКИНА

Ю. Н. Гавриш (Москва)

1. Введение

В настоящей работе представлена программа построения полиномов Жегалкина. Данная программа также позволяет распознавать выполнимость формул логики высказываний с построением моделей в случае их существования. В программе используется списочное представление формул и алгоритмы работы с ними, описанные в работе [5]. Такое представление формул является удобной реализацией схем из функциональных элементов, которые рассматривались в работе [2] для ускорения эквивалентных преобразований формул. Данная программа также используется как этап построения специальных полиномов Жегалкина, имеющих наилучшие показатели сложности-качества согласно работе [3].

Следуя работе [1], определим полином Жегалкина. Элементарная конъюнкция называется монотонной, если она не содержит отрицаний переменных. Константа 1 (т. е. элементарная конъюнкция нулевого ранга) считается по определению *монотонной* элементарной конъюнкцией. Выражение вида

$$K_1 \oplus K_2 \oplus \ldots \oplus K_s,$$

где K_i $(i = 1, 2, \ldots, s)$ — попарно различные монотонные элементарные конъюнкции над фиксированным множеством переменных, называется *полиномом Жегалкина* (или *полиномом по модулю* 2). Мы будем также рассматривать полином Жегалкина, соответствующий $s = 0$. Такой полином обозначим через 0 (независимо от множества переменных) и считаем по определению, что он равен константе 0.

2. Общее описание алгоритма

Алгоритм работы программы состоит из следующих этапов.

0) Разбор строки, задающей формулу, в обратную польскую нотацию (ОПН).

1) Преобразование строки, записанной в ОПН, в списочное представление формулы.

2) Переход к базису $\{\oplus, \wedge, 1\}$ с использованием эквивалентных преобразований.

3) Преобразование формулы к виду: сумма по $\bmod 2$ конъюнкций переменных и констант 1.

4) Составление списка конъюнктов и их упрощение.

5) Построение полинома Жегалкина из списка конъюнктов, встречающихся нечётное число раз.

В программе формула может быть сразу задана списком (а не строкой), и тогда шаги 0 и 1 пропускаются. Рассмотрим подробнее каждый из шагов алгоритма.

3. Алгоритм разбора строкового представления формулы

Алгоритм разбора строкового представления формулы базируется на алгоритме обратной польской записи, она же постфиксная нотация.

Чтобы дать индуктивное определение постфиксной нотации, обозначим для выражений в инфиксной нотации E, E_1, E_2, эквивалентные им выражения в постфиксной нотации E' , E'_1, E'_2, соответственно; а через o — произвольный бинарный оператор. Тогда переход к постфиксной нотации состоит из следующих преобразований.

1. Если E — переменная или константа, то E' есть E.

2. Если E — выражение вида $E_1 o E_2$, то E' есть $E'_1 E'_2 o$.

3. Если E — выражение вида (E_1), то E' есть E'_1.

Большим удобством постфиксной нотации является то, что запись становится бесскобочной, операнды стоят подряд перед оператором и разбор строки в последовательность действий становится достаточно простой задачей. Находим первый слева оператор, берём нужное число аргументов слева от него, пишем элемент списочного представления, заменяем вычитанный оператор и его операнды ссылкой на элемент списка, который содержит вычисление этого оператора. Продолжаем данный цикл до тех пор, пока в строке не останется одна-единственная ссылка — на результат всех действий. Подобный алгоритм, но для арифметических, а не логических операций, рассмотрен в работе [6].

Программа построена таким образом, что переменные и подформулы в списочном представлении хранятся только по одному разу. То есть по сути списочное представление имеет схемы из функциональных элементов, вообще говоря отличной от дерева. Однако предусмотрена опция, позволяющая строить древесное представление формулы.

4. Алгоритм преобразования в полином Жегалкина

Изначально формула представлена в базисе $\{\neg, \wedge, \vee, \oplus, \to, \not\to, \sim, |, \downarrow\}$. Нам необходимо получить представление этой формулы в базисе $\{\oplus, \wedge, 1\}$. Воспользуемся следующими преобразованиями:

$$\neg a = a \oplus 1$$

$$a \vee b = (a \wedge b) \oplus a \oplus b$$

$$a \leftharpoondown b = a \oplus b \oplus 1$$

$$a \to b = (a \wedge b) \oplus a \oplus 1$$

Инверсия импликации: $a \not\to b = (a \wedge b) \oplus a$

Стрелка Пирса: $a \downarrow b = \neg(a \vee b) = (a \wedge b) \oplus a \oplus b \oplus 1$

Штрих Шеффера: $a|b = \neg(a \wedge b) = (a \wedge b) \oplus 1$

Таким образом, мы получаем представление функции в базисе $\{\oplus, \wedge, 1\}$. Для реализации третьего этапа воспользуемся следующими преобразованиями:

$$(a \oplus b) \wedge c = (a \wedge c) \oplus (b \wedge c)$$

$$c \wedge (a \oplus b) = (a \wedge c) \oplus (b \wedge c)$$

При этом будем поступать так: если элемент формулы, который сейчас упрощаем, имеет только одну ссылку на себя во всей формуле, то модифицируем сам элемент, если же ссылок больше одной, то делаем копию элемента и преобразовываем уже копию элемента.

Достаточно очевидно,что данный процесс упрощения конечен и приводит к необходимому результату.

Полученная после этапа 3) формула является суммой по модулю 2 конъюнкций, которые могут повторяться, и внутри которых могут быть повторы переменных, а также в конъюнкцию могут входить константы 1. Поэтому на следующем этапе 4) преобразуем список длины n, используя следующую процедуру.

0) В начале применения процедуры $i = 0$.

1) Если i-й элемент списка есть $\oplus$ и имеет одним из своих аргументов подформулу вида $\wedge_{j=1}^{k} x_i$, то исключаем из этой подформулы все возможные повторы переменных и единиц. Полученную конъюнкцию проверяем на наличие в списке конъюнкций. Если она имеется, то увеличиваем счётчик наличия этой конъюнкции на 1, иначе вставляем конъюнкцию в массив конъюнктов, записав в счётчик наличия этой конъюнкции 1.

2) Переходим к элементу списка с номером $i + 1$.

Данная процедура реализует преобразования:

$$a \wedge a = a$$

$$a \wedge 1 = a$$

$$a \oplus a \oplus b = b$$

Для построения модели нам удобнее перейти к массиву конъюнктов, а не преобразовывать формулу, поэтому применена описанная процедура, а не прямое преобразование формулы.

5. Построение модели по полиному Жегалкина. Распознавание выполнимости формулы

Теперь у нас есть данные для построения полинома Жегалкина. Проходим по полученному на этапе 4) списку конъюнкций и удаляем из него все конъюнкции, встречающиеся чётное число раз. Из этого списка строим полином Жегалкина для исходной формулы.

Для построенного полинома Жегалкина возможны два случая: либо это константа 0, либо сумма по модулю 2 монотонных элементарных конъюнкций. В первом случае исходная формула невыполнима, во втором — выполнима.

Монотонные элементарные конъюнкции в полиноме Жегалкина образуют частично упорядоченное множество, которое имеет хотя бы один минимальный элемент — монотонную элементарную конъюнкцию. Значение каждой входящей в эту конъюнкцию переменной положим равным 1, а значение остальных — равным 0. Полученная интерпретация (набор значений переменных) является моделью для исходной формулы.

Список литературы

1. Гаврилов Г. П., Сапоженко А. А. Задачи и упражнения по дискретной математике. — М.: Наука. — 1977.

2. Ложкин С. А. Лекции по основам кибернетики: Учебное пособие. — М.: Издательский отдел Факультета ВМиК МГУ им. М.В.Ломоносова, 2004.

3. Чебурахин И. Ф. Синтез дискретных управляющих систем и математическое моделирование: теория, алгоритмы, программы. — М.: Издательство физико-математической литературы, 2004.

4. Яблонский С. В. Введение в дискретную математику. — М.: Наука. — 1986.

5. Хелемендик Р. В. Элементы математической логики и возможности ее приложений. Учебное пособие. М.: МАТИ, 2009. В печати.

6. Ахо А. В., Сети Р., Ульман Д. Компиляторы: принципы, технологии и инструменты, Вильямс, 2003 г.

О РАНГАХ И ЯДРАХ СОВЕРШЕННЫХ ДВОИЧНЫХ ТРАНЗИТИВНЫХ КОДОВ

Г. К. Гуськов, Ф. И. Соловьева (Новосибирск)

1. Введение

Транзитивные объекты играют важную роль как в теории кодирования, так и в комбинаторике, теории групп, теории графов. Следует отметить, что транзитивные коды, обладая богатыми группами автоморфизмов, по ряду своих свойств близки к линейным кодам. Для большинства оптимальных нелинейных кодов почти всегда можно найти транзитивные коды с такими же параметрами. Например, двоичный образ (под действием

отображения Грея) произвольного аддитивного кода является транзитивным кодом. Применение некоторых известных методов построения кодов, таких как метод Васильева, Плоткина и Моллара, к транзитивным кодам, удовлетворяющим некоторым дополнительным условиям, позволило получить бесконечные классы транзитивных кодов больших длин, в частности не менее $\lfloor k/2 \rfloor^2$ неэквивалентных совершенных транзитивных кодов длины $n = 2^k - 1, k > 4$ с кодовым расстоянием 3, см. [10, 11]. Для доказательства неэквивалентности построенных кодов использовались ранги и размерности ядер этих кодов. Легко видно, что применение общей проверки на четность позволяет получать из совершенных двоичных транзитивных кодов расширенные совершенные двоичные транзитивные коды. Ранее было известно $\lfloor (k+1)/2 \rfloor$ совершенных аддитивных кодов длины $n = 2^k - 1$, см. [1] (аналогично для расширенных совершенных аддитивных кодов, см. [3, 4]). С. А. Малюгиным в 2004 г., см. [5, 6] перечислены все совершенные двоичные транзитивные коды длины 15 из одношагового свитчингового класса кода Хэмминга длины 15. В работе [9] В. Н. Потаповым для каждого допустимого n было построено экспоненциальное число неэквивалентных расширенных совершенных транзитивных кодов длины $4n$ ранга на единицу больше ранга кода Хэмминга такой же длины.

Пусть E^n обозначает n-мерное метрическое пространство всех двоичных векторов длины n с метрикой Хэмминга. *Расстояние Хэмминга* $d(x, y)$ между векторами x и y из E^n равно количеству координат, в которых различаются эти векторы. *Двоичным кодом* называется произвольное подмножество C из E^n. *Совершенным двоичным кодом, исправляющим одиночные ошибки* (далее *совершенным кодом*), называется такое подмножество C из E^n, что любой вектор пространства E^n находится на расстоянии не больше 1 от некоторого единственного вектора из C. Известно, что такие коды существуют только при $n = 2^m - 1,\ m \geqslant 2$. Известно, что группа автоморфизмов пространства E^n исчерпывается всеми изометриями E^n, каждая такая изометрия определяется подстановкой π на множестве координат и добавлением произвольного вектора $v \in E^n$. Таким образом для группы автоморфизмов $Aut(E^n)$ пространства E^n справедливо $Aut(E^n) = \{(v, \pi) \mid v \in E^n, \pi \in S_n\}$, где S_n — симметрическая группа подстановок длины n. *Группой автоморфизмов* $Aut(C)$ кода C длины n назовём группу изометрий пространства E^n, переводящих код в себя. Код называется *транзитивным*, если его группа автоморфизмов действует транзитивно на всех его кодовых словах. Без ограничения общности далее будем рассматривать только коды, содержащие нулевое слово длины n. Для таких кодов удобно пользоваться следующим, эквивалентным приведенному выше, определением транзитивного кода: для

каждого кодового слова v из C найдется подстановка π из S_n такая, что $(v, \pi) \in \mathrm{Aut}(C)$, т.е. $v + \pi(C) = C$, где π может не принадлежать группе симметрий $\mathrm{Sym}(C) = \{\pi \in S_n \mid \pi(C) = C\}$ кода C.

