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

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

МАТЕРИАЛЫ VIII МОЛОДЕЖНОЙ НАУЧНОЙ ШКОЛЫ ПО ДИСКРЕТНОЙ МАТЕМАТИКЕ И ЕЕ ПРИЛОЖЕНИЯМ

(Москва, 24–29 октября 2011 г.)

Часть I

Москва 2011

МАТЕРИАЛЫ
VIII МОЛОДЕЖНОЙ НАУЧНОЙ ШКОЛЫ
ПО ДИСКРЕТНОЙ МАТЕМАТИКЕ И ЕЕ ПРИЛОЖЕНИЯМ

(Москва, 24–29 октября 2011 г.)

Часть I

Москва 2011

М34
УДК 519.7

Издание осуществлено при поддержке Российского фонда фундаментальных исследований по проекту 11–01–06838

М34 Материалы VIII молодежной научной школы по дискретной математике и ее приложениям (Москва, 24–29 октября 2011 г.). Часть I. Под редакцией А. В. Чашкина. 2011. — 54 с.

Сборник содержит материалы VIII молодежной научной школы по дискретной математике и ее приложениям, проходившей в Москве с 24 по 29 октября 2011 г. при поддержке Российского фонда фундаментальных исследований (проект 11–01–06838). Для студентов, аспирантов и научных работников в области дискретной математики и математической кибернетики.

Научное издание

МАТЕРИАЛЫ
VIII МОЛОДЕЖНОЙ НАУЧНОЙ ШКОЛЫ
ПО ДИСКРЕТНОЙ МАТЕМАТИКЕ
И ЕЕ ПРИЛОЖЕНИЯМ
(Москва, 24–29 октября 2011 г.)

Под общей редакцией А. В. ЧАШКИНА

Ответственный за выпуск *О. С. Дудакова*

СОДЕРЖАНИЕ

О НАДЕЖНОСТИ СХЕМ ИЗ ЭЛЕМЕНТОВ $E_{x\downarrow y}$, ПОДВЕРЖЕННЫХ НЕИСПРАВНОСТЯМ ТИПА 0

М. А. Алехина, А. А. Щукина (Пенза)

Введение

Рассмотрим задачу реализации булевых функций асимптотически оптимальными по надежности схемами в базисе $\{x \downarrow y\}$ ($x \downarrow y = \bar{x}\&\bar{y}$) при неисправностях типа 0 на входах или выходах базисных элементов. Докажем, что почти все булевы функции можно реализовать асимптотически оптимальными по надежности схемами, которые функционируют с ненадежностью асимптотически равной ε при $\varepsilon \to 0$, где ε — вероятность появления неисправности типа 0 на входах или на выходе базисного элемента.

Будем считать, что схема из ненадежных функциональных элементов реализует функцию $f(x_1, \ldots, x_n)$ ($n \geq 1$), если при поступлении на входы схемы набора $\tilde{a} = (a_1, \ldots, a_n)$ при отсутствии неисправностей в схеме на ее выходе появляется значение $f(\tilde{a})$. Предполагается, что на входах или выходах всех элементов схемы происходят неисправности типа 0.

Неисправности типа 0 *на входах элементов* характеризуются тем, что поступающее на вход элемента значение a, $a \in \{0, 1\}$, с вероятностью ε может превратиться в нуль. *Неисправности типа* 0 *на выходах элементов* характеризуются тем, что в исправном состоянии функциональный элемент реализует приписанную ему булеву функцию $\{x \downarrow y\}$, а в неисправном — константу 0 (нуль).

Далее будем считать, что на входах или выходах всех элементов схемы независимо друг от друга и от входов и выходов других элементов с вероятностью ε ($\varepsilon \in (0; 1/2)$) происходят неисправности типа 0.

Вычислим вероятности появления ошибок на выходе базисного элемента $E_{x\downarrow y}$ (далее будем обозначать его через E, опуская индекс) при всех входных наборах этого элемента:

$P_0(E, (00)) = \varepsilon$, $P_1(E, (01)) = P_1(E, (10)) = \varepsilon(1 - \varepsilon)$, $P_1(E, (11)) = \varepsilon^2(1 - \varepsilon)$.

Пусть $P_{\overline{f(\tilde{a})}}(S, \tilde{a})$ — вероятность появления $\overline{f(\tilde{a})}$ на выходе схемы S, реализующей булеву функцию $f(\tilde{x})$, при входном наборе $\tilde{a}$. *Ненадежность* $P(S)$ схемы S определяется как максимальное из чисел $P_{\overline{f(\tilde{a})}}(S, \tilde{a})$ по всем входным наборам $\tilde{a}$ схемы S, т. е. $P(S) = \max\{P_{\overline{f(\tilde{a})}}(S, \tilde{a})\}$. *Надежность* схемы S равна $1 - P(S)$. Очевидно, ненадежность $P(E)$ базисного элемента E равна $P(E) = \varepsilon$, а надежность $1 - \varepsilon$.

Пусть $P_\varepsilon(f) = \inf P(S)$, где инфимум берется по всем схемам S из ненадежных элементов, реализующим функцию f.

Схема A из ненадежных элементов, реализующая функцию f, называется *асимптотически оптимальной по надежности*, если $P(A) \sim P_\varepsilon(f)$ при $\varepsilon \to 0$.

1. Верхняя оценка ненадежности схем

Пусть f — произвольная булева функция; S — схема, реализующая функцию f. Возьмем два экземпляра схемы S и соединим их выходы со входами базисного элемента. Построенную схему обозначим $\psi(S)$. Очевидно, что эта схема реализует функцию $\overline{f}$. Возьмем два экземпляра схемы $\psi(S)$ и соединим их выходы со входами еще одного базисного элемента. Полученную схему обозначим $\Psi(S)$. Очевидно, что схема $\Psi(S)$ реализует исходную функцию f.

Теорема 1 [1]. *Пусть f — произвольная булева функция, S — схема, реализующая f с ненадежностью $P(S)$. Тогда схема $\Psi(S)$ реализует функцию f с ненадежностью*

$$P(\Psi(S)) \le \max\{2\alpha+\tau+2(\beta+\delta)P(S)+2P^2(S), \alpha+(\beta+\delta)(\tau+2P(S))+(\tau+2P(S))^2\},$$

где $\alpha = P_1(E,(11)) = \varepsilon^2(1-\varepsilon), \beta = P_1(E,(10)), \delta = P_1(E,(01)), \tau = P_0(E,(00))$.

Из теоремы 1 следует теорема 2, если вместо α, β, δ, τ подставить вычисленные выше вероятности ошибок на выходе базисного элемента.

Теорема 2. *Пусть f — произвольная булева функция, S — схема, реализующая f с ненадежностью $P(S)$. Тогда схема $\Psi(S)$ реализует функцию f с ненадежностью*

$$P(\Psi(S)) \le \max\{\varepsilon + 2\varepsilon^2 + 4\varepsilon P(S) + 2P^2(S), 4\varepsilon^2 + 8\varepsilon P(S) + 4P^2(S)\}.$$

Теорема 3 [1]. *Любую булеву функцию f можно реализовать такой схемой A, что при всех $\mu \in (0, 1/160]$ (μ — любая верхняя оценка ненадежности схемы, реализующей функцию $\{x \downarrow y\}$) верно неравенство $P(A) \le 4\mu$.*

Из теоремы 3 следует теорема 4, для доказательства которой следует подставить ε (ненадежность базисного элемента) вместо μ.

Теорема 4. *Любую булеву функцию f можно реализовать такой схемой A, что при всех $\varepsilon \in (0, 1/160]$ верно неравенство $P(A) \le 4\varepsilon$.*

Из теорем 2 и 4 следует теорема 5.

Теорема 5. *Любую булеву функцию f можно реализовать такой схемой B, что при всех $\varepsilon \in (0, 1/160]$ верно неравенство $P(B) \le \varepsilon + 50\varepsilon^2$.*

Доказательство. Пусть f — произвольная булева функция. По теореме 4 функцию f можно реализовать схемой A с ненадежностью $P(A) \le 4\varepsilon$. По схеме A построим схему $\Psi(A)$ и оценим ее ненадежность, используя теорему 2. Получим неравенство $P(\Psi(A)) \le \max\{\varepsilon+50\varepsilon^2, 100\varepsilon^2\}$ при $\varepsilon \in (0, 1/160]$. Схема $\Psi(A) = B$ — искомая.

Теорема 5 доказана.

2. Нижняя оценка ненадежности схем

Теорема 6 [1]. *Пусть f — произвольная булева функция, отличная от константы, S — любая схема, ее реализующая и содержащая хотя бы один функциональный элемент. Пусть подсхема C схемы S содержит выход схемы S и реализует булеву функцию g с ненадежностью $P(C) \leq 1/2$. Обозначим через $p_{11}, \ldots, p_{1k}$ всевозможные различные вероятности ошибок на выходе схемы C при нулевых входных наборах $\tilde{b}$, т. е. $g(\tilde{b}) = 0$. Аналогично, пусть $p_{01}, \ldots, p_{0m}$ — всевозможные различные вероятности ошибок на выходе схемы C при единичных входных наборах $\tilde{b}$, т. е. $g(\tilde{b}) = 1$. Полагаем $p^1 = \min\{p_{11}, \ldots, p_{1k}\}$, $p^0 = \min\{p_{01}, \ldots, p_{0m}\}$. Тогда $P(S) \geq p^i$, $i = 0, 1$.*

Очевидно, что функции $x_1, \ldots, x_n$ $(n \geq 1)$ можно реализовать абсолютно надежно (без использования функциональных элементов).

Теорема 7. *Пусть $f(x_1, \ldots, x_n)$ — произвольная булева функция, отличная от функций $x_1, \ldots, x_n$ $(n \geq 1)$ и константы 0, и пусть S — любая схема, реализующая $f(x_1, \ldots, x_n)$. Тогда при всех $\varepsilon \in (0, 1/2)$ верно неравенство $P(S) \geq \varepsilon$.*

Для доказательства теоремы 7 достаточно выделить выходной элемент схемы и воспользоваться теоремой 6, поскольку $p^0 = \varepsilon$.

Из теоремы 7 следует, что все функции, кроме, функций $x_1, \ldots, x_n$ $(n \geq 1)$ и, быть может, константы 0, в рассматриваемом базисе нельзя реализовать схемами, ненадежность которых меньше ε. Поэтому любая схема, удовлетворяющая условиям теоремы 5 и реализующая булеву функцию $f(x_1, \ldots, x_n)$, отличную от функций $x_1, \ldots, x_n$ $(n \geq 1)$ и, быть может, константы 0, функционирует с ненадежностью, асимптотически равной ε при $\varepsilon \to 0$, и является асимптотически оптимальной по надежности. Таким образом, все почти все булевы функции можно реализовать асимптотически оптимальными по надежности схемами, ненадежность которых асимптотически равна ε при $\varepsilon \to 0$.

Работа выполнена при финансовой поддержке РФФИ, номер проекта 11-01-00212а.

Список литературы

1. Алехина М. А. Синтез асимптотически оптимальных по надежности схем из ненадежных элементов (монография). — Пенза: Информационно-издательский центр ПГУ, 2006. — 156 с.

НЕТРИВИАЛЬНАЯ ВЕРХНЯЯ ОЦЕНКА СЛОЖНОСТИ ВОЗВЕДЕНИЯ В СТЕПЕНЬ С ИСПОЛЬЗОВАНИЕМ 4 ЯЧЕЕК ПАМЯТИ

К. С. Балакин (Москва)

Рассматривается классическая задача о сложности возведения в степень — нахождении минимального числа операций умножения, достаточного для возведения некоторого числа x в заданную степень n. Обычно эту задачу формулируют на языке аддитивных цепочек [1]: найти минимальную длину $l(n)$ аддитивной цепочки для числа n. Очевидно, что $l(n) \geq \log n$ (здесь и далее под обозначением $\log n$ понимается $\log_2 n$). А. Брауэр установил [2] асимптотику роста величины $l(n)$, доказав, что $l(n) \leq \log n + O(\frac{\log n}{\log \log n})$. Но приведенный в доказательстве алгоритм требует растущего с ростом n числа ячеек памяти. Возникает естественный вопрос об исследовании сложности возведения в степень в случае фиксированного числа ячеек памяти.

Определения

Изучается задача об эффективном возведении в степень с использованием t ячеек памяти. Эта задача может быть формализована следующим образом.

Определение. *Аддитивной t-цепочкой для натурального числа n* называется последовательность $a^{(0)}, a^{(1)}, \ldots, a^{(r)}$ наборов $a^{(i)} = (a_1^{(i)}, \ldots, a_t^{(i)})$, таких, что:

1) $a^{(0)} = (1, \ldots, 1)$;

2) найдется $u \in \{1, \ldots, t\}$, такое, что $a_u^{(r)} = n$;

3) для любого значения $i \in \{1, \ldots, r\}$ найдется $j_0 \in \{1, \ldots, t\}$, такое, что $a_{j_0}^{(i)} = a_k^{(i-1)} + a_s^{(i-1)}$, где $1 \leq k, s \leq t$, и при этом $a_j^{(i)} = a_j^{(i-1)}$ для всех $j \neq j_0$.

Под $l_t(n)$ будем понимать минимально возможную длину r аддитивной t-цепочки для числа n.

Простейшие свойства и оценки

Утверждение 1. *При $t > 1$ любое число n можно вычислить, используя t ячеек памяти. В случае $t = 1$ можно вычислить лишь числа вида 2^k.*

Утверждение 2. *Для любого фиксированного t, $t \geq 2$, при $n \to \infty$ справедливо соотношение $l_t(n) \asymp \log n$.*

Доказательство. Этот простой факт следует из очевидной нижней оценки $\log n \leq l_t(n)$ и неравенств $l_t(n) \leq l_2(n) \leq \log n + v(n)$, где $v(n)$ — число единиц в двоичной записи числа n. Очевидно, что $v(n) \leq \log n$.

Теорема 1 (нижняя оценка). *Для любого фиксированного t, $t \geq 2$, найдется такое $\varepsilon = \varepsilon(t) > 0$, что при $n \to \infty$ доля чисел k из множества $\{1, \ldots, n\}$, удовлетворяющих условию $l_t(k) \geq (1+\varepsilon) \log n$, стремится к 1.*

Доказательство приводится в [3].

Утверждение 3 (тривиальная верхняя оценка). *Для любого натурального k для справедливости оценки $l_t(n) \le (1+\frac{1}{k})\log n$ достаточно, чтобы $t \ge 1 + 2^{k-1}$.*

Доказательство. Оценка следует из того, что 2^{k-1} ячеек памяти достаточно для получения всех возможных остатков от деления на 2^k. Это так, потому что можно хранить лишь те числа, в двоичной записи которых старший и младший разряд равны 1 и, кроме того, саму единицу (длина двоичной записи при этом не превосходит k). Таким образом, учитывая, что для вычислений требуется ещё одна ячейка для хранения промежуточного результата, получаем:

$$t \ge \sum_{i=2}^{k} 2^{i-2} + 1 + 1 = 1 + 2^{k-1}.$$

Вычисления с помощью 4-цепочек

Приведённое выше утверждение может быть переформулировано следующим образом:

$$l_t(n) \le \left(1 + \frac{1}{1 + \lfloor \log(t-1) \rfloor}\right) \log n.$$

Для случаев $t = 2, 3$ выполняется равенство $\lfloor \log(t-1) \rfloor = \log(t-1)$. Соответственно, возникает вопрос, можно ли улучшить общую верхнюю оценку в случае, когда подобного равенства нет, т. е. при $t = 4$? Иными словами, возникает вопрос, можно ли улучшить оценку $l_4(n) \le \frac{3}{2}\log n$?

Определение. *Методом "$x - y - z$"* будем называть следующий способ вычисления с использованием четырёх ячеек памяти: когда $a^{(i)} = (a_1^{(i)}, x, y, z)$, начиная с некоторого номера $i = i_0$ (т. е. $a^{(i)}$ представляют собой последовательность промежуточных результатов вычислений).

Аналогичные определения можно дать и для других размерностей t, отличных от 4.

Замечание. Обычно процесс вычислений будет построен так, чтобы за сложение $a_1^{(i)}$ с x, y или z вычислялось в точности $(1 + \lfloor \log x \rfloor)$, $(1 + \lfloor \log y \rfloor)$ либо $(1 + \lfloor \log z \rfloor)$ соответственно символов двоичного представления числа n.

Теорема 2. *Найдется такой параметр $\varepsilon > 0$, что для любого n выполняется оценка $l_4(n) \le \left(\frac{3}{2} - \varepsilon\right)\log n$.*

Доказательство. Пусть ε — некоторый положительный параметр, значение которого выберем позже.

Обозначим через α долю единиц в двоичной записи числа n, через β — долю нулей в двоичной записи числа n. Очевидно, что $\alpha + \beta = 1$.

Случай 1. Предположим, что $\alpha \ge 2/3{+}2\varepsilon$. Пусть в двоичной записи числа n $1\ldots10\ldots01\ldots10\ldots0\ldots\ldots1\ldots10\ldots0$ количество "блоков" из единиц равно

u, количество единиц — s_i, $i = 1, \ldots, u$. При этом длины блоков из нулей положительны (кроме, может быть, последнего). Очевидно, что $\sum\limits_{i=1}^{u} s_i = \alpha \log n$, $u \leq \beta \log n + 1$. Обозначим через a количество таких блоков, что для них $s_i = 3v_i$, через b — т. ч. $s_i = 3v_i + 1$, через c — т. ч. $s_i = 3v_i + 2$. С помощью метода "$1 - 3 - 7$" получаем:

$$l_4(n) \leq \log n + \frac{\alpha \log n - b - 2c}{3} + b + c.$$

Так как $\alpha \geq 2/3 + 2\varepsilon$, то выполняется следующее соотношение:

$$2b + c \leq 2a + 2b + 2c \leq 2\beta \log n + 2 \leq 2\left(\frac{1}{3} - 2\varepsilon\right)\log n + 2 \leq \left(\frac{2}{3} - 3\varepsilon\right)\log n.$$

Отсюда следует

$$\frac{\alpha \log n + 2b + c}{\log n} \leq \frac{3}{2} - 3\varepsilon,$$

из чего и получается оценка

$$l_4(n) \leq (3/2 - \varepsilon)\log n.$$

Случай 2. Пусть $\alpha < 2/3 + 2\varepsilon$. Разобьём двоичную запись числа n на непересекающиеся блоки длины 3 (один блок может быть меньшей длины). Рассмотрим количество блоков вида '111'. Обозначим это число через x_1.

Случай 2.1. Если $x_1 \geq (1/12 + 3\varepsilon/2)\log n$, то выполняется неравенство (при использовании метода "$1 - 7$"):

$$\begin{aligned} l_4(n) &\leq \log n + x_1 + \alpha \log n - 3x_1 \leq \\ &\leq \log n(1 + 2/3 + 2\varepsilon - 2(1/12 + 3\varepsilon/2)) \leq (3/2 - \varepsilon)\log n. \end{aligned}$$

Случай 2.2. Теперь пусть $x_1 < (1/12 + 3\varepsilon/2)\log n$. Если применить метод "$1 - 3 - 5$" , то на вычисление каждого блока, кроме блоков вида '111', понадобится не более чем по четыре операции (из них три удвоения), а на блоки из трех единиц — не более чем по 5 операций (три удвоения и по одному прибавлению 1 и 5). Следовательно:

$$l_4(n) \leq \left\lceil \frac{4}{3}\log n \right\rceil + x_1 \leq \log n \left(\frac{4}{3} + \frac{1}{12} + \frac{3}{2}\varepsilon\right).$$

Теперь возьмем ε таким, чтобы $\frac{4}{3} + \frac{1}{12} + \frac{3}{2}\varepsilon \leq \frac{3}{2} - \varepsilon$.

Итак, желаемая оценка получена.

Замечание. Из приведённого выше доказательства следует, что за ε можно взять, например, $\frac{1}{30}$.

Работа выполнена при финансовой поддержке РФФИ (проект 11–01–00508) и программы фундаментальных исследований ОМН РАН „Алгебраические и комбинаторные методы математической кибернетики и информационные системы нового поколения“.

Список литературы

1. Кнут Д. Е. Искусство программирования для ЭВМ. Т. 2. — М.: Мир, 1977.
2. Brauer A. On addition chains // Bull. Amer. Math. Soc. — 1939. — V. 45. — P. 736–739.
3. Балакин К. С. О сложности возведения в степень при ограничениях на используемую память // Материалы X международного семинара "Дискретная математика и ее приложения" — 2010. — С. 85–88.

ОБ ОДНОМ МЕТОДЕ ПОВЫШЕНИЯ НАДЕЖНОСТИ СХЕМ, РЕАЛИЗУЮЩИХ ФУНКЦИИ ИЗ P_3

О. Ю. Барсукова (Пенза)

Пусть $E_3 = \{0, 1, 2\}$. Рассмотрим функции $f(x_1, \ldots, x_n) : (E_3)^n \to E_3$ $(n \geq 1)$.

Обозначим через P_3 множество всех функций 3-значной логики и положим $\tilde{x} = (x_1, \ldots, x_n)$. Рассмотрим реализацию функций из P_3 схемами из ненадежных функциональных элементов в базисе Россера – Туркетта $\{0, 1, 2, J_0(x_1), J_1(x_1), J_2(x_1), \max\{x_1, x_2\}, \min\{x_1, x_2\}\}$. Для краткости обозначим $\min\{x_1, x_2\}$ через &, а $\max\{x_1, x_2\}$ через $\vee$.

Будем считать, что схема из ненадежных элементов реализует функцию $f(\tilde{x})$, если при поступлении на входы схемы набора $\tilde{a}$ при отсутствии неисправностей на выходе схемы появляется значение $f(\tilde{a})$.

Предположим, что каждый элемент базиса на любом входном наборе $\hat{a}$ $(\hat{a} = (a_1, a_2))$ таком, что $f(\hat{a}) = \tau$, с вероятностью ε выдает значение $\bar{\tau} = \mu$ и с вероятностью ε выдает значение $\bar{\mu}$. Все элементы схемы переходят в неисправные состояния независимо друг от друга.