2. Ранги и ядра

Для полноты изложения приведём определения двух конструкций транзитивных двоичных кодов, приведённых в [11], построенных с использованием кодов Васильева (см. [2]) и Моллара (см. [7]).

Пусть C — произвольный транзитивный код длины n с кодовым расстоянием d_1, причём d_1 — нечётно, а B — линейный код длины n с кодовым расстоянием d_2, такой, что для любого автоморфизма $(y, \pi) \in Aut(C)$ выполняется $\pi \in Sym(B)$. Тогда код Васильева

$$C^{2n+1} = \{(x, |x|, x + y) \mid x \in B,\ \ y \in C\}$$

длины $2n + 1$ является транзитивным.

Известно, что конструкция Моллара является обобщением конструкции Васильева. Пусть C^t и D^m — произвольные двоичные коды длин t и m соответственно, с кодовыми расстояниями не менее 3. Пусть

$$x = (x_{11}, x_{12}, \ldots, x_{1m}, x_{21}, \ldots, x_{2m}, \ldots, x_{t1}, \ldots, x_{tm}) \in E^{tm}.$$

Функции $p_1(x)$ и $p_2(x)$, определенные как

$$p_1(x) = \Big(\sum_{j=1}^{m} x_{1j}, \ldots, \sum_{j=1}^{m} x_{tj}\Big) \in E^t,\ \ p_2(x) = \Big(\sum_{i=1}^{t} x_{i1}, \ldots, \sum_{i=1}^{t} x_{im}\Big) \in E^m,$$

называются *обобщенными проверками на четность*.

Множество

$$C^n = \{(x, y + p_1(x), z + p_2(x)) \mid x \in E^{tm}, y \in C^t, z \in D^m\}$$

является двоичным *кодом Моллара* длины $n = tm + t + m$ с кодовым расстоянием 3 (см. [7]). В работе [11] было показано, что если коды C^t и D^m транзитивны, то код Моллара C^n транзитивен.

Далее потребуются следующие понятия и вспомогательные утверждения. *Ядро* кода C состоит из всех векторов $x \in C$ таких, что $x + C = C$. Размерности ядра и линейной оболочки обозначим через $k(C)$ и $r(C)$ соответственно, $r(C)$ называется *рангом* кода C. Величины $\delta(C) = r(C) - n + \log_2(n + 1)$ и $\varepsilon(C) = n - \log_2(n + 1) - k(C)$ называются *прибавкой ранга* и *дефектом ядра* кода C, соответственно.

Лемма 1 [11]. *Для прибавки ранга δ и дефекта ядра ε произвольного кода Моллара C^n длины n справедливо*

$$\delta = \delta_1 + \delta_2, \ \ \varepsilon = \varepsilon_1 + \varepsilon_2,$$

где δ_1 и δ_2 — прибавки рангов, а ε_1 и ε_2 — дефекты ядер кодов C^t и D^m, соответственно.

Следствие 1 [11]. *Для произвольного совершенного кода Васильева $C^n = \{(x, |x|, x + y) \mid x \in E^{(n-1)/2}, \ y \in C^{(n-1)/2}\}$ длины n и кода $C^{(n-1)/2}$ прибавки рангов и дефекты ядер совпадают.*

В работе [8] исследованы ядра и линейные оболочки совершенных аддитивных кодов. Эти результаты могут быть переформулированы следующим образом, используя прибавки ранга и дефекты ядер:

Лемма 2. *Существуют совершенные транзитивные коды длины $n = 2^k - 1$, для которых справедливо*
$(\delta, \varepsilon) \in \{(0,0), (1,2), (2,3)\}$ *при* $k = 4$,
$1 \leqslant \delta \leqslant \lfloor (k+1)/2 \rfloor$, $\varepsilon = 2^{k-1} - 2^{k-\delta-1} - \delta - 1$ *и* $\delta = 0$, $\varepsilon = 2^k - k - 1$ *при* $k > 4$.

В работах [5, 6] приведена классификация всех совершенных двоичных транзитивных кодов длины 15, полученных простыми свитчингами кода Хэмминга длины 15, в частности, был получен следующий результат

Лемма 3 [5, 6]. *Существуют совершенные двоичные транзитивные коды длины 15, для которых*

$$(\delta, \varepsilon) \in \{(1,2), (1,4), (2,3), (3,3), (3,6)\}.$$

Используя конструкцию Моллара и совершенные транзитивные коды с вышеприведёнными в леммах 2, 3 значениями пар (δ, ε), применяя лемму 1, получим

Лемма 4. *Для каждой пары (δ, ε) из множества*

$$\begin{aligned} A_0 = \{&(0,0), (1,2), (1,4), (2,3), (2,4), (2,6), (2,8), (3,3), (3,5), (3,6), \\ &(3,7), (4,5), (4,6), (4,7), (4,8), (4,10), (5,6), (5,9), (6,6), (6,9), (6,12)\} \end{aligned} \tag{1}$$

существует совершенный двоичный транзитивный код Моллара длины 255 с прибавкой ранга δ и дефектом ядра ε.

Используя лемму 4, а также конструкции Моллара и Васильева, можно получить общий вид для прибавок ранга и дефектов ядер известных

совершенных транзитивных кодов длины $n = 2^{k+8} - 1$, $k > 4$, а именно, справедливо следующее утверждение

Теорема. *Для любых* $n = 2^{k+8} - 1$, $k > 4$, *и любых пар* (δ, ε) *таких, что* $(\delta, \varepsilon) \in \{(\delta', 2^k - k + \varepsilon' - 1), (s + \delta', 2^{k-1} - 2^{k-s-1} - s + \varepsilon' - 1)\}$, *где* $(\delta', \varepsilon') \in A_0$ *и* $1 \leqslant s \leqslant \lfloor (k+1)/2 \rfloor$, *существует совершенный двоичный транзитивный код длины* n *с прибавкой ранга* δ *и дефектом ядра* ε.

Замечания. Следует отметить, что на сегодняшний день не найдена нетривиальная верхняя оценка числа неэквивалентных совершенных двоичных транзитивных кодов. Кроме того, согласно классификации совершенных транзитивных кодов длины 15, принадлежащих классу одношаговых свитчингов кода Хэмминга длины 15, данной С.А.Малюгиным в [5, 6], существуют неэквивалентные совершенные транзитивные коды длины 15, имеющие одинаковые пары (δ, ε) для прибавок рангов и дефектов ядер, т.е. подход, описанный выше, в данном случае неэффективен. Таким образом, представляется целесообразным разрабатывать новые критерии для различения неэквивалентности транзитивных (и необязательно транзитивных) кодов.

Список литературы

1. Borges J., Rifa J. K. A characterization of 1-perfect additive codes, IEEE Trans. Inform. Theory. 1999. V. 45. P. 1688–1697.

2. Васильев Ю. Л. О негрупповых плотно упакованных кодах, Проблемы кибернетики. М: Наука, 1962. Вып. 8. С. 337–339.

3. Кротов Д. С. Z_4-линейные совершенные коды, Дискрет. анализ и исслед. операций. 2000. Сер. 1. Т. 7. N. 4. С. 78–90.

4. Krotov D. S. Z_4-linear Hadamard and extended perfect codes, Proc. Int. Workshop «Coding and Cryptography WCC'2001». Paris, France. January, 8-12, 2001. P. 329–334.

5. Малюгин С.А. Транзитивные совершенные коды длины 15, Тр. конф. «Дискретный анализ и исследование операций». Новосибирск: Изд-во Инта математики, 2004. С. 96.

6. Малюгин С. А. О классах эквивалентности совершенных двоичных кодов длины 15. Препринт № 138. Новосибирск: Институт математики СО РАН, 2004. С. 34.

7. Mollard M. A generalized parity function and its use in the construction of perfect codes, SIAM J. Alg. Discrete Math, 1986. V. 7. N. 1. P. 113–115.

8. Phelps K. T., Rifá J. On Binary 1-Perfect Additive Codes: Some Structural Properties, IEEE Trans. Inform. Theory, 2002. V. 48. N. 9. P. 2587–2592.

9. Потапов В. Н. О нижней оценке числа транзитивных совершенных кодов, Дискрет. анализ и исслед. операций. Сер. 1. 2006. Т. 13. N. 4. С. 49–59.

10. Solov'eva F.I. On transitive codes, Тр. конф. «Дискретный анализ и исследование операций». Новосибирск: Изд-во Ин-та математики, 2004. С. 99.

11. Соловьева Ф. И. О построении транзитивных кодов, Проблемы передачи информации, 2005. Вып. 3. С. 23-31.

ОЦЕНКИ СЛОЖНОСТИ ПСЕВДОЛИНЕЙНЫХ ФУНКЦИЙ

Д. А. Дагаев (Москва)

В данной работе исследуется сложность реализации формулами функций трехзначной логики, принимающих значения из множества $\{0, 1\}$, ограничения которых на множестве наборов из нулей и единиц являются линейными булевыми функциями. О сложности реализации булевых функций формулами см. [1–3]. В [4,5] найдены верхние оценки функций Шеннона для некоторых классов трехзначной логики. Все необходимые определения можно найти в [1–3, 6–8].

Множество всех функций k-значной логики обозначим через P_k, $k \geqslant 2$, а множество всех функций из P_3, принимающих значения только из множества E_2, — через $P_{3,2}$. Пусть $F \subseteq P_{3,2}$. Обозначим через $F(n)$ множество всех функций из F, зависящих от переменных $x_1, ..., x_n$, $n \geqslant 1$. Обозначим через L множество всех линейных булевых функций. Будем обозначать конъюнкцию x_1 и x_2 и сумму по модулю два x_1 и x_2 через $x_1 \& x_2$ и $x_1 \oplus x_2$, соответственно.

Пусть $f(x_1, ..., x_n) \in P_{3,2}$. Проекцией функции $f(x_1, ..., x_n)$ называется такая булева функция $prf(x_1, ..., x_n)$, значение которой на произвольном наборе $\widetilde{\alpha} \in E_2^n$ определяется равенством $prf(\widetilde{\alpha}) = f(\widetilde{\alpha})$. 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 $f(x_1, ..., x_n) \in P_{3,2}$ называется псевдолинейной, если $f \in \mathcal{L}$. Очевидно, что $pr\mathcal{L} = L$.