Пусть схема S реализует функцию $f(\tilde{x})$. Обозначим через $P_{f(\tilde{a})\neq\tau}(S, \tilde{a})$ вероятность ошибки на выходе схемы S при входном наборе $\tilde{a}$, на котором $f(\tilde{a}) = \tau$. Таким образом, $P_{f(\tilde{a})\neq\tau}(S, \tilde{a}) = P_{\tau+1}(S, \tilde{a}) + P_{\tau+2}(S, \tilde{a})$. Например, если схема S реализует функцию $f(\tilde{x})$, и входной набор $\tilde{a}$ является нулевым, т. е. $f(\tilde{a}) = 0$, то вероятность ошибки равна $P_{f(\tilde{a})\neq 0}(S, \tilde{a}) = P_1(S, \tilde{a}) + P_2(S, \tilde{a})$.

Ненадежностью схемы S будем называть число $P(S) = \max\{P_{f(\tilde{a})\neq\tau}(S, \tilde{a})\}$, где максимум берется по всем входным наборам $\tilde{a}$ схемы S.

Рассмотрим функциональный элемент $E_\&$ с функцией &. Вычислим p_0, p_1, p_2 вероятности появления 0, 1, 2 на выходе элемента $E_\&$ (см. табл. 1).

Замечание. *Очевидно,* $P(E_\&) = 2\varepsilon$, *а надежность* $1 - 2\varepsilon$.

Пусть $f(\tilde{x})$ — произвольная функция из P_3. Пусть S — произвольная схема, реализующая $f(\tilde{x})$. Возьмем два экземпляра схемы S и соединим их выходы со входами элемента E с функцией e (см. рис. 1).

Таблица 1

xy	$x\&y$	p_0	p_1	p_2
0 0	0	$1-2\varepsilon$	ε	ε
0 1	0	$1-2\varepsilon$	ε	ε
0 2	0	$1-2\varepsilon$	ε	ε
1 0	0	$1-2\varepsilon$	ε	ε
1 1	1	ε	$1-2\varepsilon$	ε
1 2	1	ε	$1-2\varepsilon$	ε
2 0	0	$1-2\varepsilon$	ε	ε
2 1	1	ε	$1-2\varepsilon$	ε
2 2	2	ε	ε	$1-2\varepsilon$

Обозначим $P_i(B,\tilde{a})$ — вероятность появления значения i на выходе B при входном наборе $\tilde{a}$.

Справедлива лемма 1.

Лемма 1. *Пусть* $e = \&$ (*рис.* 1); $p_0(S,\tilde{a}), p_1(S,\tilde{a}), p_2(S,\tilde{a})$ — *вероятности появления* $0, 1, 2$ *на выходе схемы* S *при входном наборе* $\tilde{a}$. *Тогда вероятности появления неверных значений на выходе схемы* B *равны*:

$P_1(B,\tilde{a}) = \varepsilon + p_1^2(S,\tilde{a})(1-3\varepsilon) + p_1(S,\tilde{a})p_2(S,\tilde{a})(2-6\varepsilon)$,

$P_2(B,\tilde{a}) = \varepsilon + p_2^2(S,\tilde{a})(1-3\varepsilon) + 2p_1(S,\tilde{a})\varepsilon - 2p_1^2(S,\tilde{a})\varepsilon$, *если набор* $\tilde{a}$ *такой, что* $f(\tilde{a}) = 0$;

$P_0(B,\tilde{a}) = \varepsilon + p_0^2(S,\tilde{a})(3\varepsilon-1) + p_0(S,\tilde{a})(2-6\varepsilon)$,

$P_2(B,\tilde{a}) = \varepsilon + p_2^2(S,\tilde{a})(1-3\varepsilon)$, *если набор* $\tilde{a}$ *такой, что* $f(\tilde{a}) = 1$;

$P_0(B,\tilde{a}) = \varepsilon + p_0^2(S,\tilde{a})(3\varepsilon-1) + p_0(S,\tilde{a})(2-6\varepsilon)$,

$P_0(B,\tilde{a}) = \varepsilon + p_1^2(S,\tilde{a})(3\varepsilon-1) + p_1(S,\tilde{a})(2-6\varepsilon) + p_0\ (S,\tilde{a})p_1(S,\tilde{a})(6\varepsilon-2)$, *если набор* $\tilde{a}$ *такой, что* $f(\tilde{a}) = 2$.

Доказательство проводится непосредственным вычислением с помощью формулы полной вероятности.

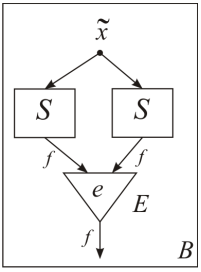

Рис.1

Рассмотрим функциональный элемент $E_\vee$ с функцией $\vee$. Вычислим p_0, p_1, p_2 вероятности появления 0, 1, 2 на выходе элемента $E_\vee$ (см. таб. 2).

Таблица 2

xy	$x \vee y$	p_0	p_1	p_2
0 0	0	$1-2\varepsilon$	ε	ε
0 1	1	ε	$1-2\varepsilon$	ε
0 2	2	ε	ε	$1-2\varepsilon$
1 0	1	ε	$1-2\varepsilon$	ε
1 1	1	ε	$1-2\varepsilon$	ε
1 2	2	ε	ε	$1-2\varepsilon$
2 0	2	ε	ε	$1-2\varepsilon$
2 1	2	ε	ε	$1-2\varepsilon$
2 2	2	ε	ε	$1-2\varepsilon$

Справедлива лемма 2.

Лемма 2. *Пусть* $e = \vee$ (*рис.* 1); $p_0(S,\tilde{a}), p_1(S,\tilde{a}), p_2(S,\tilde{a})$ — *вероятности появления* $0, 1, 2$ *на выходе схемы* S *при входном наборе* $\tilde{a}$. *Тогда вероятности появления неверных значений на выходе схемы* B *равны*:

$P_1(S,\tilde{a}) = \varepsilon + p_1^2(S,\tilde{a})(3\varepsilon-1) + p_1(S,\tilde{a})(2-6\varepsilon) + p_1(S,\tilde{a})p_2(S,\tilde{a})(6\varepsilon-2)$,

$P_2(S,\tilde{a}) = \varepsilon + p_2^2(S,\tilde{a})(3\varepsilon-1) + p_2(S,\tilde{a})(2-6\varepsilon)$, *если набор* $\tilde{a}$ *такой, что* $f(\tilde{a}) = 0$;

$P_0(S,\tilde{a}) = \varepsilon + p_0^2(S,\tilde{a})(1-3\varepsilon) + 2p_0(S,\tilde{a})\varepsilon + 2p_2(S,\tilde{a})\varepsilon$,

$P_2(S,\tilde{a}) = \varepsilon - p_2^2(S,\tilde{a})\varepsilon + p_2(S,\tilde{a})(2-2\varepsilon) - p_2^2(S,\tilde{a})$, *если набор* $\tilde{a}$ *такой, что* $f(\tilde{a}) = 1$;

$P_0(S,\tilde{a}) = \varepsilon + p_0^2(S,\tilde{a})(1-3\varepsilon)$,

$P_1(S,\tilde{a}) = \varepsilon + p_0(S,\tilde{a})p_1(S,\tilde{a})(2-6\varepsilon) + p_1^2(S,\tilde{a})(1-3\varepsilon)$, *если набор* $\tilde{a}$ *такой, что* $f(\tilde{a}) = 2$.

С помощью лемм 1 и 2 доказывается теорема 1.

Теорема 1. *Пусть* $f(\tilde{x})$ — *произвольная функция, пусть схема* S *реализует* $f(\tilde{x})$ *с ненадежностью* $P(S)$. *Тогда схема* $\psi(S)$ (*см. рис.* 2) *реализует функцию* f *с ненадежностью*

$$P(\psi(S)) \le 6\varepsilon + 4\varepsilon P(S) + 8P^2(S).$$

С использованием теоремы 1 доказывается теорема 2.

Теорема 2. *Любую функцию* $f(x_1,\ldots,x_n)$ *можно реализовать такой схемой* S, *что при всех* $\varepsilon \le 1/(8(2n+1)(1+4\cdot 3^n(3n+1)))$ *верно неравенство*

$$P(S) \le 6\varepsilon + 420\varepsilon^2.$$

Работа выполнена при финансовой поддержке РФФИ, номер проекта 11-01-00212а.

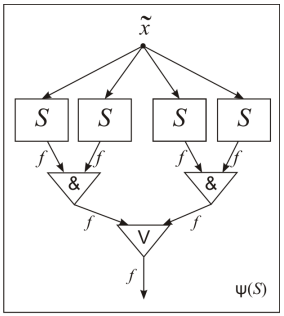

Рис.2

Список литературы

1. Яблонский С. В. Введение в дискретную математику. — М.: Наука, 1986.
2. Алехина М. А. Синтез асимптотически оптимальных по надежности схем. — Пенза: Информац.-издат.центр ПГУ, 2006.
3. Васин А. В. Об асимптотически оптимальных схемах в базисе $x\&y, x \vee y, \bar{x}$ при инверсных неисправностях на выходах элементов // Известия высших учебных заведений. Поволжский регион. Физико-математические науки. — 2008. — № 4. — С. 3–17.

ОБ ЭФФЕКТИВНО ФУНКЦИОНАЛЬНО РАЗРЕШИМЫХ КЛАССАХ В ТРЕХЗНАЧНОЙ ЛОГИКЕ

А. В. Бухман (Москва)

В данном докладе рассмотрены вопросы построения эффективных алгоритмов для проверки сохранения функциями из P_k некоторых предикатов. Эта проблема актуальна так как её решение ведёт к построению эффективного решения проблемы полноты системы функций. В работе продолжены исследования начатые в [1–2].

1. Определения

Будем обозначать $E_k = \{0, \ldots, k-1\}$.

Определение 1. *Функцией k-значной логики*, зависящей от n переменных, будем называть любое отображение вида $f : E_k^n \to E_k$.

Множество всех функций k-значной логики будем обозначать P_k.

Обычным образом [3] вводится операция суперпозиции над функциями из P_k.

Определение 2. Пусть $Q \subset P_3$. Множество Q называется *замкнутым классом*, если всякая функция, полученная в результате суперпозиции любых функций из Q, принадлежит Q.

Определение 3. Пусть $m \geq 1$, *m-местным предикатом* $\rho(x)$ на E_k называется любое отображение вида $E_k^m \to \{0,1\}$. Если a некоторый набор из E_k^m такой, что $\rho(a) = 1$, то говорят, что предикат верен на этом наборе, иначе он ложен на этом наборе.

Определение 4. *Функция $f(x_1, \ldots, x_n) \in P_k$ сохраняет предикат ρ* на E_k, если для любых $a_1^1, \ldots, a_1^m, \ldots, a_n^1, \ldots, a_n^m \in E_k$ таких, что

$$\rho(a_1^1, \ldots, a_1^m) = 1, \ldots, \rho(a_n^1, \ldots, a_n^m) = 1$$

будет верно $\rho(f(a_1^1, \ldots, a_n^1), \ldots, f(a_1^m, \ldots, a_n^m)) = 1$.

Множество всех функций k-значной логики, сохраняющих предикат ρ, будем обозначать $A_k(\rho)$.

Верна следующая теорема.

Теорема 1 [3]. *Путь ρ — m-местный предикат на E_k. Тогда множество $A_k(\rho)$ — замкнутый класс.*

Определение 5. *Матрицей предиката* называется матрица, столбцами которой являются все наборы (выписанные в произвольном порядке), на которых предикат верен.

В данной работе будет рассматриваться специальный класс предикатов — центральные предикаты. Прежде чем ввести понятие центрального предиката дадим несколько вспомогательных определений.

Определение 6. Пусть $m \geq 2$, m-местный предикат $\rho(x)$ на E_k назовём *тотально симметричным*, если для любого набора $(a_1, \ldots, a_m) \in E_k^m$ такого, что $\rho(a_1, \ldots, a_m) = 1$, и для любой перестановки s над множеством $\{1, \ldots, m\}$ верно, что $\rho(a_{s(1)}, \ldots, a_{s(m)}) = 1$.

Определение 7. Пусть $m \geq 2$, m-местный предикат $\rho(x)$ на E_k называется *тотально рефлексивным*, если он верен на всех наборах из E_k^m, в которых есть хотя бы два совпадающих элемента.

Определение 8. Предикат *обладает центром* $C \subset E_k, C \neq \emptyset$, если он верен на любом наборе, содержащем хотя бы один элемент $c \in C$.

Теперь введём понятие центрального предиката.

Определение 9. Пусть $m \geq 2$, m-местный предикат на E_k, отличный от тождественно истинного, называется *центральным*, если обладает следующими свойствами:

1. Является тотально симметричным.
2. Является тотально рефлексивным.
3. Обладает центром.

Любой одноместный предикат, который верен хотя бы на одном элементе, будем считать по определению центральным.

В данной работе рассматривается задание функции в виде полиномов.

Определение 10. *Мономом* над переменными $x_1, \ldots, x_n$ называется любое выражение вида $x_{i_i}^{j_1} \ldots x_{i_l}^{j_l}$, где $l \geq 1$, $1 \leq i_1, \ldots, i_l \leq n$, $1 \leq j_1, \ldots, j_l \leq k-1$, все переменные различны; либо просто 1.

Равенство мономов рассматривается с точностью до перестановки сомножителей.

Определение 11. *Полиномом* называется сумма по модулю k конечного числа различных мономов с ненулевыми коэффициентами из E_k или 0 (можно понимать как сумму нулевого числа мономов). *Длиной* полинома называется число его слагаемых. Длину нулевого полинома будем считать равной 0.

Равенство полиномов рассматривается с точностью до перестановки слагаемых.

Известно, что всякая функция трёхзначной логики может быть представлена полиномом, причём однозначно. Далее будем считать, что функция подаётся на вход алгоритму(машине Тьюринга) в виде полинома. Таким образом, если в полиноме функции n переменных имеется L слагаемых, то длина записи входного слова будет $N = Ln$.

2. Предикаты с центром $C = \{0\}$

В P_3 есть только один двуместный центральный предикат с центром 0. Ниже приводится матрица этого предиката.

$$\begin{pmatrix} 0 & 1 & 2 & 0 & 1 & 0 & 2 \\ 0 & 1 & 2 & 1 & 0 & 2 & 0 \end{pmatrix}$$

Для краткости ρ_0^k будем обозначать двуместный предикат над E_k, который верен на тех и только тех наборах, у которых обе компоненты совпадают или одна равна 0. Понятно, что ρ_0^k — двуместный центральный предикат над E_k с центром $C = \{0\}$.

Рассмотрим функцию $\phi_m^k : E_k^m \to E_k$. Определим её

$$\phi_m^k(x_1, \ldots, x_m) = x_1 \ldots x_m \prod_{1 \leq i < j \leq m} (x_i - x_j).$$

Например, $\phi_2^3(x, y) = (x - y)xy$.

Нетрудно видеть, что если k — простое число, то $\phi_2^k(a_1, a_2) = 0$ тогда и только тогда, когда ρ_0^k верен на наборе (a_1, a_2).

Утверждение 1. *Пусть k — простое, $f(x_1, \ldots, x_n) \in P_k^n$, эта функция сохраняет ρ_0^k, тогда и только тогда, когда верно, что*

$$h(x_1, \ldots, x_n, y_1, \ldots, y_n, z_1, \ldots, z_n) =$$
$$= \phi_2^k(f(x_1 y_1^{k-1}, \ldots, x_n y_n^{k-1}),\ f(x_1 z_1^{k-1}, \ldots, x_n z_n^{k-1})) \equiv 0.$$

Теорема 2. *Пусть k — простое число. Можно построить полиномиальный алгоритм, который по полиному функции из P_k может определить, сохраняет ли эта функция двуместный центральный предикат ρ_0^k.*

Доказательство. Построим этот алгоритм.

Воспользуемся утверждением 1. Пусть на вход алгоритма поступает P_f — полином исследуемой функции. Преобразуем его в полином функции h из утверждения 1. Для этого:

1. вместо x_i подставляем $x_i y_i^2$ в P_f, приводим подобные, получаем полином P_{f1};

2. вместо x_i подставляем $x_i z_i^2$ в P_f, приводим подобные, получаем полином P_{f2};

3. в полином функции ϕ вместо переменных подставляем полиномы P_{f1}, P_{f2}, раскрываем скобки, приводим подобные;

4. если в результате получился полином, который имеет хотя бы одно слагаемое, то выдаём ответ "нет". Иначе "да".

Алгоритму на вход подаётся запись длины $N = L(n+2)$, где L — длина полинома P_f, n – количество переменных. Оценим сложность алгоритма в рамках алгоритмической модели введённой ранее. Шаги 1 и 2 алгоритма выполняются со сложностью $O(N^2)$. Оценим сложность шага 3. Полином функции $\phi_2^k(x-y)$ имеет вид $x^2y + (k-1)xy^2$. При подстановке вместо переменных полиномов P_{f1} и P_{f2} нужно будет выполнить не более чем $O(N^3)$ операций (так как умножение полиномов длины N можно выполнить за $O(N^2)$ операций). В итоге получится выражение, длина которого $O(N^3)$. Операция приведения подобных имеет квадратичную сложность. Сложность полученного алгоритма $O(N^6)$.

3. Оценки на длину полинома

В этом разделе будет получена оценка на длину полинома функции из P_3, обладающей некоторым свойством. Также будет показано, как это свойство связано с сохранением функцией центральных предикатов.

Пусть $\alpha = (a_1, \ldots, a_n) \in E_3^n$. Тогда обозначим $E_3^n|_\alpha$ множество

$$\{(b_1, \ldots, b_n) \in E_3^n \mid \forall i (a_i \neq b_i)\}.$$

Пусть набор $\gamma = (c_1, \ldots, c_n) \in E_3^n|_\alpha$. *Противоположным набору γ в множестве $E_3^n|_\alpha$* будем называть набор $\overline{\gamma} = (d_1, \ldots, d_n) \in E_3^n|_\alpha$, такой что $\forall i (d_i \neq c_i)$.

Лемма 1. *Пусть* $n \geq 2$, $\alpha = (a_1, \ldots, a_n) \in \{0, 2\}^n$, $\gamma = (c_1, \ldots, c_n) \in E_3^n|_\alpha$. *Тогда для любой функции* $f \in P_3^n$ *такой, что*

$f(\gamma) = 0$,
$f(\overline{\gamma}) = 2$,
$f(x) = 1$, $x \in E_3^n|_\alpha \setminus (\{\gamma\} \cup \{\overline{\gamma}\})$,

верно, что длина полинома данной функции не меньше, чем $2^{n/2} - 2$.

Замечание. Заметим, что утверждение леммы 1 можно применить к распознаванию свойства функции из P_3 сохранять двуместный центральный предикат с центром 1. Пусть функция $f(x_1, \ldots, x_n) \in P_3$ не сохраняет двуместный центральный предикат с центром 1. Тогда существует набор $\alpha \in E_3^n$, и пара наборов $\beta \in E_3^n|_\alpha, \gamma \in E_3^n|_\alpha$. На этих наборах выполнено $f(\beta) = 2, f(\gamma) = 0$, а для любого набора x такого, что его $x_i = \alpha_i$ или $x_i = \beta_i$ или $x_i = 1$, если $\beta_i \neq \alpha_i$ верно, что $f(x) = 1$. Не ограничивая общности предположим, что наборы β и γ отличаются в первых j компонентах. Заметим, что функция $f(x_1, \ldots, x_j, \beta_{j+1}, \ldots, \beta n)$ удовлетворяет условию леммы 1. Отсюда следует, что длина полинома исходной функции больше либо равна $2^{j/2} - 2$.

Основываясь на приведённом выше замечании можно доказать следующие теоремы.

Теорема 3. *Можно построить детерминированный алгоритм сложности* $2^{O(\log^2(N))}$ (N *— длина входа*), *который по полиному функции из* P_3 *может определить, сохраняет ли эта функция двуместный центральный предикат с центром* $\{1\}$.

Доказательство. Заметим два факта.

1. Если $L < 2^{n/2}$, то достаточно проверить сохранение функцией предиката на наборах длины $< 2\log(L)$. Потребуется $O(C_{2\log L}^n)$ проверок. Заметим, что $C_{2\log L}^n < n^{\log L} < 2^{\log L \log n} < 2^{\log^2 Ln}$.

2. Если $L \geq 2^{n/2}$, то простой перебор даст полиномиальную оценку на сложность алгоритма.

Алгоритм состоит в том, что сначала проверяет какое из двух условий верно, а затем применяет соответствующий алгоритм. Окончательно имеем сложность $O(2^{\log^2 N})$.

Теорема 4. *Можно построить детерминированный алгоритм сложности* $2^{O(\log^2(N))}$ (N *— длина входа*), *который по полиному функции из* P_3 *может определить, сохраняет ли эта функция двуместный центральный предикат с центром* $\{2\}$.

Доказательство аналогично предыдущей теореме.

Список литературы

1. Селезнева С. Н. О сложности распознавания полноты множества булевых функций, реализованных полиномами Жегалкина //Дискретная математика. — 1997. — Т. 4, вып. 9. — С. 34–41.

2. Селезнева С. Н. Полиномиальный алгоритм для распознавания принадлежности реализованной полиномом функции k-значной логики предполным классам самодвойственных функций //Дискретная математика. — 1998. — Т. 3, вып. 10. — С. 64–72.
3. Яблонский С. В. Функциональные построения в k-значной логике // Труды МИАН им. В.А. Стеклова. — 1958. — Т. 51, — С. 5–142.

О ВЕРХНЕЙ ОЦЕНКЕ НЕНАДЕЖНОСТИ НЕВЕТВЯЩИХСЯ ПРОГРАММ С НЕНАДЕЖНЫМ ОПЕРАТОРОМ УСЛОВНОЙ ОСТАНОВКИ

С. М. Грабовская (Пенза)

Введение

Рассматривается реализация булевых функций неветвящимися программами с операторами условной остановки (стоп-операторами) [1] в полном конечном базисе B, содержащем нелинейную функцию двух переменных, т. е. некоторую функцию вида $(x_1^{c_1}\&x_2^{c_2})^{c_3}$ $(c_1, c_2, c_3 \in \{0, 1\})$. *Программы с оператором условной остановки* характеризуются наличием управляющей команды – команды условной остановки, дающей возможность досрочного прекращения работы при выполнении определенного условия. В исправном состоянии стоп-оператор срабатывает при поступлении на его вход единицы. При этом программа прекращает работу, а результатом работы программы считается значение выходной переменной z, вычисленное перед остановкой.