Обозначим через $j_i(x)$ функцию из $P_{3,2}$, равную 1 в случае $x = i$ и 0 в остальных случаях, $i = 0, 1, 2$. Обозначим 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 следующие системы псевдолинейных функций. Положим

$$\mathfrak{A} = \{1, j_1(x) + j_1(y)\}, \quad \mathfrak{E} = \{1, j_0(x) + j_0(y)\},$$

$$\mathfrak{B} = \mathfrak{A} \cup \{j_1(x)j_1(y)j_2(z), j_0(x), j_1(x), j_2(x)\},$$

$$\mathfrak{D}_r = \mathfrak{A} \cup \{j_2(x_1)j_2(x_2)...j_2(x_r)\}.$$

В работе [7] описаны все замкнутые классы псевдолинейных функций: $\mathcal{L}$, L_2, $L_{2,\infty}$, $L_{2,r}(1 \leqslant r \leqslant \infty)$, $Z_{2,0} \cap \mathcal{L}$, $Z_{2,1} \cap \mathcal{L}$. В частности, показано, что $[\mathfrak{B}] = \mathcal{L}$, $[\mathfrak{D}_r] = L_{2,r} \cap \mathcal{L}$, $[\mathfrak{A}] = Z_{2,0} \cap \mathcal{L}$, $[\mathfrak{E}] = Z_{2,1} \cap \mathcal{L}$.

Ниже устанавливаются оценки функций Шеннона для следующих классов: $\mathcal{L}$, $L_{2,r} \cap \mathcal{L}$, $Z_{2,0} \cap \mathcal{L}$ и $Z_{2,1} \cap \mathcal{L}$.

Теорема 1. *Пусть* $Q = Z_{2,0} \cap \mathcal{L}$, $U = Z_{2,1} \cap \mathcal{L}$, $V_r = L_{2,r} \cap \mathcal{L}$, *где* $1 \leqslant r < \infty$. *Тогда имеют место следующие соотношения:*

$$L_{\mathfrak{A}}(Q(n)) = L_{\mathfrak{E}}(U(n)) = n + 1 \quad \textit{при всех } n \geqslant 2; \tag{1}$$

$$L_{\mathfrak{D}_r}(V_r(n)) = 1 + n + r(C_n^1 + C_n^2 + ... + C_n^r) \quad \textit{при всех } n \geqslant r \geqslant 1; \tag{2}$$

$$L_{\mathfrak{B}}(\mathcal{L}(n)) \sim \frac{3^n}{\log_2 n}. \tag{3}$$

Равенства, указанные в (1), очевидны.

Доказательство соотношения (2) опирается на утверждение о том, что для функции

$$f(x_1, ..., x_n) = 1 + j_1(x_1) + ... + j_1(x_n) + j_2(x_1) + ... + j_2(x_n) + ...$$

$$... + j_2(x_1)j_2(x_2) + ... + j_2(x_{n-1})j_2(x_n) + ... + j_2(x_1)...j_2(x_n)$$

выполняется равенство $L_{\mathfrak{D}_r}(f) = 1 + n + r(C_n^1 + C_n^2 + ... + C_n^r)$.

Нижняя оценка в (3) следует из мощностных соображений. Доказательство верхней оценки в соотношении (3) опирается на существование специального разбиения множества всех наборов длины n, получающегося на основе метода построения совершенных кодов Хэмминга [8]. Кроме того, используется метод, являющийся модификацией асимптотически оптимального метода синтеза формул над системой $\{\&, \vee, \bar{}\}$ [2].

Автор выражает благодарность 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. Лупанов О. Б. О сложности реализации функций алгебры логики формулами // Проблемы кибернетики. — 1960. — Вып. 3. — С. 61–80.

2. Лупанов О. Б. О синтезе некоторых классов управляющих систем // Проблемы кибернетики. — 1963. — Вып. 10. — С. 63–97.

3. Угольников А. Б. О глубине формул в неполных базисах // Математические вопросы кибернетики. — 1988. — Вып. 1. — С. 242–245.

4. Дагаев Д. А. Глубина и сложность реализации формулами функций из некоторых классов трехзначной логики // Тезисы докладов XV Международной конференции «Проблемы теоретической кибернетики» (Казань, 2—7 июня 2008 г.) Казань: Отечество, 2008. С. 24.

5. Дагаев Д. А. О глубине формул, реализующих функции из некоторых классов трехзначной логики // Материалы IX Междунар. семинара "Дискретная математика и ее приложения"(Москва, 18—23 июня 2007 г.) М.: Издательство механико-математического факультета МГУ, 2007. С. 84–87.

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

7. Lau D. Function Algebras on Finite Sets. Springer-Verlag, Berlin, 2006.

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

МЕТОД ТЕХНИЧЕСКОГО ДИАГНОСТИРОВАНИЯ НА ОСНОВЕ АНАЛИЗА ГЕОМЕТРИЧЕСКИХ ОБРАЗОВ ФУНКЦИОНИРОВАНИЯ

К. В. Елисеев (Саратов)

1. Введение

Методы решения задач технического диагностирования, управления и синтеза систем используют задание законов функционирования систем. В фазовых картинах систематизированы и представлены фазовые траектории, определяющие поведение систем. Большое разнообразие фазовых

картин в работах [1–2] сведено к единой форме — символьным и числовым графикам, точки которых размещаются на геометрических кривых линиях. Это позволяет не только сводить фазовые картины к удобной стандартной форме, но и использовать для постановок и решения задач мощные средства непрерывной математики: актуальную бесконечность, непрерывность, бесконечно малые величины, предельные переходы, суммирование бесконечных рядов и т.п. Существенной оказывается возможность доопределения фазовых картин, представленных частично заданными геометрическими образами, с использованием классических методов интерполяции.

Распространенным методом диагностики и распознавания сердечно-сосудистых заболеваний является электрокардиография. Электрокардиограмма представлена кривыми. Кривые характеризуется набором зубцов, по временным и амплитудным параметрам которых ставится диагноз. Процедуру нахождения характеристик электрокардиограмма выполняет врач-кардиолог на основе визуального анализа. Такая схема достаточно проста, но надежность её зависит от профессиональности и физического состояния врача, требует значительных затрат времени. Эта схема работает в течении долгого времени из-за отсутствия альтернативных подходов к решению задачи расшифровки ЭКГ. Предлагаемый в данной работе математический аппарат позволит расширить область изучения конкретных кривых, представляющих собой электрокардиограмму.

Изображение электрокардиограмм графиками на основе работы [2] позволяет представлять их ломаными линиями в декартовой системе координат. Такие ломаные линии допускают интерпретацию как геометрические образы законов функционирования автоматов (см. [2]). Частично изображённые электрокардиограммы после их представления частично заданными геометрическими образами могут быть дополнены с использованием классических методов интерполяции. В результате отдельные электрокардиограммы оказываются фазовыми траекториями поведения дискретных детерминированных автоматов, и такие автоматы являются моделями конкретных заболеваний в целом.

На основании этого для повышения эффективности методов анализа электрокардиограмм могут быть использованы методы распознавания автоматов средствами условных и безусловных экспериментов. Специальные источники (см., например, [3]) позволяют устанавливать соответствие между свойствами электрокардиограмм и свойствами дискретных детерминированных динамических систем в форме автоматов, в которых входными сигналами представлены действующие на организм пациента силы. В данной статье предлагается перевести электрокардиограмму в геометрические образы, провести интерполяцию частично заданные геометрические

образы, определяющих электрокардиограммы, определить эффективность методов интерполяции.

2. Метод перевода электрокардиограмм в геометрический образ

Имеем электрокардиограмму, снятую у пациента по 12 отведениям. Разбиваем её на отдельные отведения. Из каждого отведения выделяется геометрическая кривая и заносится в систему координат, у которой минимальное значение оси Y будет ноль. Для перевода в геометрический образ наносим (выбираем) точки на сетке таким образом, если вершина зубца находится не на пересечении сетки, то для геометрического образа вершину перемещаем в ближайшее незанятое пересечение сетки, и по этим точкам строится геометрический образ.

Выходные сигналы будут показывать величину конкретного зубца в электрокардиограмме, а входной сигнал один и тот же, то есть получаем геометрический образ законов функционирования инициального автомата (A, s). Аналогично переводим в геометрические образы другие отведения. В результате получаем 12 геометрических образов законов функционирования инициальных автоматов, описывающих работу конкретного сердца.

3. Вычислительный эксперимент

Преобразование фазовых картин в геометрические образы законов функционирования автоматов и взаимнооднозначное представление этих геометрических образов последовательностями вторых координат точек геометрических образов позволяют рассматривать любую последовательность элементов их конечного множества как закодированную фазовую картину. Одной из задач интерполяции является определение координат ключевых узлов поведения функции. Данное свойство интерполяции будет применено к определению ключевых узлов геометрического образа законов функционирования частично определенного автомата. После замены символьного определения автомата (табличного, матричного и т.д.) соответствующей числовой структурой в форме геометрического образа появляется возможность методами интерполяции преобразовывать частично заданные законы функционирования в полностью заданные законы. Сложности выбора метода интерполяции связаны с тем, что доопределение связей входных и выходных сигналов должны соответствовать интерпретации автомата как модели объекта из прикладной области.

В данной статье рассматривается интерполяция не полностью определённых фазовых картин по узлам интерполяции. С помощью вычислительных экспериментов для выбранных фазовых траекторий рассматриваются

эффективность интерполяции. Это позволяет использовать методы синтеза дискретных систем, предполагающих полностью определённые законы функционирования для случаев частично заданных законов. Проведён анализ применимости методов интерполяции законов функционирования дискретных детерминированных систем. Для этого использована числовая форма геометрических образов автоматов. Целью интерполяции является пополнение частично заданных законов функционирования автоматов, что позволяет при проектировании систем использовать полностью определённые законы функционирования систем. Для фундаментального подхода в замене символьных автоматных моделей числовыми структурами, для доопределении функций переходов и выходов автомата с помощью развитых методов интерполяции и экстраполяции, а так же для применения математических методов анализа и классификации в работах Твердохлебова В.А. [1-2] предложено и разработано представление законов функционирования автомата числовыми структурами в виде геометрических образов, т.е. в форме размещения автоматного отображения на символьных и числовых геометрических фигурах.

В проведённом вычислительном эксперименте анализировалась эффективность метода интерполяции (МНК) частично заданной (полученной) электрокардиограммы. Метод применялся к отрезку длиной 50 знаков. Пропущенными элементами последовательности являлись, в первом варианте рассмотрения, 10 элементов и, во втором варианте рассмотрения, 18 элементов. В результате пропуска элементов в последовательности получили частично определённые последовательности (в первом варианте) и частично определённый последовательностью геометрический образ законов функционирования автомата (во втором варианте). Элементы оси абсцисс при интерпретации последовательности как последовательности вторых координат вершин геометрического образа законов функционирования автомата, после выбора множества входных сигналов X автомата в зависимости от числа элементов в X, получают интерпретацию как последовательности входных сигналов. На основании этого интерполяция позволяет сопоставить последовательностям входных сигналов, имеющих по линейному порядку ω_1 номера последовательности. Следовательно, через числовую интерполяцию доопределены законы функционирования автомата как для числовой, так и для символьной форм задания законов функционирования автомата.

Вычислительный эксперимент показал, что повышение степени полинома со второй на пятую для анализируемой последовательности (для законов функционирования автомата, представленных последовательностью) не даёт существенных преимуществ, и метод не является эффективным

Список литературы

1. Твердохлебов В. А. Рекуррентно-автоматные характеристики динамических систем. // Материалы 9-ой Междунар. конф. «Интеллектуальные системы и компьютерные науки» — М.:Т.1. Ч.2.,2006. С.168-171.