Полагаем, что оператор условной остановки подвержен двум типам неисправностей. *Неисправность первого типа* характеризуется тем, что при поступлении единицы на вход стоп-оператора он с вероятностью δ $(\delta \in (0, 1/2))$ не срабатывает, и, следовательно, работа программы продолжается. *Неисправность второго типа* такова, что при поступлении нуля на вход стоп-оператора он с вероятностью η $(\eta \in (0, 1/2))$ срабатывает, и, следовательно, работа программы прекращается.

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

Считаем, что программа с ненадежными операторами реализует булеву функцию $f(x_1, x_2, \ldots, x_n)$, если при отсутствии неисправностей во всех ее операторах (как вычислительных, так и остановки) на каждом входном наборе $\tilde{a}$ $(\tilde{a} = (a_1, a_2, \ldots, a_n))$ значение выходной переменной z равно $f(\tilde{a})$.

Нетрудно видеть, что схемы из функциональных элементов являются частным случаем неветвящихся программ с условной остановкой, точнее, схему из функциональных элементов можно считать программой, в которой нет ни одного стоп-оператора.

Ненадежностью $N(Pr)$ программы Pr назовем максимальную вероятность ошибки на выходе программы Pr при всевозможных входных наборах. Надежность программы Pr равна $1 - N(Pr)$.

Теорема 1. *Пусть B — полный конечный базис, программа Pr_g реализует функцию $g(x_1, x_2, x_3) = x_1^{a_1}x_2^{a_2} \vee x_1^{a_1}x_3^{a_3} \vee x_2^{a_2}x_3^{a_3}$ $(a_i \in \{0,1\},\ i \in \{1,\ 2,\ 3\})$ с ненадежностью $N(Pr_g)$. Тогда любую булеву функцию f в этом базисе можно реализовать программой Pr_f, ненадежность которой при всех $\varepsilon \in (0,\ 1/960]$ удовлетворяет неравенству*

$$N(Pr_f) \leqslant \max\{v^1,\ v^0\} + 15,6\varepsilon \cdot N(Pr_g) + 81,12\varepsilon^2,$$

где v^1 и v^0 — вероятности ошибок программы Pr_g на наборах $(\bar{a}_1, \bar{a}_2, \bar{a}_3)$ и (a_1, a_2, a_3) соответственно.

Доказательство. Пусть программа Pr_g реализует некоторую функцию $g(x_1, x_2, x_3) = x_1^{a_1}x_2^{a_2} \vee x_1^{a_1}x_3^{a_3} \vee x_2^{a_2}x_3^{a_3}$ $(a_i \in \{0,1\},\ i \in \{1,\ 2,\ 3\})$. Обозначим через f^a функцию f, если $a = 1$, и функцию $\bar{f}$, если $a = 0$. Известно [3], что в произвольном полном конечном базисе любую булеву функцию f можно реализовать схемой S, ненадежность которой $N(S) \leqslant 5,2\varepsilon$ при всех $\varepsilon \in (0,\ 1/960]$. Обозначим $P(\varepsilon) = 5,2\varepsilon$. Используя по одному экземпляру схем S_1, S_2 и S_3 и программу $Pr_g(x_1, x_2, x_3)$, построим для функции f неветвящуюся программу Pr_f (см. рис. 1).

Pr_f :
$y_1 = f^{a_1}[S_1]$
$y_2 = f^{a_2}[S_2]$
$y_3 = f^{a_3}[S_3]$
$Pr_g(y_1,\ y_2,\ y_3)$

Рис. 1

Пусть $\tilde{\beta}$ — произвольный входной набор программы Pr_f, а $P(S_i, \tilde{\beta})$ — вероятности ошибок на выходах схем S_i $(i \in \{1,\ 2,\ 3\})$ соответственно при входном наборе $\tilde{\beta}$. Обозначим $P_i = P(S_i, \tilde{\beta}),\ \ i \in \{1,\ 2,\ 3\}$. Очевидно, что $\max\{P_1, P_2, P_3\} \leqslant \{N(S_1), N(S_2), N(S_3)\} \leqslant P(\varepsilon)$. Пусть входной набор $\tilde{\beta}$ такой, что $f(\tilde{\beta}) = 0$. На наборе $\tilde{\beta}$ оценим вероятность ошибки $P(Pr_f, \tilde{\beta})$ программы Pr_f, т. е. вероятность появления единицы.

$$P(Pr_f, \tilde{\beta}) \leqslant (1-P_1)(1-P_2)(1-P_3) \cdot v^1 +$$
$$+[P_1(1-P_2)(1-P_3) + (1-P_1)P_2(1-P_3) + (1-P_1)(1-P_2)P_3] \cdot N(Pr_g) +$$
$$+[P_1P_2(1-P_3) + (1-P_1)P_2P_3 + P_1(1-P_2)P_3] + P_1P_2P_3 \leqslant$$
$$\leqslant v^1 + 3P(\varepsilon)N(Pr_g) + 3P^2(\varepsilon).$$

Пусть входной набор $\tilde{\beta}$ такой, что $f(\tilde{\beta}) = 1$. На наборе $\tilde{\beta}$ оценим вероятность ошибки $P(Pr_f, \tilde{\beta})$ программы Pr_f, т. е. вероятность появления нуля. Аналогично получаем $P(Pr_f, \tilde{\beta}) \leqslant v^0 + 3P(\varepsilon)N(Pr_g) + 3P^2(\varepsilon)$.

Поскольку $N(Pr_f) = \max\limits_{\tilde{\beta}} P(Pr_f, \tilde{\beta})$, тогда справедливо неравенство $N(Pr_f) \leqslant \max\{v^1,\ v^0\} + 3P(\varepsilon)N(Pr_g) + 3P^2(\varepsilon)$. Подставляя в последнее неравенство значение $P(\varepsilon)$ и учитывая условие $\varepsilon \in (0,\ 1/960]$, получим $N(Pr_f) \leqslant \max\{v^1, v^0\} + 15,6\varepsilon N(Pr_g) + 81,12\varepsilon^2$. Теорема 1 доказана.

Наборы $(\bar{a}_1, \bar{a}_2, \bar{a}_3)$ и (a_1, a_2, a_3) для функции

$$g(x_1, x_2, x_3) = x_1^{a_1}x_2^{a_2} \vee x_1^{a_1}x_3^{a_3} \vee x_2^{a_2}x_3^{a_3}$$

будем называть *характеристическими*.

Основные результаты

Пусть полный конечный базис B содержит нелинейную функцию двух переменных, т. е. некоторую функцию вида $(x_1^{c_1}\&x_2^{c_2})^{c_3}$ $(c_1, c_2, c_3 \in \{0, 1\})$. Таким образом, базис B содержит хотя бы одну из функций $x_1 \vee x_2$, $\bar{x}_1 \vee x_2$, $\bar{x}_1 \vee \bar{x}_2$, $x_1\&x_2$, $\bar{x}_1\&x_2$, $\bar{x}_1\&\bar{x}_2$.

Основной результат этой статьи сформулирован в теореме 2.

Теорема 2. *В полном конечном базисе B, содержащем нелинейную функцию двух переменных, любую булеву функцию f можно реализовать такой программой Pr_f, что при всех $\varepsilon \in (0,\ 1/960]$ справедливо неравенство $N(Pr_f) \leqslant \varepsilon + 129\sigma^2$, где $\sigma = \max\{\varepsilon, \delta, \eta\}$.*

Доказательству теоремы 2 предпошлем леммы 1–3.

Лемма 1. *Если полный конечный базис содержит хотя бы одну из функций $x_1 \vee x_2$, $\bar{x}_1 \vee x_2$, $\bar{x}_1 \vee \bar{x}_2$ или $x_1\&x_2$, то в этом базисе можно реализовать функцию $g(x_1, x_2, x_3) = x_1^{a_1}x_2^{a_2} \vee x_1^{a_1}x_3^{a_3} \vee x_2^{a_2}x_3^{a_3}$ $(a_1, a_2, a_3 \in \{0, 1\})$ такой неветвящейся программой Pr_g (рис. 2 для $x_1 \vee x_2$, $a_1 = a_2 = a_3 = 1$; рис. 3 для $\bar{x}_1 \vee x_2$, $a_1 = 0$, $a_2 = a_3 = 1$; рис. 4 для $\bar{x}_1 \vee \bar{x}_2$, $a_1 = a_3 = 0$, $a_2 = 1$; рис. 5 для $x_1\&x_2$, $a_1 = 0$, $a_2 = a_3 = 1$), что справедливы неравенства $\max\{v^1,\ v^0\} \leqslant \varepsilon$ и $N(Pr_g) \leqslant 3\sigma$, где v^1, v^0 — вероятности ошибок программы Pr_g на соответствующих характеристических наборах, $\sigma = \max\{\varepsilon, \delta, \eta\}$.*

Pr_g :	Pr_g :	Pr_g :	Pr_g :
$z = x_2 \vee x_3$	$z = \bar{x}_1 \vee x_3$	$z = \bar{x}_1 \vee \bar{x}_3$	$z = x_2\&x_3$
$stop(x_1)$	$stop(x_2)$	$stop(x_2)$	$stop(x_1)$
$z = x_2$	$z = x_2$	$z = x_2$	$z = x_2$
$stop(x_3)$	$stop(x_1)$	$stop(x_1)$	$stop(x_2)$
$z = x_3$	$z = x_3$	$z = \bar{x}_3 \vee \bar{x}_3$	$z = x_3$
Рис. 2	Рис. 3	Рис. 4	Рис. 5

Обозначим через T_0 [2] класс всех булевых функций $f(x_1, \ldots, x_n)$, сохраняющих константу 0, то есть функций, для которых выполнено равенство $f(0, \ldots, 0) = 0$.

По теореме Поста о функциональной полноте [2] любой полный конечный базис содержит функцию f_{T_0}, которая не сохраняет константу 0, то есть $f_{T_0}(0, \ldots, 0) = 1$ ($f_{T_0} \notin T_0$).

Лемма 2 [2]. *Любой полный конечный базис содержит такую функцию h, что $h(x, \ldots, x) \in \{1, \bar{x}\}$.*

Лемма 3. *Если полный конечный базис содержит хотя бы одну из функций $\bar{x}_1 \& x_2$ или $\bar{x}_1 \& \bar{x}_2$, то в этом базисе можно реализовать функцию $g(x_1, x_2, x_3) = x_1^{a_1} x_2^{a_2} \vee x_1^{a_1} x_3^{a_3} \vee x_2^{a_2} x_3^{a_3}$ (a_1, a_2, $a_3 \in \{0, 1\}$) такой неветвящейся программой Pr_g (рис. 6 а, б для $\bar{x}_1 \& x_2$, $a_1 = a_2 = 0$, $a_3 = 1$; рис. 7 а, б для $\bar{x}_1 \& \bar{x}_2$, $a_1 = a_2 = a_3 = 0$), что справедливы неравенства $\max\{v^1, v^0\} \leqslant \varepsilon + \delta^2$ и $N(Pr_g) \leqslant 3\sigma$, где v^1, v^0 — вероятности ошибок программы Pr_g на соответствующих характеристических наборах, $\sigma = \max\{\varepsilon, \delta, \eta\}$.*

Pr_g:	Pr_g:
$z = \bar{x}_2 \& x_3$	$z = \bar{x}_2 \& x_3$
$stop(x_1)$	$stop(x_1)$
$z = x_3$	$z = x_3$
$stop(x_2)$	$stop(x_2)$
$z = \bar{x}_2$	$z = 1$
а)	б)

Рис. 6

Pr_g:	Pr_g:
$z = \bar{x}_2 \& \bar{x}_3$	$z = \bar{x}_2 \& \bar{x}_3$
$stop(x_1)$	$stop(x_1)$
$z = \bar{x}_3$	$z = \bar{x}_3 \& \bar{x}_3$
$stop(x_2)$	$stop(x_2)$
$z = \bar{x}_2$	$z = 1$
а)	б)

Рис. 7

Рисунки 6 а, 7 а соответствуют случаю, когда в базисе содержится $\bar{x}$, а рисунки 6 б, 7 б — случаю, когда в базисе содержится константа 1 (см. лемму 3).