2. Твердохлебов В. А. Методы интерполяции в техническом диагностировании. // Ж-л «Проблемы управления» — М.:№2 2007. С.28-34.

3. Хемптон Дж. Р. 150 клинических ситуаций: пер. с англ. — М.:Мед. лит., 2007. 320с.

КЛАССИФИКАЦИЯ ДИСКРЕТНЫХ ДЕТЕРМИНИРОВАННЫХ АВТОМАТОВ ПО СВОЙСТВАМ ГЕОМЕТРИЧЕСКИХ ОБРАЗОВ

А. С. Епифанов (Саратов)

1. Введение

Задание законов функционирования дискретных детерминированных динамических систем (автоматов), разработанное и изложенное в монографии [1], позволяет строить модели для систем большой размерности, интерпретировать математические структуры в виде геометрических кривых или произвольных последовательностей как задание автоматов. Для изучения связей свойств законов функционирования автоматов со свойствами новых, задающих автоматы, числовых непрерывных структур проведено исследование 8594 фундаментальных математических последовательностей из банка целочисленных последовательностей [4] (США).

Для каждой последовательности рассмотрены начальные отрезки длин до 80 элементов, по ним построены геометрические образы законов функционирования автоматов и автоматы минимизированы. При таком исследовании преобразования цифровых последовательностей в законы функционирования рассматривались различные значения мощности входного алфавита и анализировалась специфика влияния изменения мощности входного алфавита. Разработанный в [1] спектр динамических параметров использован для классификации и оценок сложности как последовательностей, так и законов функционирования. Основные результаты приведены в монографии [2].

2. Геометрические образы законов функционирования автоматов

Преобразование символьной формы автоматной модели в числовую структуру (геометрический образ законов функционирования автомата) включает линейное упорядочивание автоматного отображения

$$\rho_s = \bigcup_{p \in X^*} \{(p, \lambda(s,p))\}$$

для инициального автомата $A_s = (S, X, Y, \delta, \lambda, s)$, где S, X и Y — соответственно, множества состояний, входных и выходных сигналов, δ — функция переходов ($\delta : S \times X \to S$), λ — функция выходов ($\lambda : S \times X \to Y$). Автоматное отображение ρ_s взаимнооднозначно преобразуется в автоматное отображение вида $\rho'_s = \bigcup_{p \in X^*} \{(p, \lambda'(s,p))\}$, где $\lambda'(s,p)$ — последний знак последовательности $\lambda(s,p)$. Для преобразования множества пар ρ_s и ρ'_s в графики на множестве всех слов в алфавите X вводится линейный порядок ω_1 (см. [1]). Упорядоченные множества пар (ρ_s, ω_1) и (ρ'_s, ω_1) дополняются линейными порядками ω_0 на Y^* и ω_2 на Y. В результате получаем графики $(\rho_s, \omega_1, \omega_0)$ и $(\rho'_s, \omega_1, \omega_2)$. Построенные графики размещены в системе координат с осью абсцисс (X^*, ω_1) и осями ординат соответственно (Y^*, ω_0) и (Y, ω_2). Замена элементов множеств X^* и Y в графике $\gamma_s = (\rho'_s, \omega_1, \omega_2)$ их номерами по порядкам ω_1 и ω_2 позволяет преобразовать символьный график γ_s в числовой график в системе координат с осью абсцисс N^+ и осью ординат $\{1, 2, ..., l\}$, где $|Y| = l$. Из геометрического образа γ_s автомата A_s выделяется последовательность вторых координат точек геометрического образа, которая взаимнооднозначно соответствует полному геометрическому образу. В результате законы функционирования автомата (т. е., фазовая картина) и конкретные процессы функционирования автомата (т. е., фазовые траектории) оказываются взаимнооднозначно определёнными последовательностью вторых координат точек геометрического образа. Произвольная последовательность элементов из конечного множества может рассматриваться как последовательность вторых координат точек геометрического образа и, следовательно, как задание законов функционирования автомата. Это позволяет некоторые свойства законов функционирования автомата представлять свойствами последовательностей.

3. Автоматная интерпретация фундаментальных математических последовательностей

В работе [1] предложен новый тип автомата — $(H, m, d(H))$-автомат. Законы функционирования данного типа автомата задаются числовой последовательностью H, которая полагается последовательностью вторых коор-

динат точек геометрического образа. Рассматривается начальный отрезок длины $d(H)$ последовательности H. Величина m — мощность входного алфавита автомата,а количество выходных сигналов определяется спецификой начального отрезка последовательности H длины $d(H)$ (число различных значений элементов в начальном отрезке длины $d(H)$).

В статье содержатся результаты по построению и анализу КДА, законы функционирования которых определены начальными отрезками геометрических образов и выбором числа входных сигналов автомата. Для этого из банка последовательностей [4] извлечены 8594 последовательностей и каждая последовательность представлена набором начальных отрезков, имеющих длины 50, 60, 70 и 80 знаков. Полученное множество из 34376 последовательностей рассматривается как множество начальных отрезков последовательностей вторых координат точек геометрического образа законов функционирования автоматов. Соответствующие последовательности первых координат точек геометрического образа определялись вариантами выбора числа входных сигналов автомата и линейным порядком ω на множестве входных последовательностей. Рассматривались множества входных сигналов, содержащие 2, 5 и 10 элементов. Подробное описание метода синтеза автомата по произвольной последовательности содержится в монографии [1]. Рассматриваемому множеству из 34376 последовательностей, при трех различных значениях мощности входного алфавита и трех способах доопределения функции переходов сопоставляется класс автоматов, состоящий из 309384 элементов. Далее осуществляется минимизация автоматов из построенного класса и разбиение на подклассы автоматов по числу состояний в автомате после минимизации. Проведено более подробное исследование некоторых классов $(H, m, d(H))$-автоматов, где $H \in \{\pi, e, \chi_F, \chi_P\}$, $m \in \{2, 5, 10\}$, $d(H) \in \{50, 60, 70, 80, 90, 100\}$, χ_F — характеристическая последовательность для чисел Фибоначчи, χ_P — характеристическая последовательность распределения простых чисел в натуральном ряду.

Анализировались три способа доопределения функции переходов: циклическое доопределениие, доопределение в начальное состояние, доопределение с использованием генератора случайных чисел (состояние выбирается из множества возможных случайным образом). После минимизации определялись эквивалентные по числу состояний автоматы. В таблице в качестве примера приведены законы функционирования автомата, построенного по последовательности длины 50, определяющей приближение фундаментальной математической величины e. При построении приведенного в таблице автомата использовано циклическое доопределение функции переходов δ и $|X| = 10$.

δ	s_0	s_1	s_2	s_3	s_4
x_1	s_1	s_1	s_1	s_1	s_1
x_2	s_2	s_2	s_2	s_2	s_2
x_3	s_3	s_3	s_3	s_3	s_3
x_4	s_4	s_4	s_4	s_4	s_4
x_5	s_0	s_0	s_0	s_0	s_0
x_6	s_1	s_1	s_1	s_1	s_1
x_7	s_2	s_2	s_2	s_2	s_2
x_8	s_3	s_3	s_3	s_3	s_3
x_9	s_4	s_4	s_4	s_4	s_4
x_{10}	s_0	s_0	s_0	s_0	s_0

λ	s_0	s_1	s_2	s_3	s_4
x_1	y_2	y_4	y_2	y_6	y_7
x_2	y_7	y_5	y_8	y_2	y_0
x_3	y_1	y_9	y_7	y_4	y_9
x_4	y_8	y_4	y_4	y_9	y_3
x_5	y_2	y_5	y_7	y_7	y_6
x_6	y_8	y_2	y_1	y_7	y_9
x_7	y_1	y_3	y_3	y_5	y_9
x_8	y_8	y_5	y_5	y_7	y_9
x_9	y_2	y_3	y_2	y_2	y_5
x_{10}	y_8	y_6	y_6	y_4	y_9

Табличное задание законов функционирования автомата, построенного по последовательности, определяющей приближение числа e.

В результате анализа класса π-автоматов, т. е. класса автоматов построенных по последовательностям, задающим приближение фундаментальной математической величины π длины 50, 60, 70, 80, 90, 100 знаков, при рассмотрении входных алфавитов различной мощности ($|X| = 2, 5, 10$) отмечено, что при различных способах доопределения функции переходов меняется число состояний у автоматов после минимизации. Так при циклическом доопределении функции переходов отмечено, что у всех построенных π-автоматов число классов эквивалентности совпадает с числом состояний. Таким образом все члены класса π-автоматов (при циклическом доооопределении функции переходов) являются минимальными по числу состояний. При доопределении в начальное состояние из постренных восемнадцати π-автоматов у трех автоматов после минимизации число состояний уменьшилось: у (π,2,70)-автомата до 34 состояний, у (π,2,80)-автомата до 39 состояний, и у (π,2,90)-автомата — до 43 состояний.

4. Классификация дискретных детерминированных автоматов по свойствам геометрических образов

Базовой моделью дискретных детерминированных динамических систем являются конечные детерминированные автоматы. Сравнение по сложности таких автоматов может быть сделано на основе сравнения математических структур, представляющих специфику законов функционирования автомата. В качестве таких структур могут быть использованы геометрические образы законов функционирования автоматов. Сравнение по сложности законов функционирования автоматов производится на основе сравнения спектров последовательностей. На основании того, что на структуру характеристических последовательностей ограничения не накладываются,

и она может быть любой последовательностью элементов из конечного множества, метод сравнения моделей по сложности допускает интерпретацию на любых, в частности числовых, последовательностях. С содержательной точки зрения, спектрами определяется сложность последовательностей с учетом свойств различных вариантов рекуррентных определений последовательностей. В вариантах таких определений числовыми показателями являются порядки рекуррентных форм, определяющих отдельные отрезки последовательностей, и количества смен рекуррентных форм, используемых для определения отрезков последовательности. Уровни спектра построены иерархически по добавлению в спектр новых параметров. В связи с этим эквивалентность последовательностей представляется через t-эквивалентности, определяемые уровнем Ω_t, $0 \leqslant t \leqslant 3$. В результате построения и анализа спектров для 8594 последовательностей длины 80, извлеченных из банка OEIS, определены эквивалентные по сложности последовательности (и, соответственно, эквивалентные по сложности законы функционирования автоматов, представленные данными последовательностями). В один класс эквивалентных по сложности автоматов на третьем уровне Ω_3 спектра Ω попали автоматы, заданные последовательностями: π, $10 - \pi$, последовательностью Мадонны. С точки зрения спектра оказались эквивалентными автоматы, представленные последовательностью

$$\begin{aligned}\xi_1 = \langle & 0,1,1,2,2,2,2,3,3,3,3,3,3,3,3,4,4,4,4,4,4,4,4,4,4,4,4,4,4,4,5,\\ & 5,5,5,5,5,5,5,5,5,5,5,5,5,5,5,5,5,5,5,5,5,5,5,5,5,5,5,5,5,5,6,6,\\ & 6,6,6,6,6,6,6,6,6,6,6,6,6,6,6,6,6,6,6,6,6,6,6,6,6,6,6,6,6,6,6,6\rangle\end{aligned}$$

и последовательностью

$$\begin{aligned}\xi_2 = \langle & 1,0,0,1,1,1,1,0,0,0,0,0,0,0,0,1,1,1,1,1,1,1,1,1,1,1,1,1,\\ & 1,1,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,\\ & 0,0,0,0,1,1,1,1,1,1,1,1,1,1,1,1,1,1,1,1,1,1,1,1,1,1,1,1,1\rangle\,.\end{aligned}$$

Подробное описание исследования банка фундаментальных математических величин и геометрических кривых (спираль Фибоначчи, лемниската Бернулли, баллистическая кривая, эвольвента круга, логарифмическая спираль, спираль Архимеда, астроида, спираль Галилео, брахистохрона, кардиоида, кривая преследования, циссоида, кривая Гаусса и др.) представлено в работе [2].