Доказательство теоремы 2

Пусть B — полный конечный базис, содержащий нелинейную функцию двух переменных, т. е. некоторую функцию вида $(x_1^{c_1} \& x_2^{c_2})^{c_3}$ ($c_1, c_2, c_3 \in \{0, 1\}$). Возможны шесть вариантов:

1) $c_1 = c_2 = c_3 = 0$; 2) $c_1 = 1$, $c_2 = c_3 = 0$;
3) $c_1 = c_2 = 1$, $c_3 = 0$; 4) $c_1 = c_2 = c_3 = 1$;
5) $c_1 = 0$, $c_2 = c_3 = 1$; 6) $c_1 = c_2 = 0$, $c_3 = 1$.

В каждом из этих случаев по леммам 1 и 3 соответственно некоторую функцию $g(x_1, x_2, x_3) = x_1^{a_1} x_2^{a_2} \vee x_2^{a_2} x_3^{a_3} \vee x_1^{a_1} x_3^{a_3}$ ($a_i \in \{0, 1\}$, $i \in \{1, 2, 3\}$) можно реализовать программой Pr_g, ненадежность которой $N(Pr_g) \leqslant 3\sigma$, а максимум из вероятностей ошибок на характеристических наборах не больше $\varepsilon + \delta^2$. Отметим, что значения параметров a_i ($i = 1, 2, 3$) во всех случаях

различны и соответственно равны:

$$\begin{array}{ll} 1)\ a_1 = a_2 = a_3 = 1; & 2)\ a_1 = 0,\ a_2 = a_3 = 1; \\ 3)\ a_1 = 0,\ a_2 = 1,\ a_3 = 0; & 4)\ a_1 = 0,\ a_2 = a_3 = 1; \\ 5)\ a_1 = \ a_2 = 0,\ a_3 = 1; & 6)\ a_1 = \ a_2 = \ a_3 = 0. \end{array}$$

Пусть f — любая булева функция. Воспользуемся теоремой 1, выбирая значения a_1, a_2, a_3 в каждом случае соответствующим образом. Тогда функцию f можно реализовать неветвящейся программой, ненадежность которой удовлетворяет неравенству

$$N(Pr_f) \leqslant \max\{v^1, v^0\} + 15,6\varepsilon \cdot N(Pr_g) + 81,12\varepsilon^2 \leqslant \varepsilon + 129\sigma^2.$$

Теорема 2 доказана.

Заключение

Таким образом, в полном конечном базисе, содержащем нелинейную функцию двух переменных и ненадежный оператор условной остановки, любую булеву функцию можно реализовать неветвящейся программой с ненадежностью не больше $\varepsilon + 129\sigma^2$ при всех $\varepsilon \in (0,\ 1/960]$ и $\sigma = \max\{\varepsilon,\ \delta,\ \eta\}$.

Сравним полученный результат с результатами для схем из функциональных элементов.

Обозначим $N_\varepsilon(f) = \inf N(S)$, где инфимум берется по всем схемам S из ненадежных элементов, реализующим булеву функцию f. 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. $\lim\limits_{\varepsilon \to 0} \frac{N_\varepsilon(f)}{N_\varepsilon(A)} = 1$.

В различных полных базисах из двухвходовых элементов [4] почти все булевы функции можно реализовать асимптотически оптимальными по надежности схемами из функциональных элементов с ненадежностью, асимптотически равной $k_B \cdot \varepsilon$ при $\varepsilon \to 0$. Константа k_B зависит от базиса, причем $k_B \in \{2, 3, 4, 5\}$. Например, $k_B = 5$ в базисе $B = \{\bar{x}_1 \& x_2, 1\}$, $k_B = 4$ в базисе $B = \{\bar{x}_1 \& x_2, \bar{x}_1\}$, $k_B = 3$ в базисе $B = \{\bar{x}_1 \& \bar{x}_2\}$, $k_B = 2$ в базисе $B = \{x_1 \& x_2, x_1 \oplus x_2, 1\}$.

Работа выполнена при финансовой поддержке Российского фонда фундаментальных исследований (номер проекта 11-01-00212а).

Список литературы

1. Чашкин А. В. О среднем времени вычисления значений булевых функций // Дискретный анализ и исследование операций. — 1997. — Т. 4, № 1. — С. 3–17.
2. Яблонский С. В. Введение в дискретную математику: Учебное пособие для вузов / Под ред. В. А. Садовничего. — М.: Высш. шк., 2001.
3. Алехина М. А., Васин А. В. О надежности схем в базисах, содержащих функции не более чем трех переменных // "Ученые записки Казанского государственного университета. Серия Физико-математические науки". — 2009. — Т. 151, кн. 2. — С. 25–35.

4. Васин А. В. Асимптотически оптимальные по надежности схемы в полных базисах из трехвходовых элементов // Дисс. ... канд. физико-математических наук. — Пенза: Информационно-издательский центр ПГУ, 2010.

О СЛОЖНОСТИ РЕАЛИЗАЦИИ ФОРМУЛАМИ ФУНКЦИЙ ИЗ $P_{k,2}$, $k \geqslant 3$

Д. А. Дагаев (Москва)

В работе рассматривается задача о сложности реализации формулами функций многозначной логики из замкнутых классов определенного вида. Получен результат, обобщающий теоремы 1 и 2 из [1] на случай функций произвольной значности.

Сначала дадим необходимые определения (см. также работы [1–6]). Пусть $k \geqslant 2$. Множество всех функций k-значной логики будем обозначать через P_k, а множество всех функций k-значной логики, принимающих значения только из множества $\{0,1\}$, — через $P_{k,2}$. Пусть $G \subseteq P_k$. Обозначим через $[G]$ замкнутый класс, порожденный системой G, а через $G(n)$ — множество всех функций из G, зависящих от переменных $x_1, \ldots, x_n$, $n \geqslant 1$. Пусть $f(x_1, \ldots, x_n) \in [G]$, Φ — формула над G, реализующая функцию f, а $F \subseteq [G]$. Обозначим через $L(\Phi)$ число символов переменных и констант, входящих в формулу Φ (сложность формулы Φ), а через $L_G(F(n))$ — функцию Шеннона для множества F.

Будем говорить, что булева функция $f(x_1, \ldots, x_n)$ удовлетворяет условию $< 0^\infty >$ (соответственно $< 1^\infty >$), если существует переменная x_i, $1 \leqslant i \leqslant n$, такая, что $f(x_1, \ldots, x_n) \geqslant x_i$ (соответственно $f(x_1, \ldots, x_n) \leqslant x_i$). Далее будем придерживаться обозначений для замкнутых классов булевых функций из работы [5], а именно: S — множество всех самодвойственных функций; T_i — множество всех функций, сохраняющих константу i, $i = 0, 1$; M — множество всех монотонных функций; L — множество всех линейных функций; O^∞ — множество всех функций, удовлетворяющих условию $< 0^\infty >$; I^∞ — множество всех функций, удовлетворяющих условию $< 1^\infty >$; K — множество всех конъюнкций; D — множество всех дизъюнкций; U — множество всех функций, существенно зависящих не более чем от одной переменной; C — множество всех функций, не имеющих существенных переменных.

Пусть $i \in \{0,1\}$. Положим

$$L_i = L \cap T_i,\ M_i = M \cap T_i,\ U_i = U \cap T_i,\ C_i = C \cap T_i;$$

$$M_{01} = M_0 \cap M_1,\ L_{01} = L_0 \cap L_1,\ U_{01} = U_0 \cap U_1;$$

$$O_0^\infty = T_0 \cap O^\infty,\ I_1^\infty = T_1 \cap I^\infty;$$

$$MO^\infty = M \cap O^\infty,\ MI^\infty = M \cap I^\infty,\ MO_0^\infty = M \cap O_0^\infty,\ MI_1^\infty = M \cap I_1^\infty.$$

Определим отображение «проекция» (обозначение: pr_k) из множества $P_{k,2}$ в множество P_2, $k \geqslant 3$. Пусть $f(x_1, \ldots, x_n) \in P_{k,2}$. Проекцией функции f называется булева функция $pr_k f(x_1, \ldots, x_n)$, значение которой на произвольном наборе $\widetilde{\alpha} \in \{0,1\}^n$ определяется равенством $pr_k f(\widetilde{\alpha}) = f(\widetilde{\alpha})$. Проекцией $pr_k F$ множества функций $F \subseteq P_{k,2}$ называется множество $\bigcup\{pr_k f\}$, где объединение берется по всем функциям $f \in F$. Нетрудно показать, что для любого замкнутого класса $F \subseteq P_{k,2}$ множество $pr_k F$ является замкнутым классом булевых функций.

Пусть B — произвольный замкнутый класс булевых функций. Для любого $k \geqslant 3$ положим

$$pr_k^{-1} B = \{f \in P_{k,2} |\ pr_k f \in B\}.$$

Легко видеть, что множество $pr_k^{-1} B$ является замкнутым классом. Более того, для любого замкнутого класса $F \subseteq P_{k,2}$, такого, что $pr_k F = B$, выполняется соотношение $F \subseteq pr_k^{-1} B$, поскольку множество $pr_k^{-1} B$ содержит все функции из $P_{k,2}$, проекция которых принадлежит множеству B. Класс $pr_k^{-1} B$ будем называть максимальным замкнутым классом. Таким образом, каждому замкнутому классу булевых функций соответствует ровно один максимальный класс функций из $P_{k,2}$, $k \geqslant 3$.

Известно (см. [6]), что при любом $k \geqslant 3$ максимальный замкнутый класс $pr_k^{-1} B$ является конечно-порожденным тогда и только тогда, когда $U_{01} \subseteq B$.

Отметим некоторые известные результаты в задаче о сложности реализации функций k-значной логики формулами над конечными системами.

В задаче о сложности реализации булевых функций над конечными полными системами основополагающие результаты были получены О. Б. Лупановым, доказавшим [2–4], что для любой конечной полной системы булевых функций G выполняется соотношение

$$L_G(P_2(n)) \sim \frac{2^n}{\log_2 n}.$$

Задача о поведении функций Шеннона для множества всех булевых функций тесно связана с задачей о поведении функций Шеннона, соответствующих замкнутым классам булевых функций при реализации функций формулами в полных конечных базисах. Для всех замкнутых классов булевых функций, не содержащихся в множестве $S \cup L \cup K \cup D$, и любого конечного полного базиса асимптотически точные формулы для соответствующих функций Шеннона были получены А. Е. Андреевым [7].