5. Краткие выводы

В работе построены и проанализированы классы дискретных детерминированных автоматов, определенные на основе математических свойств

геометрических образов, задающих законы функционирования автоматов. Используемый геометрический подход позволяет исследовать свойства законов функционирования дискретных детерминированных динамических систем на основе анализа свойств геометрических кривых или последовательностей. Изложенные в статье результаты показывают возможность практического использования аппарата геометрических образов для задания и исследования свойств законов функционирования дискретных детерминированных динамических систем (автоматов). Определены эквивалентные по сложности геометрические кривые, т. е. эквивалентные по сложности законы функционирования автоматов.

Список литературы

1. Твердохлебов В. А. Геометрические образы законов функционирования автоматов. — Саратов: Изд-во Научная книга, 2008г. 183с.

2. Епифанов А. С. Анализ фазовых картин дискретных динамических систем. — Саратов: Изд-во Научная книга, 2008. 156 с.

3. Епифанов А. С. Анализ геометрических образов и свойств автоматов. — Восьмая международная конференция «Дискретные модели в теории управляющих систем»: Эл. сборник материалов конференции.: М. 2009. С. 66-70.

4. http://www.research.att.com/ njas/sequences/Seis.html

СИНТЕЗ НАДЕЖНЫХ НЕВЕТВЯЩИХСЯ ПРОГРАММ С УСЛОВНОЙ ОСТАНОВКОЙ

С. М. Зиновьева (Пенза)

Рассматривается реализация булевых функций неветвящимися программами с условной остановкой [1]. Предполагается, что все операторы остановки абсолютно надежны, работают без сбоев, а остальные (вычислительные) операторы — конъюнкторы, дизъюнкторы, инверторы – 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 $\bar{\varphi}$. Считаем, что программа Pr реализует функцию $f(x_1, x_2, ..., x_n)$, 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.

Чтобы сформулировать известные результаты для схем из функциональных элементов, которые отличаются от неветвящихся программ наличием оператора условной остановки, введем необходимые определения.

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 $f(x_1, x_2, ..., x_n)$. Схема A из ненадежных элементов, реализующая функцию f, называется асимптотически оптимальной по надежности, если $N(A) \sim N_\varepsilon(f)$ при $\varepsilon \to 0$, т. е.

$$\lim_{\varepsilon \to 0} \frac{N_\varepsilon(f)}{N(A)} = 1.$$

Теорема 1 [2]. *При $\varepsilon \in (0, 1/128]$ любую булеву функцию f можно реализовать такой схемой S, что $N(S) \leqslant 3\varepsilon + 32\varepsilon^2$.*

Обозначим $K(n)$ — множество булевых функций $f(x_1, x_2, ..., x_n)$, не представимых в виде $(x_i^a \& h(\tilde{x}))^b$ $(i \in \{1, 2, ..., n\},\ a \in \{0, 1\})$.

Теорема 2 [2]. *Пусть $\varepsilon \in (0, 1/6]$, а $f(x_1, x_2, ..., x_n) \in K(n)$. Тогда для ненадежности $N(S)$ любой схемы S, реализующей функцию f, имеет место $N(S) \geqslant 3\varepsilon - 6\varepsilon^2 + 4\varepsilon^3$.*

Из теорем 1 и 2 следует, что в базисе $\{x_1 \& x_2, x_1 \vee x_2, \bar{x}_1\}$ для почти всех функций асимптотически оптимальные по надежности схемы функционируют с ненадежностью, асимптотически равной 3ε при $\varepsilon \to 0$.

Для неветвящихся программ с условной остановкой верны лемма 1 и теорема 3.

Наборы	*Выход I*		*Выход II*	
	P_0^I	P_1^I	P_0^{II}	P_1^{II}
(000)	-	ε	$1 - 2\varepsilon + 3\varepsilon^3 - 2\varepsilon^4$	$\varepsilon - 3\varepsilon^3 + 2\varepsilon^4$
(001),(010)	-	ε	$1 - 3\varepsilon + 5\varepsilon^2 - 5\varepsilon^3 + 2\varepsilon^4$	$2\varepsilon - 5\varepsilon^2 + 5\varepsilon^3 - 2\varepsilon^4$
(100)	-	ε	$1 - 3\varepsilon + 5\varepsilon^2 - 5\varepsilon^3 + 2\varepsilon^4$	$2\varepsilon - 5\varepsilon^2 + 5\varepsilon^3 - 2\varepsilon^4$
(011)	-	$1 - \varepsilon$	$\varepsilon - 2\varepsilon^2 + 3\varepsilon^3 - 2\varepsilon^4$	$2\varepsilon^2 - 3\varepsilon^3 + 2\varepsilon^4$
(101), (110)	-	ε	$3\varepsilon - 8\varepsilon^2 + 7\varepsilon^3 - 2\varepsilon^4$	$1 - 4\varepsilon + 8\varepsilon^2 - 7\varepsilon^3 + 2\varepsilon^4$
(111)	-	$1 - \varepsilon$	$3\varepsilon^2 - 5\varepsilon^3 + 2\varepsilon^4$	$\varepsilon - 3\varepsilon^2 + 5\varepsilon^3 - 2\varepsilon^4$

Лемма 1. *При* $\varepsilon \in (0, 1/128]$ *программа* Pr_g (*рис.* 1) *реализует функцию голосования* $g(x_1, x_2, x_3) = x_1x_2 \vee x_2x_3 \vee x_1x_3$ *с ненадежностью* $N(Pr_g) \leqslant 3\varepsilon$, *а вероятности* $P_0^I, P_1^I, P_0^{II}, P_1^{II}$ *появления нуля и единицы соответственно на каждом из двух выходов I и II приведены в таблице.*

Доказательство. Запишем функцию голосования в виде $g(\widetilde{x}) = (x_2x_3 \vee x_1)(x_2 \vee x_3)$ и представим программу с оператором условной остановки как функциональную схему (рис. 1, 2).

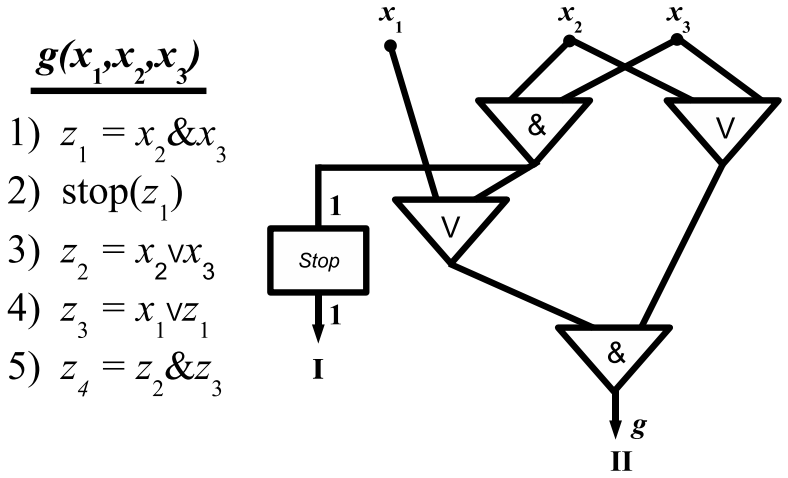

Рис. 1 Рис. 2

Поскольку оператор остановки абсолютно надежен и срабатывает, когда на его вход поступает единица (при этом на выходе оператора тоже единица), в графе P_0^I в таблице стоят прочерки, т. е. нуль не может появиться на выходе I программы с условной остановкой (рис. 1, 2).

Вычислим и оценим вероятности P_1^I, P_0^{II}, P_1^{II} программы Pr_g на всех входных наборах $\widetilde{a}$.

$\widetilde{\mathbf{a}} = (\mathbf{000})$:
$P_1^I(Pr_g, \widetilde{a}) = \varepsilon$;
$P_1^{II}(Pr_g, \widetilde{a}) = (1-\varepsilon)[(1-\varepsilon)\varepsilon + \varepsilon((1-\varepsilon)\varepsilon + \varepsilon(1-\varepsilon))] = \varepsilon - 3\varepsilon^3 + 2\varepsilon^4 < \varepsilon$;
$P_0^{II}(Pr_g, \widetilde{a}) = 1 - \varepsilon - \varepsilon + 3\varepsilon^3 - 2\varepsilon^4 = 1 - 2\varepsilon + 3\varepsilon^3 - 2\varepsilon^4$.

$\widetilde{\mathbf{a}} = (\mathbf{001}), \widetilde{\mathbf{a}} = (\mathbf{010})$:
$P_1^I(Pr_g, \widetilde{a}) = \varepsilon$;
$P_1^{II}(Pr_g, \widetilde{a}) = (1-\varepsilon)[(1-\varepsilon)\varepsilon + \varepsilon(\varepsilon\cdot\varepsilon + (1-\varepsilon)(1-\varepsilon)] = 2\varepsilon - 5\varepsilon^2 + 5\varepsilon^3 - 2\varepsilon^4 < 2\varepsilon$;
$P_0^{II}(Pr_g, \widetilde{a}) = 1 - \varepsilon - 2\varepsilon + 5\varepsilon^2 - 5\varepsilon^3 + 2\varepsilon^4 = 1 - 3\varepsilon + 5\varepsilon^2 - 5\varepsilon^3 + 2\varepsilon^4$.

$\widetilde{\mathbf{a}} = (\mathbf{100})$:
$P_1(Pr_g, \widetilde{a}) = \varepsilon$;
$P_1(Pr_g, \widetilde{a}) = (1-\varepsilon)[\varepsilon\cdot\varepsilon + (1-\varepsilon)(\varepsilon(1-\varepsilon) + (1-\varepsilon)\varepsilon)] = 2\varepsilon - 5\varepsilon^2 + 5\varepsilon^3 - 2\varepsilon^4 < 2\varepsilon$;
$P_0^{II}(Pr_g, \widetilde{a}) = 1 - \varepsilon - 2\varepsilon + 5\varepsilon^2 - 5\varepsilon^3 + 2\varepsilon^4 = 1 - 3\varepsilon + 5\varepsilon^2 - 5\varepsilon^3 + 2\varepsilon^4$.

Заметим, что на рассмотренных наборах (000), (001), (010), (100) ошибкой будет появление 1, и вероятность ошибки на выходе программы Pr_g будет равна $\max\{P_1^I, P_1^{II}\}$, который не превосходит 2ε.

$\widetilde{\mathbf{a}} = (\mathbf{011})$:
$P_0^I(Pr_g, \widetilde{a}) = 1 - \varepsilon$;
$P_0^{II}(Pr_g, \widetilde{a}) = (1-\varepsilon)\cdot 0 + \varepsilon[(1-\varepsilon)(1-\varepsilon) + \varepsilon(\varepsilon(1-\varepsilon) + (1-\varepsilon)\varepsilon)] =$
$= \varepsilon - 2\varepsilon^2 + 3\varepsilon^3 - 2\varepsilon^4 < \varepsilon$;
$P_1^{II}(Pr_g, \widetilde{a}) = 1 - 1 + \varepsilon - \varepsilon + 2\varepsilon^2 - 3\varepsilon^3 + 2\varepsilon^4 = 2\varepsilon^2 - 3\varepsilon^3 + 2\varepsilon^4$.

$\widetilde{\mathbf{a}} = (\mathbf{101}), \widetilde{\mathbf{a}} = (\mathbf{110})$:
$P_0^I(Pr_g, \widetilde{a}) = \varepsilon$;
$P_0^{II}(Pr_g, \widetilde{a}) = \varepsilon\cdot 0 + (1-\varepsilon)[\varepsilon\cdot(1-\varepsilon) + (1-\varepsilon)(\varepsilon(1-\varepsilon) + (1-\varepsilon)\varepsilon)] =$
$= 3\varepsilon - 8\varepsilon^2 + 7\varepsilon^3 - 2\varepsilon^4 < 3\varepsilon$;
$P_1^{II}(Pr_g, \widetilde{a}) = 1 - \varepsilon - 3\varepsilon + 8\varepsilon^2 - 7\varepsilon^3 + 2\varepsilon^4 = 1 - 4\varepsilon + 8\varepsilon^2 - 7\varepsilon^3 + 2\varepsilon^4$.

$\widetilde{\mathbf{a}} = (\mathbf{111})$:
$P_0^I(Pr_g, \widetilde{a}) = 1 - \varepsilon$;
$P_0^{II}(Pr_g, \widetilde{a}) = (1-\varepsilon)\cdot 0 + \varepsilon[\varepsilon(1-\varepsilon) + (1-\varepsilon)(\varepsilon(1-\varepsilon) + (1-\varepsilon)\varepsilon)] =$
$= 3\varepsilon^2 - 5\varepsilon^3 + 2\varepsilon^4 < 3\varepsilon^2$;
$P_1^{II}(Pr_g, \widetilde{a}) = 1 - \varepsilon - 3\varepsilon^2 + 5\varepsilon^3 - 2\varepsilon^4 = 1 - 4\varepsilon^2 + 5\varepsilon^3 - 2\varepsilon^4$.

Заметим, что на рассмотренных наборах (000), (001), (010), (100) ошибкой будет появление 0, и вероятность ошибки на выходе программы Pr_g будет равна P_0^{II}, которая не превосходит 3ε.

Лемма 1 доказана.

Теорема 3. *При $\varepsilon \in (0, 1/128]$ любую булеву функцию можно реализовать такой программой Pr_f, что $N(Pr_f) \leqslant \varepsilon + 41\varepsilon^2$.*

Доказательство. Пусть $f(x_1, x_2, ..., x_n)$ — произвольная булева функция. По теореме 1 ее можно реализовать неветвящейся программой (схемой) S с ненадежностью $N(S) \leqslant 3\varepsilon + 32\varepsilon^2$.

Используя эту схему S, построим для f неветвящуюся программу с условной остановкой Pr_f и представим ее схемой (рис. 3).

Вычислим и оценим вероятности ошибки для каждого из двух выходов I и II программы Pr_f (рис. 3).

Пусть набор $\widetilde{a}$ такой, что $f(\widetilde{a}) = 0$. Оценим вероятность ошибки на выходе I:

$$P_1(Pr_f, \widetilde{a}) = (1-p_1)^3\varepsilon + 3(1-p_1)^2 p_1\varepsilon + (1-p_1)p_1^2(1-\varepsilon) + \\ + 2(1-p_1)p_1^2\varepsilon + p_1^3(1-\varepsilon) \leqslant \varepsilon + 3\varepsilon p_1 + p_1^2,$$

где $p_1 \leqslant 3\varepsilon + 32\varepsilon^2$, тогда $P_1(Pr_f, \widetilde{a}) \leqslant \varepsilon + 21\varepsilon^2$.

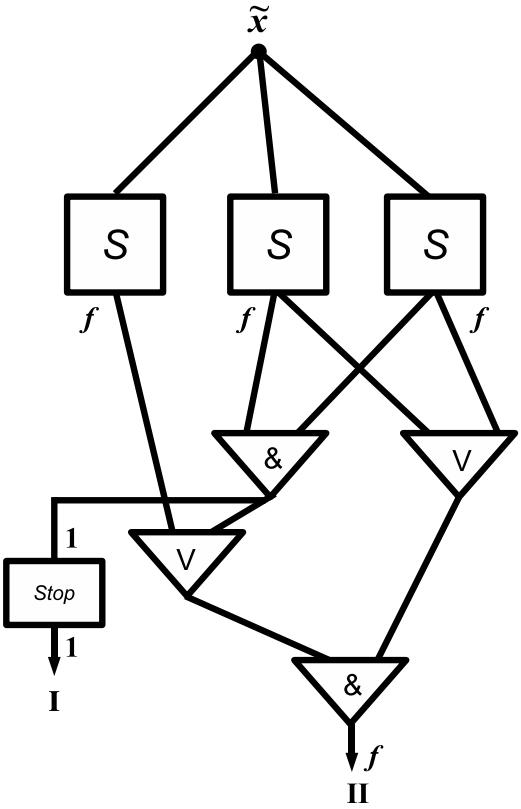

Рис. 3

Оценим вероятность ошибки на выходе II программы:

$$P_1(Pr_f, \widetilde{a}) = (1-p_1)^3[\varepsilon - 3\varepsilon^3 + 2\varepsilon^4] + 3(1-p_1)^2 p_1[2\varepsilon - 5\varepsilon^2 + 5\varepsilon^3 - 2\varepsilon^4] + \\ + (1-p_1)p_1^2[2\varepsilon^2 - 3\varepsilon^3 + 2\varepsilon^4] + 2(1-p_1)p_1^2[1 - 4\varepsilon + 8\varepsilon^2 - 7\varepsilon^3 + 2\varepsilon^4] + \\ + p_1^3[\varepsilon - 3\varepsilon^2 + 5\varepsilon^3 - 2\varepsilon^4] \leqslant \varepsilon + 6\varepsilon p_1 + 2p_1^2,$$

тогда $P_1(Pr_f, \widetilde{a}) \leqslant \varepsilon + 41\varepsilon^2$.

Пусть набор $\widetilde{a}$ такой, что $f(\widetilde{a}) = 1$. Ошибкой программы будет появление нуля на выходе II. На выходе I может появиться лишь 1, поэтому оценим вероятность ошибки на выходе II программы Pr_f:

$$P_0(Pr_f, \widetilde{a}) = p_0^3[1 - 2\varepsilon + 3\varepsilon^3 - 2\varepsilon^4] + 3p_0^2(1-p_0)[1 - 3\varepsilon + 5\varepsilon^2 - 5\varepsilon^3 + 2\varepsilon^4] + \\ + 2p_0(1-p_0)^2[3\varepsilon - 8\varepsilon^2 + 7\varepsilon^3 - 2\varepsilon^4] + p_0(1-p_0)^2[\varepsilon - 2\varepsilon^2 + 3\varepsilon^3 - 2\varepsilon^4] + \\ + (1-p_0)^3[3\varepsilon^2 - 5\varepsilon^3 + 2\varepsilon^4] \leqslant 3p_0^2 + 7\varepsilon p_0 + 3\varepsilon^2,$$

где $p_0 \leqslant 3\varepsilon + 32\varepsilon^2$. Тогда $P_0(Pr_f, \widetilde{a}) \leqslant 53\varepsilon^2$.

Выбирая из полученных для вероятности ошибок значений максимальное, видим, что ненадежность программы $N(Pr_f)$ удовлетворяет неравенству $N(Pr_f) \leqslant \varepsilon + 41\varepsilon^2$.

Теорема 3 доказана.

Проведенные исследования показывают, что при $\varepsilon \leqslant 1/128$ все булевы функции в базисе $\{x\&y, x \vee y, \overline{x}\}$ можно реализовать программами с условной остановкой, которые функционируют с ненадежностью не больше $\varepsilon + 41\varepsilon^2$, в то время, как ненадежность асимптотически оптимальных схем не превосходит $3\varepsilon + 32\varepsilon^2$.

Список литературы

1. Чашкин А. В. О среднем времени вычисления значений булевых функций. Дискретный анализ и исследование операций. Январь – март 1997. Том 4, N1. С. 60 – 78.

2. Васин А. В. Об асимптотически оптимальных схемах в базисе $\{x_1\&x_2, x_1 \vee x_2, \bar{x}_1\}$ при инверсных неисправностях на выходах элементов // Известия высших учебных заведений. Поволжский регион. Физико-математические науки. N 4. 2008. С. 3 – 17.

3. von Neuman J. Probabilistic logics and the synthesis of reliable organisms from unreliable components // Automata studies, edited by Shannon C., Mc. Carthy J. Princeton University Press, 1956. (Русский перевод: Автоматы. М.: ИЛ, 1956. С. 68 – 139.)

СИСТЕМЫ РАЗНОСТНЫХ УРАВНЕНИЙ НА КОНЕЧНОМЕРНОМ СТАНДАРТНОМ СИМПЛЕКСЕ

О. А. Кузенков, Д. В. Капитанов (Нижний Новгород)

Системы разностных уравнений широко используются при описании самых разных процессов и систем — электрических, механических, демографических, биологических, экономических и др. К разностным уравнениям приводят многочисленные экологические задачи и модели популяционной динамики, экономические задачи. В данной работе рассматриваются системы разностных уравнений, относительно вектор-функций принимающих значения из стандартного симплекса [2] — подмножества конечномерного евклидова пространства, состоящего из векторов с неотрицательными координатами, сумма которых равна единице. Системы, обладающие такими свойствами, называются системами на стандартном симплексе. Эти системы имеют широкое прикладное значение. Таким образом, рассматривается система разностных уравнений вида

$$\Delta x_i = F_i(x) \cdot \Delta t; \quad i = \overline{1, n}; \tag{1}$$

при выполнении следующих условий

$$\sum_{i=1}^{n} x_i = 1, \quad x_i \geqslant 0; \quad i = \overline{1,n}. \tag{2}$$

Здесь и далее под x понимается n-мерный вектор $x = (x_1, \ldots, x_n)$, а под Δx_i — конечные разности $\Delta x_i = x_i(t_0 + (k+1)\Delta t) - x_i(t_0 + k\Delta t)$, $i = \overline{1,n}$. Систему (1), решение которой в любой момент времени принадлежит стандартному симплексу (2), при любых начальных условиях, принадлежащих симплексу (2), будем называть системой на стандартном симплексе.

Справедливо следующее утверждение. Систему (1), в которой функции $F_i(x)$, $i = \overline{1,n}$, являются непрерывными по совокупности переменных, удовлетворяют условию Липшица по переменным x, имеют непрерывные частные производные $\dfrac{\partial F_i}{\partial x_i}$, в точках, где $x_i = 0$, и удовлетворяют условию квазиположительности в виде равенства

$$F_i(x_1, x_2, \ldots, x_{i-1}, 0, x_{i+1}, \ldots, x_n) = 0, \quad i = \overline{1,n}, \tag{3}$$

можно представить в виде:

$$\Delta x_i = G_i(x) x_i \Delta t, \tag{4}$$

где функции $G_i(x)$ являются непрерывными. Систему вида (4) принято называть системой с наследованием.