Другая постановка задачи связана с вопросом о сложности реализации булевых функций из замкнутых классов, порожденных произвольными конечными системами. А. Б. Угольников доказал [5], что для любой конечной системы булевых функций G найдется константа $c = c(G)$, такая, что для любой функции $f(x_1, \ldots, x_n)$ из $[G]$ имеет место неравенство $L_G(f) \leqslant c^n$.

В задаче о сложности реализации функций многозначной логики известные на данный момент результаты имеют меньшую общность, чем в случае булевых функций. Ряд авторов (см. [8, 9]) для некоторых конечных полных

систем функций $G \subseteq P_k$, $k \geqslant 3$, показали справедливость соотношения

$$L_G(P_k(n)) \sim \frac{k^n}{\log_k n}.$$

Перейдем к известным результатам в задаче о сложности реализации функций из максимальных классов. В работе [10] для некоторой конечной порождающей системы класса $pr_3^{-1}L$ была получена асимптотически точная оценка для соответствующей функции Шеннона. В [1, 11] для каждого конечно-порожденного максимального класса функций из $P_{3,2}$ и некоторой его конечной порождающей системы были получены верхняя и нижняя асимптотические оценки для функций Шеннона.

Теорема 1 [1]. *Пусть B — произвольный замкнутый класс булевых функций, такой, что $U_{01} \subseteq B$. Тогда существует конечная порождающая система G класса $pr_3^{-1}B$, такая, что*

$$\frac{3^n}{\log_2 n} \lesssim L_G(pr_3^{-1}B(n)) \lesssim \frac{3^n}{\log_2 n} + L_{pr_3G}(B(n)).$$

В качестве следствия из этой теоремы и известных результатов о сложности булевых функций для некоторых максимальных классов и некоторых их конечных порождающих систем была получена асимптотически точная оценка для соответствующих функций Шеннона.

Теорема 2 [1]. *Пусть B — замкнутый класс булевых функций, такой, что выполняется по крайней мере одно из следующих условий:*

1) $L_{01} \subseteq B$;
2) $M_{01} \subseteq B$;
3) $B \in \{O^\infty, O_0^\infty, I^\infty, I_1^\infty, MO^\infty, MO_0^\infty, MI^\infty, MI_1^\infty\}$;
4) $U_{01} \subseteq B \subseteq K$;
5) $U_{01} \subseteq B \subseteq D$.

Тогда найдется конечная система $G \subseteq P_{3,2}$, такая, что $[G] = pr_3^{-1}B$ и

$$L_G(pr_3^{-1}B(n)) \sim \frac{3^n}{\log_2 n}.$$

В данной работе результаты, аналогичные теоремам 1 и 2, получены для максимальных классов функций из $P_{k,2}$, $k \geqslant 3$. Справедливы следующие утверждения.

Теорема 3. *Пусть B — произвольный замкнутый класс булевых функций, такой, что $U_{01} \subseteq B$, и пусть $k \geqslant 3$. Тогда существует конечная порождающая система G класса $pr_k^{-1}B$, такая, что*

$$\frac{k^n}{\log_2 n} \lesssim L_G(pr_k^{-1}B(n)) \lesssim \frac{k^n}{\log_2 n} + L_{pr_kG}(B(n)).$$

Теорема 4. *Пусть B — замкнутый класс булевых функций, такой, что выполняется по крайней мере одно из следующих условий*:

1) $L_{01} \subseteq B$;
2) $M_{01} \subseteq B$;
3) $B \in \{O^\infty, O_0^\infty, I^\infty, I_1^\infty, MO^\infty, MO_0^\infty, MI^\infty, MI_1^\infty\}$;
4) $U_{01} \subseteq B \subseteq K$;
5) $U_{01} \subseteq B \subseteq D$.

Пусть $k \geqslant 3$. Тогда найдется конечная система $G \subseteq P_{k,2}$, такая, что $[G] = pr_k^{-1}B$ и

$$L_G(pr_k^{-1}B(n)) \sim \frac{k^n}{\log_2 n}.$$

Схема доказательства этих теорем аналогична схеме доказательства теорем 1 и 2 (см. [1]).

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

Работа выполнена при финансовой поддержке РФФИ, проект №11-01-00508, и программы фундаментальных исследований Отделения математических наук РАН «Алгебраические и комбинаторные методы математической кибернетики и информационные системы нового поколения», проект «Задачи оптимального синтеза управляющих систем».

Список литературы

1. Дагаев Д. А. О сложности функций из некоторых классов трехзначной логики // Вестник Московского университета. Серия 1. Математика. Механика. — 2011. — № 3. — С. 60–63.
2. Лупанов О. Б. О сложности реализации функций алгебры логики формулами // Проблемы кибернетики. — 1960. — Вып. 3. — С. 61–80.
3. Лупанов О. Б. О синтезе некоторых классов управляющих систем // Проблемы кибернетики. — 1963. — Вып. 10. — С. 63–97.
4. Лупанов О. Б. Асимптотические оценки сложности управляющих систем // М.: Изд-во МГУ, 1984.
5. Угольников А. Б. О глубине и сложности формул, реализующих функции из замкнутых классов // Доклады АН СССР. — 1988. — Т. 298, № 6. — С. 1341–1344.
6. Lau D. Function Algebras on Finite Sets. —Berlin: Springer-Verlag, 2006.
7. Андреев А. Е. О синтезе функциональных сетей. Докт. диссертация. М.: МГУ им. М. В. Ломоносова, 1985.
8. Гашков С. Б. О параллельном вычислении некоторых классов многочленов с растущим числом переменных // Вестник Московского университета. Серия 1. Математика. Механика. — 1991. — № 2. — С. 88–92.
9. Захарова Е. Ю. Реализация функций из P_k формулами // Математические заметки. — 1972. — Т. 11, вып. 1. — С. 99–108.

10. Дагаев Д. А. О сложности псевдолинейных функций // Вестник Московского университета. Серия 1. Математика. Механика. — 2010. — № 2. — С. 53–56.
11. Дагаев Д. А. Реализация формулами функций из некоторых классов трехзначной логики // Мат-лы XVI Межд. конф. «Проблемы теоретической кибернетики» (Нижний Новгород, 20–25 июня 2011 г.). — Нижний Новгород: Изд-во Нижегородского гос. ун-та. — 2011. — С. 136–138.

О СУЩЕСТВОВАНИИ ПОРОЖДАЮЩИХ СИСТЕМ СПЕЦИАЛЬНОГО ВИДА В КЛАССАХ МОНОТОННЫХ ФУНКЦИЙ k-ЗНАЧНОЙ ЛОГИКИ

О. С. Дудакова (Москва)

Известно, что при $k \leq 7$ все предполные классы функций k-значной логики являются конечно-порожденными [1], а начиная с $k = 8$ существуют предполные классы монотонных функций, не имеющие конечного базиса [2]; полного описания конечно-порожденных предполных классов монотонных функций к настоящему времени не получено. В работах автора [3]–[6] получен критерий конечной порожденности для предполных классов функций, монотонных относительно частично упорядоченных множеств ширины два, а также условия существования конечных порождающих систем для ряда других семейств классов монотонных функций. В данной работе продолжены исследования в этом направлении.

Пусть $\preccurlyeq$ — частичный порядок на множестве $E_k = \{1, 2, \ldots, k\}$. Положим $\mathcal{P} = (E_k, \preccurlyeq)$. Будем считать, что множество $\mathcal{P}$ имеет наименьший и наибольший элементы. Через $\mathcal{M}_\mathcal{P}$ будем обозначать класс всех монотонных функций над $\mathcal{P}$ (отметим, что класс $\mathcal{M}_\mathcal{P}$ является предполным [7]).

Функцию $\lambda(x_0, x_1, \ldots, x_k)$ будем называть *функцией выбора*, если для каждого набора $(i, a_1, \ldots, a_k) \in \mathcal{P}^{k+1}$ выполняется равенство

$$\lambda(i, a_1, \ldots, a_k) = a_i.$$

Легко видеть, что если замкнутый класс функций k-значной логики содержит все константы $1, 2, \ldots, k$ и функцию выбора, то он является конечно-порожденным. Отметим также, что если $\mathcal{P}$ — частично упорядоченное множество, содержащее хотя бы одну цепь длины 2, то $\lambda(x_0, x_1, \ldots, x_k) \notin \mathcal{M}_\mathcal{P}$.

Положим

$$\mathcal{P}_\lambda = \{(a, b_1, \ldots, b_k) \in \mathcal{P}^{k+1} \mid \text{ если } i \preccurlyeq j, \text{ то } b_i \preccurlyeq b_j\}.$$

Легко видеть, что функция λ монотонна на множестве $\mathcal{P}_\lambda$. Назовем *монотонной функцией выбора* функцию $\nu(x_0, x_1, \ldots, x_k)$ из $\mathcal{M}_\mathcal{P}$, совпадающую на множестве $\mathcal{P}_\lambda$ с функцией $\lambda(x_0, x_1, \ldots, x_k)$. Нетрудно показать, что если

класс $\mathcal{M}_{\mathcal{P}}$ содержит монотонную функцию выбора, то он является конечнопорожденным.

Пусть a_1 и a_2 — элементы множества $\mathcal{P}$, не сравнимые относительно частичного порядка $\preccurlyeq$. Элемент $b \in \mathcal{P}$ называется *верхней гранью* элементов a_1 и a_2, если выполняется неравенство $a_1, a_2 \preccurlyeq b$. Верхняя грань b элементов a_1 и a_2 называется *минимальной верхней гранью* этих элементов, если не существует такой верхней грани c элементов a_1 и a_2, что $c \neq b$ и $c \preccurlyeq b$. Верхняя грань b элементов a_1 и a_2 называется *точной верхней гранью* этих элементов ($\sup(a_1, a_2)$), если для любой верхней грани c элементов a_1 и a_2 выполняется неравенство $b \preccurlyeq c$ Аналогичным образом определяется *нижняя, максимальная нижняя* и *точная нижняя грань* элементов a_1 и a_2 (точная нижняя грань обозначается через $\inf(a_1, a_2)$). Через $|\mathcal{P}|$ будем обозначать число элементов множества $\mathcal{P}$. Положим $w_{\mathcal{P}} = \max |J|$, где максимум берется по всем антицепям J множества $\mathcal{P}$; величину $w_{\mathcal{P}}$ будем называть *шириной* множества $\mathcal{P}$.

В работе [8] был получен следующий результат.

Теорема 1 [8]. *Пусть $\mathcal{P}$ — частично упорядоченное множество ширины два. Класс $\mathcal{M}_{\mathcal{P}}$ содержит монотонную функцию выбора тогда и только тогда, когда для любых элементов $a, b \in \mathcal{P}$ в $\mathcal{P}$ существует либо* $\sup(a, b)$, *либо* $\inf(a, b)$.

Основным результатом настоящей работы является частичное обобщение теоремы 1 на случай множеств произвольной ширины.

Теорема 2. *Пусть $\mathcal{P}$ — произвольное частично упорядоченное множество. Если класс $\mathcal{M}_{\mathcal{P}}$ содержит монотонную функцию выбора, то для любой пары несравнимых элементов a_1 и a_2 множества $\mathcal{P}$, таких что a_1 и a_2 не имеют в $\mathcal{P}$ точной верхней грани, и для любой верхней грани c элементов a_1 и a_2, не сравнимой с некоторой минимальной верхней гранью b этих элементов, в $\mathcal{P}$ существует* $\sup(b, c)$.