Лемма. *Если система* (1) *на стандартном симплексе* (2) *является системой с наследованием, то при* $x_i(t_0) = 0$ *справедливо тождество* $x_i(t_0 + k\Delta t) \equiv 0$ *для любого номера* $k > 0$.

Для сохранения целостности изложения материала приведем ниже ряд фактов, доказательство которых можно найти в [1]. Пусть для системы (1) справедливы условия сохранения положительности решения

$$\frac{F_i(x)}{x_i} \cdot \Delta t \geqslant -1; \quad x_i \neq 0,$$

тогда для того, чтобы решение системы (1) удовлетворяло тождеству

$$\sum_{i=1}^{n} x_i(t_k) \equiv 1,$$

при любых начальных условиях $x_i(t_0) = x_i^0$, $i = \overline{1,n}$, принадлежащих стандартному симплексу (2), необходимо и достаточно, чтобы равенство

$$\sum_{i=1}^{n} F_i(x) = 0$$

выполнялось в точках x, удовлетворяющих условию $\sum_{i=1}^{n} x_i = 1$.

Для любой системы (1) на стандартном симплексе (2) справедливо представление

$$\Delta x_i = \left(\Phi_i(x) - x_i \sum_{j=1}^{n} \Phi_j(x) \right) \Delta t, \quad i = \overline{1,n}, \tag{5}$$

где функции $\Phi_i(x)$ квазиположительные, положительно однородные, удовлетворяют условию Липшица, и, кроме того неотрицательные. Кроме того, для любой системы (1) на стандартном симплексе (2) справедливо второе представление

$$\Delta x_i = \frac{\left(\Phi_i(x) - x_i \cdot \sum_{j=1}^{n} \Phi_j(x) \right) \cdot \Delta t}{\sum_{j=1}^{n} \Phi_j(x) \cdot \Delta t + 1}, \quad i = \overline{1,n}, \tag{6}$$

где функции $\Phi_i(x)$ — положительно однородные.

Определение 1. Систему (1) на симплексе (2) будем называть [2] *системой отбора*, если найдётся такой номер i, что независимо от начальных условий, принадлежащих симплексу, с ненулевой i-й координатой, имеют место предельные соотношения

$$\lim_{n\to\infty} x_i(t_0 + n\Delta t) = 1; \quad \lim_{n\to\infty} x_j(t_0 + n\Delta t) = 0; \quad i \neq j. \tag{7}$$

Не уменьшая общности, можно считать, что $i = 1$, в противном случае достаточно переобозначить переменные.

Теорема 1. *Для того, чтобы система с наследованием* (1), (2) *являлась системой отбора необходимо и достаточно, чтобы вдоль любой фазовой траектории системы* (1), *соответствующей начальным условиям* $x_1(t_0) > 0;\ x_i(t_0) > 0$, *выполнялись равенства*

$$\sum_{n=1}^{\infty} \left(\ln\left(1 + \frac{F_1(x)}{x_1}\right) - \ln\left(1 + \frac{F_i(x)}{x_i}\right) \right) = +\infty. \tag{8}$$

Доказательство. *Необходимость.* Пусть в некоторой точке x на стандартном симплексе координаты $x_i(t_0)$ отличны от нуля для индексов $i \in E_1$ и равны нулю для индексов $i \in E_2$, $E_1 \bigcap E_2 = \varnothing$, $E_1 \bigcup E_2 = \{1, 2, \ldots, n\}$. Тогда, в силу леммы будет справедливо тождество $x_i(t_0 + n\Delta t) = 0,\ i \in E_2$. Для индексов $i \in E_1$ запишем систему (1) в виде

$$x_i(t_0 + (k+1)\Delta t) = x_i(t_0 + k\Delta t) + x_i(t_0 + k\Delta t)\frac{F_i(x)}{x_i(t_0 + k\Delta t)}\Delta t,\ i \in E_1.$$

В этом представлении, перебирая последовательно $k = 0, \ldots, n-1$, будем иметь систему

$$\begin{aligned} x_i(t_0 + \Delta t) &= x_i(t_0)\left(1 + \frac{F_i(x(t_0))\Delta t}{x_i(t_0)}\right), \\ x_i(t_0 + 2\Delta t) &= x_i(t_0 + \Delta t)\left(1 + \frac{F_i(x(t_0 + \Delta t))\Delta t}{x_i(t_0 + \Delta t)}\right) = \\ &= x_i(t_0)\left(1 + \frac{F_i(x(t_0))\Delta t}{x_i(t_0)}\right)\left(1 + \frac{F_i(x(t_0 + \Delta t))\Delta t}{x_i(t_0 + \Delta t)}\right). \end{aligned}$$

И так далее, продолжая подобные рассуждения в результате получим

$$x_i(t_0 + n\Delta t) = x_i(t_0)\prod_{k=0}^{n-1}\left(1 + \frac{F_i(x)\Delta t}{x_i(t_0 + k\Delta t)}\right),\ i \in E_1.$$

Рассмотрим отношение

$$\frac{x_1(t_0 + n\Delta t)}{x_i(t_0 + n\Delta t)} = \frac{x_1(t_0)}{x_i(t_0)} \cdot \frac{\prod\limits_{k=0}^{n-1}\left(1 + \dfrac{F_1(x)\Delta t}{x_1(t_0 + k\Delta t)}\right)}{\prod\limits_{k=0}^{n-1}\left(1 + \dfrac{F_i(x)\Delta t}{x_i(t_0 + k\Delta t)}\right)} =$$

$$= \frac{x_1(t_0)}{x_i(t_0)}\exp\left[\ln\prod_{k=0}^{n-1}\left(1 + \frac{F_1(x)}{x_1}\right) - \ln\prod_{k=0}^{n-1}\left(1 + \frac{F_i(x)}{x_i}\right)\right] =$$

$$= \frac{x_1(t_0)}{x_i(t_0)}\exp\left(\sum_{k=0}^{n-1}\left[\ln\left(1 + \frac{F_1(x)}{x_1}\right) - \ln\left(1 + \frac{F_i(x)}{x_i}\right)\right]\right),\ i \in E_1 \setminus \{1\}.$$

То есть, справедливо равенство

$$\frac{x_1}{x_i} = \frac{x_1(t_0)}{x_i(t_0)}\exp\left(\sum_{k=0}^{n-1}\left[\ln\left(1 + \frac{F_1(x)}{x_1}\right) - \ln\left(1 + \frac{F_i(x)}{x_i}\right)\right]\right),\ i \in E_1 \setminus \{1\}. \tag{9}$$

Так как по условию теоремы система (1), (2) является системой отбора, то $\lim\limits_{n\to\infty}\dfrac{x_1}{x_i}=+\infty$, а значит, учитывая равенство (9), при $x_i(t_0)>0$, ряд (8) тоже будет расходится к $+\infty$.

Достаточность. Если для индексов $i\in E_1/\{1\}$ выполнено равенство (8), то перейдя к пределу в равенстве (9), учитывая $x_i(t_0)>0$, получим

$$\lim_{n\to\infty}\frac{x_1}{x_i}(t_0+n\Delta t)=+\infty.$$

Это означает, что

$$\lim_{n\to\infty}x_i(t_0+n\Delta t)=0,\ i\in E_1\setminus\{1\}.$$

Но эти условия являются условиями отбора. Теорема доказана.

Определение 2. *Временным средним величины* $\xi(n)$ будем называть следующее выражение:

$$\lim_{n\to\infty}\frac{1}{n}\sum_{k=1}^{n}\xi(k)=\langle\xi(n)\rangle.$$

Теорема 2. *Для того, чтобы система с наследованием* (1) *являлась системой отбора, достаточно, чтобы вдоль любой фазовой траектории системы* (1) *с начальными условиями, удовлетворяющими соотношениям* $x_1(t_0)>0$, $x_i(t_0)>0$, *выполнялись неравенства*

$$\left\langle\ln\left(1+\frac{F_1(x)}{x_1}\right)\right\rangle>\left\langle\ln\left(1+\frac{F_i(x)}{x_i}\right)\right\rangle. \tag{10}$$

Доказательство. Пусть в некоторой точке x на стандартном симплексе координаты $x_i(t_0)$ отличны от нуля для индексов $i\in E_1$ и равны нулю для индексов $i\in E_2$, $E_1\bigcap E_2=\varnothing$, $E_1\bigcup E_2=\{1,2,\ldots,n\}$. Тогда, в силу леммы будет справедливо тождество $x_i(t_0+n\Delta t)=0,\ i\in E_2$. Из определения временного среднего следует, что для индексов $i\in E_1$ условие (10) можно представить в виде:

$$\lim_{n\to\infty}\frac{1}{n}\sum_{k=1}^{n}\ln\left(1+\frac{F_1(x)}{x_1}\right)-\lim_{n\to\infty}\frac{1}{n}\sum_{k=1}^{n}\ln\left(1+\frac{F_i(x)}{x_i}\right)=$$

$$=\lim_{n\to\infty}\frac{1}{n}\sum_{k=1}^{n}\left(\ln\left(1+\frac{F_1(x)}{x_1}\right)-\ln\left(1+\frac{F_i(x)}{x_i}\right)\right)>0.$$

$\exists N > 0: \quad \forall n > N:$

$$\lim_{n\to\infty} \sum_{k=1}^{n} \left(\ln\left(1 + \frac{F_1(x)}{x_1}\right) - \ln\left(1 + \frac{F_i(x)}{x_i}\right)\right) > \lim_{n\to\infty} (n \cdot N) = \infty.$$

Отсюда

$$\sum_{k=1}^{\infty} \left(\ln\left(1 + \frac{F_1(x)}{x_1}\right) - \ln\left(1 + \frac{F_i(x)}{x_i}\right)\right) = +\infty,$$

это есть ни что иное, как условие (8), что и доказывает теорему.

Список литературы

1. Кузенков О. А., Рябова Е. А. Математическое моделирование процессов отбора. Учебное пособие. — Н.Новгород: Изд-во ННГУ, 2007. 324 с.

2. Кузенков О. А., Капитанов Д. В. Системы разностных уравнений на единичном симплексе. // МКО Сб. научных трудов. Том 2. Под ред. Г. Ю. Ризниченко. — Ижевск: НИЦ «Регулярная и хаотическая динамика». 2006. С. 39–50

О МИНИМАЛЬНОМ РАССТОЯНИИ В КЛАССЕ БЕНТ-ФУНКЦИЙ

Н. А. Коломеец, А. В. Павлов (Новосибирск)

1. Общий вид бент-функций на минимальном расстоянии

Определение. $\mathfrak{B}_n$ — класс бент-функций от n переменных.

Определение. Пусть $f, g \in \mathcal{F}_n$. Тогда $D(f,g) = \{x \in E^n | f(x) \neq g(x)\}$.

Определение. Пусть $A \subseteq \mathcal{F}_n$. Тогда

$$d(A) = \min\{\mathrm{dist}(f,g) | f, g \in A, f \neq g\}.$$

Определение. Пусть $f \in \mathcal{F}_n, D \subseteq E^n$. Будем говорить, что f *аффинна на* D, если для некоторых $w_0 \in E^n, c \in E$ выполнятся

$$\forall x \in D \ f(x) = w_0 \cdot x \oplus c.$$

Теорема 1. $d(\mathfrak{B}_n) \geqslant 2^{n/2}$

Доказательство. Предположим, что существуют различные $f, g \in \mathfrak{B}_n$ такие, что $|D(f,g)| < 2^{n/2}$. Разность коэффициентов Уолша f и g будет равна

$$W_f(w) - W_g(w) = 2 \cdot \sum_{x \in D(f,g)} (-1)^{f(x) \oplus w \cdot x}.$$

Для упрощения равенства введем следующее обозначение:

$$a(w) = \sum_{x \in D(f,g)} (-1)^{f(x) \oplus w \cdot x},$$

где $f, g \in \mathfrak{B}_n$, следовательно,

$$a(w) \in \{0,\ 2^{n/2},\ -2^{n/2}\}.$$

Также, исходя из определения $a(w)$ и предполагаемой мощности $D(f,g)$,

$$\forall w \in E^n\ |a(w)| \leqslant |D(f,g)| < 2^{n/2}.$$

Получается, что $\forall w \in E^n\ a(w) = 0$, следовательно,

$$\forall w \in E^n\ W_f(w) = W_g(w).$$

Но Уолш-спектр однозначно определяет функцию, следовательно, $f = g$, следовательно, противоречие с тем, что f и g различны.

Лемма 1. *Пусть $f, g \in \mathfrak{B}_n$. Тогда $|D(f,g)| = |D(\tilde{f}, \tilde{g})|$, где $\tilde{f}$ такова, что $(-1)^{\tilde{f}(w)} \cdot 2^{n/2} = W_f(w)$.*

Доказательство. Воспользуемся формулой свертки

$$W_{f \oplus g}(0) = \frac{1}{2^n} \cdot \sum_{x \in E^n} W_f(x) \cdot W_g(x) = \sum_{x \in E^n} (-1)^{\tilde{f}(x) \oplus \tilde{g}(x)} = W_{\tilde{f} \oplus \tilde{g}}(0).$$

Лемма 2. *Пусть $D \subseteq E^n$, $|D| = 2^k$, $rk(D) = k+1$ и $\forall x, y \in D$ имеет место $x \oplus y \notin D$. Тогда D — линейное многообразие.*

Доказательство. Пусть $\overline{D}$ — линейная оболочка D, $U = \overline{D} \setminus D$, $x_0 \in D$. Покажем, что $U = x_0 \oplus D$.

Понятно, что $x_0 \oplus D \subseteq U$. Также

$$|U| = |\overline{D}| - |D| = 2^{k+1} - 2^k = 2^k = |D| = |x_0 + D|.$$

Следовательно, $U = x_0 \oplus D$, $D = x_0 \oplus U$. Из условия теоремы следует, что

$$\forall x, y \in D : x \oplus y \in U.$$

Теперь покажем, что U — подпространство E^n.

Во-первых, $0 \in U$, так как $0 = x_0 \oplus x_0 \in U$. Во-вторых, U замкнуто относительно $\oplus$: пусть $x, y \in U$, тогда $x = x_0 \oplus x'$, $y = x_0 \oplus y'$, где $x', y' \in D$. Следовательно:

$$x \oplus y = (x_0 \oplus x') \oplus (x_0 \oplus y') = x' \oplus y' \in U.$$

Таким образом, U — подпространство E^n, следовательно D — линейное многообразие.

Теорема 2. *Пусть $f, g \in \mathcal{F}_n$ таковы, что $f \in \mathfrak{B}_n$ и $|D(f,g)| = 2^{n/2}$. Тогда $g \in \mathfrak{B}_n \iff D(f,g) = x_0 + U, U \leqslant E^n$ и f аффинна на $D(f,g)$.*

Доказательство. ($\Longrightarrow$): Пусть $f, g \in \mathfrak{B}_n, |D(f,g)| = 2^{n/2}$. Покажем, что $D(f,g) = x_0 + U, U \leqslant E^n$ и f аффинна на $D(f,g)$. Из предыдущей теоремы

$$a(w) = \sum_{x \in D(f,g)} (-1)^{f(x) \oplus w \cdot x},$$

$$W_f(w) - W_g(w) = 2 \cdot a(w).$$

Так как $f, g \in \mathfrak{B}_n$, то

$$a(w) \in \{0, 2^{n/2}, -2^{n/2}\}.$$

Определим три множества:

$$W_{=0} = \{w \in E^n |\ a(w) = 0\},$$

$$W_{\neq 0} = \{w \in E^n |\ a(w) \neq 0\},$$

$$W_2 = \{w \in E^n |\ |a(w)| = 2^{n/2}\}.$$

По лемме 1

$$|W_{\neq 0}| = |D(f,g)|.$$

Понятно, что $|a(w)| = |D(f,g)| = 2^{n/2} \iff \forall x \in D(f,g)\ f(x) = w_0 \cdot x \oplus c$. То есть, аффинность мы доказали. Таким образом, $\forall w \in W_{\neq 0}$ является решением одной из следующих систем:

$$\{a \cdot w = a \cdot w_0, \forall a \in D(f,g);$$

$$\{a \cdot w = a \cdot w_0 \oplus 1, \forall a \in D(f,g).$$

Обозначив $w \oplus w_0$ за x, получаем равносильные системы уравнений:

$$\{a \cdot x = 0, \forall a \in D(f,g); \tag{1}$$

$$\{a \cdot x = 1, \forall a \in D(f,g). \tag{2}$$

Видно, что решения систем не пересекаются.
Теперь оценим $|W_{\neq 0}|$:

$$2^{n/2} = |W_{\neq 0}| \leqslant 2 \cdot 2^{n-rk(D(f,g))} = 2^{n-rk(D(f,g))+1}.$$

Отсюда

$$rk(D(f,g)) \leqslant n/2 + 1.$$

Но исходя из мощности множества $D(f,g)$ получаем

$$rk(D(f,g)) \in \{n/2, n/2+1\}.$$

Рассматриваем два случая.
Случай 1. $rk(D(f,g)) = n/2$. Очевидно, в этом случае $D(f,g)$ является подпространством.
Случай 2. $rk(D(f,g)) = n/2+1$. В этом случае обе системы должны иметь решение, поэтому у второй системы должно существовать частное решение

$$\exists t_0 \ (t_0 \cdot a = 1, \forall a \in D(f,g)).$$

Если существуют $x, y \in D(f,g) \mid x \oplus y \in D(f,g)$, то вторая система будет противоречива: с одной стороны

$$t_0 \cdot x = 1, t_0 \cdot y = 1 \Longrightarrow t_0 \cdot (x \oplus y) = 0,$$

с другой стороны

$$t_0 \cdot (x \oplus y) = 1.$$

Следовательно, выполняется условие леммы 2 для множества $D(f,g)$ (мощность и ранг множества, очевидно, удовлетворяют условию леммы). Таким образом, $D(f,g)$ — линейное многообразие. Необходимость доказана.

($\Longleftarrow$) Пусть $\forall x \in D(f,g)\ f(x) = w_0 \cdot x \oplus c$, а $D(f,g) = x_0 + U$. Сначала покажем, что $|W_2| = 2^{n/2} = |D(f,g)|$:
Случай 1. $D(f,g)$ — подпространство. Тогда вторая система решения не имеет, а первая имеет $2^{n-n/2}$, т. е. $|W_2| = 2^{n/2} = |D(f,g)|$.
Случай 2. $D(f,g)$ — линейное многообразие (но не подпространство). Покажем, что вторая система имеет частное решение. Для линейного многообразия вторую систему можно переписать следующим образом:

$$t \cdot x_0 = 1, \ \forall a \in U : t \cdot a = 0.$$

Рассмотрим $U^{\perp}$: если доказать, что в нем существует t_0, такой что выполнено $t_0 \cdot x_0 = 1$, то мы докажем существование частного решения. Предположим, что такого t_0 не существует. Тогда

$$\forall t \in U^{\perp}\ t \cdot x_0 = 0,$$

но это означает, что $x_0 \in (U^{\perp})^{\perp} = U$, т. е. получается, что $D(f,g)$ — подпространство. Однако, мы предполагали, что U не является подпространством, следовательно частное решение у второй системы существует. Тогда

$$|W_2| = 2 \cdot 2^{n-n/2-1} = 2^{n/2}.$$

Таким образом, мы доказали, что $|W_2| = |D(f,g)|$.
Отсюда следует, что

$$|W_2| = |W_{\neq 0}|,$$

$$a(w) \in \{0,\ 2^{n/2},\ -2^{n/2}\}.$$

Осталось доказать, что $g \in \mathfrak{B}_n$. Имеем

$$W_g(w) = W_f(w) - 2 \cdot a(w),$$

следовательно,

$$W_g(w) \in \{2^{n/2},\ -2^{n/2},\ 3 \cdot 2^{n/2},\ -3 \cdot 2^{n/2}\},$$

но если

$$\min_{w \in E^n} \{|W_g(w)|\} \geqslant 2^{n/2},$$

то из равенства Парсеваля следует

$$\forall w \in E^n\ |W_g(w)| = 2^{n/2}.$$

Получаем, что $g \in \mathfrak{B}_n$. Теорема доказана.

Следствие 1. $d(\mathfrak{B}_n) = 2^{n/2}$.

Доказательство. Достаточно применить теорему 2 к

$$f(x) = x_1 \cdot x_2 \oplus x_3 \cdot x_4 \oplus \cdots \oplus x_{n-1} \cdot x_n.$$

Определение. Пусть $f \in \mathfrak{B}_n$. Обозначим

$$L_{all}(f) = \{L \subseteq E^n \mid L = x_0 \oplus U,\ x_0 \in E^n,\ U \leqslant E^n,\ \dim(U) = n/2,\ f \text{ аффинна на } L\}.$$

Следствие 2. *Пусть* $f \in \mathfrak{B}_n$. *Тогда все* $g \in \mathfrak{B}_n$ *на минимальном расстоянии от* $f(x)$ *имеют следующий вид*

$$g(x) = f(x) \oplus I_L(x), \ L \in L_{all}(f).$$

2. $\mathbf{L_{all}}$ для бент-функций

Утверждение 1. *Любая функция из* $\mathfrak{B}_6$ *имеет непустое* L_{all}.

Утверждение 2. *Любая функция из* $\mathfrak{B}_8$ *степени не больше* 3 *имеет непустое* L_{all}.

Утверждение 3. *Любая функция из* $\mathfrak{B}_n$, *аффинно эквивалентная функции в виде линейного разветвления с индексом линейности* $n/2$, *имеет непустое* L_{all}. *В частности, любая функция из класса Мэйорана — МакФарланда имеет непустое* L_{all}.

Утверждение 4. *Существуют бент-функции от* 8 *переменных, имеющие непустое* L_{all}, *которые не являются аффинно эквивалентными функциям в виде линейного разветвления с показателем линейности* 4.

Список литературы

1. Токарева Н. Н. Бент-функции: результаты и приложения. Обзор работ. // Прикладная дискретная математика — 2009. Т. 3, вып. 1. С. 15–37.

2. McFarland R. L. A family of difference sets in non-cyclic groups // Combin. Theory. Ser. A. — 1973. Т. 15, вып. 1. С. 1–10.