Отметим, что для частично упорядоченных множеств ширины два необходимые условия существования монотонной функции выбора, приведенные в теоремах 1 и 2, эквивалентны.

Работа выполнена при финансовой поддержке РФФИ, проект № 11-01-00508, и программы фундаментальных исследований Отделения математических наук РАН "Алгебраические и комбинаторные методы математической кибернетики и информационные системы нового поколения", проект "Задачи оптимального синтеза управляющих систем".

Список литературы

1. Lau D. Bestimmung der Ordnung maximaler Klassen von Funktionen der k-wertigen Logik // Z. math Log. und Grundl. Math. — 1978. — 24. — S. 79–96.
2. Tardos G. A not finitely generated maximal clone of monotone operations // Order. — 1986. — 3. — P. 211–218.

3. Дудакова О. С. О классах функций k-значной логики, монотонных относительно множеств ширины два // Вестн. Моск. ун-та. Серия 1. Математика. Механика. — 2008. — № 1. — С. 31–37.
4. Дудакова О. С. О конечной порожденности замкнутых классов монотонных функций в P_k // Учен. зап. Казан. ун-та. Серия Физ.-матем. науки. — 2009. — Т. 151, кн. 2. — С. 65–71.
5. Дудакова О. С. О конечной порожденности предполных классов монотонных функций девятизначной логики // Мат-лы XVIII Междунар. школы-семинара "Синтез и сложность управляющих систем" (Пенза, 28 сентября – 3 октября 2009 г.). — М.: Изд-во мех.-матем. ф-та МГУ. — 2009. — С. 38–41.
6. Дудакова О. С. О классах функций k-значной логики, монотонных относительно множеств ширины три // Мат-лы X Междунар. семинара "Дискретная математика и ее приложения" (Москва, МГУ, 1–6 февраля 2010 г.). — М.: Изд-во мех.-матем. ф-та МГУ. — 2010. — С. 178-180.
7. Мартынюк В. В. Исследование некоторых классов в многозначных логиках // Проблемы кибернетики. — М.: Наука. — 1960. — Т. 3. — С. 49–60.
8. Дудакова О. С. О порождающих системах специального вида для предполных классов монотонных функций k-значной логики // Мат-лы XVI Междунар. конф. "Проблемы теоретической кибернетики" (Нижний Новгород, 20–25 июня 2011 г.). — Нижний Новгород: Изд-во Нижегородского гос. ун-та. — 2011. — С. 145–147.

ОЦЕНКА ЧИСЛА ГРАФОВ В НЕКОТОРЫХ ПОДКЛАССАХ ДВУДОЛЬНЫХ ГРАФОВ

В. А. Замараев (Нижний Новгород)

Введение

В работе рассматриваются обыкновенные, помеченные графы с множеством вершин $\{1, \ldots, n\}$. Множество $\mathcal{X}$ называется *наследственным классом графов*, если любой граф, изоморфный порожденному подграфу графа из $\mathcal{X}$, также принадлежит $\mathcal{X}$. В [2] В. Е. Алексеев доказал, что для любого бесконечного наследственного класса графов $\mathcal{X}$, отличного от класса всех графов, справедливо следующее соотношение:

$$\log_2 |\mathcal{X}_n| = \left(1 - \frac{1}{c(\mathcal{X})}\right) \frac{n^2}{2} + o(n^2), \tag{1}$$

где $c(\mathcal{X})$ — натуральное число, называемое индексом класса $\mathcal{X}$, а $\mathcal{X}_n$ — множество всех n-вершинных графов из класса $\mathcal{X}$. Из (1) видно, что семейство

наследственных классов графов разбивается на счетное множество *слоев*, каждый из которых состоит из классов с определенным значением индекса. Множество классов с индексом, равным 1, образует *унитарный* слой. Для классов из этого слоя соотношение (1) не дает асимптотической оценки величины $\log_2 |\mathcal{X}_n|$, знание которой важно, например, при экономном кодировании графов из класса $\mathcal{X}$ [1]. Для исследования асимптотического поведения функции $\log_2 |\mathcal{X}_n|$ для классов из унитарного слоя В. Е. Алексеев ввел понятие равновеликости [3]. Два класса графов $\mathcal{X}$ и $\mathcal{Y}$ называются *равновеликими*, если существуют положительные числа c_1, c_2 и n_0 такие, что $|\mathcal{Y}_n|^{c_1} \leq |\mathcal{X}_n| \leq |\mathcal{Y}_n|^{c_2}$ для любого $n > n_0$. Равновеликость является отношением эквивалентности, а классы эквивалентности на множестве наследственных классов графов называются *ярусами*.

В [6] были выделены первые четыре яруса унитарного слоя, для которых $\log_2 |\mathcal{X}_n|$ по порядку совпадает с 1, $\log n$, n, $n \log n$, и показано, что никаких промежуточных типов поведения не существует. Эти ярусы называются константным, полиномиальным, экспоненциальным и факториальным соответственно. Независимо такой же результат был получен В. Е. Алексеевым [3]. Более того, для первых трех ярусов В. Е. Алексеев получил структурные описания и в каждом из четырех нашел все минимальные элементы. Факториальный ярус является наименьшим, для которого такой характеризации неизвестно. В то же время этому ярусу принадлежат многие классы, представляющие большой интерес с теоретической и практической точек зрения. Например, он содержит: реберные графы, интервальные графы, леса, планарные графы, кографы и др.

Классы графов, для которых функция $\log_2 |\mathcal{X}_n|$ растет быстрее чем $n \log n$, называются сверхфакториальными. Формально класс называется *сверхфакториальным*, если для любых положительных c и n_0 существует $n > n_0$, такое, что $|\mathcal{X}_n| > n^{cn}$.

Обозначим через $\mathcal{B}, \overline{\mathcal{B}}$ и $\mathcal{S}$ класс двудольных, кодвудольных и расщепляемых графов соответственно. Количество n-вершинных графов в каждом из этих классов равно $2^{\frac{n^2}{4}+o(n^2)}$ [2], и поэтому каждый них является сферхфакториальным. В настоящей работе рассматриваются два семейства наследственных подклассов класса двудольных графов и доказывается, что каждый из этих классов является не более чем факториальным. Интерес к подклассам двудольных графов вызван следующей гипотезой, предложенной в [5]:

Гипотеза. Наследственный класс $\mathcal{X}$ является факториальным тогда и только тогда, когда по крайней мере один из классов: $\mathcal{X} \cap \mathcal{B}$, $\mathcal{X} \cap \overline{\mathcal{B}}$ и $\mathcal{X} \cap \mathcal{S}$ является факториальным и каждый из этих классов не более чем факториальный.

В работе используется описание наследственных классов через множество запрещенных порожденных подграфов. Пусть M — множество графов, тогда через $Free(M)$ принято обозначать множество всех графов, не содержащих порожденных подграфов, изоморфных графам из M. Множество графов $\mathcal{X}$ является наследственным классом тогда и только тогда, когда $\mathcal{X} = Free(M)$ для некоторого M.

Используя общепринятую символику, через C_n и $K_{p,q}$ мы будем обозначать простой n-вершинный цикл и полный двудольный граф с p и q вершинами в каждой из долей соответственно. Через $T_{h,d}$ будем обозначать корневое дерево высоты h, в котором каждая вершина, находящаяся на расстоянии не более чем $h-1$ от корня, имеет ровно d потомков. Например, граф $T_{1,d}$ есть звезда с d листьями — $K_{1,d}$. Подграф графа G, порождаемый множеством вершин A, будем обозначать через $G[A]$.

1. Двудольные графы без порожденного C_4

Известно, что класс двудольных графов, не содержащих C_4 в качестве порожденного подграфа, является сверхфакториальным (см., например, [4]). Один из результатов данной работы говорит о том, что если кроме C_4 запретить еще и некоторый фиксированный лес, то такой подкласс двудольных графов становится не более чем факториальным. Для доказательства этого утверждения нам потребуется вспомогательная лемма.

Лемма 1. *Для любых $h \geq 1$, $d \geq 2$, всякий граф из класса $Free(C_4, T_{h,d}) \cap \mathcal{B}$ содержит вершину, степень которой не превосходит $c(h,d) = \frac{d^h-1}{d-1} + d - 2$.*

Доказательство. Докажем лемму по индукции по h. Для $h = 1$ лемма верна в силу того, что всякая вершина двудольного графа, не содержащего $K_{1,d}$, имеет степень не более $d-1$.

Предположим, что лемма верна для всех значений, меньших h, и для любого фиксированного $d \geq 2$. Рассмотрим произвольный граф G из класса $Free(C_4, T_{h,d}) \cap \mathcal{B}$. Мы можем считать, что G содержит порожденный $T_{h-1,d}$, иначе по предположению индукции в G была бы вершина, степень которой не превосходит $c(h-1,d) < c(h,d)$. Обозначим через $M \subseteq V(G)$ множество вершин, порождающих $T_{h-1,d}$ в G. Пусть $v \in M$ — корень этого дерева, а $D_k \in M$ — множество вершин, отстоящих от v на расстоянии k в $G[M]$. В частности, $D_0 = \{v\}$, а $D_k = \emptyset$, при $k \geq h$. Для $0 \leq k \leq h-1$, $|D_k| = d^k$, поэтому

$$|M| = \sum_{k=0}^{h-1} d^k = \frac{d^h - 1}{d-1}. \tag{2}$$

Предположим от противного, что каждая вершина графа G имеет степень не менее $c(h,d)+1 = \frac{d^h-1}{d-1} + d - 1$. Тогда любая вершина $u \in D_{h-1}$ имеет по крайней мере d соседних вершин, ни одна из которых не смежна ни с какой другой вершиной из M. Действительно, M содержит $\frac{d^h-1}{d-1} - 1$ вершин, отличных от u. Каждая из этих вершин может иметь не более одного общего соседа с u, иначе в графе найдется порожденный C_4. Обозначим через S_u множество вершин, смежных с u, но не смежных с другими вершинами из M. Объединение $S = \bigcup_{u \in D_{h-1}} S_u$ — подмножество одной из долей графа G, и поэтому является независимым множеством в G. Из этих рассуждений следует, что $M \cup S$ порождает запрещенное дерево $T_{h,d}$. Данное противоречие приводит

нас к заключению, что в G есть вершина, степень которой не превосходит $c(h,d)$.

Теорема 1. *Для любого леса F, класс $Free(C_4,F)\cap\mathcal{B}$ является не более чем факториальным.*

Доказательство. Заметим, что произвольный лес F является порожденным подграфом дерева $T_{h,d}$, для некоторых $h\geq 1$ и $d\geq 2$. Очевидно, что для таких h и d класс $Free(C_4,F)\cap\mathcal{B}$ является подклассом $Free(C_4,T_{h,d})\cap\mathcal{B}$. Таким образом, для доказательства теоремы достаточно получить верхнюю факториальную оценку числа n-вершинных графов в классе $Free(C_4,T_{h,d})\cap\mathcal{B}$.

Из леммы 1 следует, что в любом n-вершинном графе из наследственного класса $Free(C_4,T_{h,d})\cap\mathcal{B}$ число ребер не превосходит cn, где $c=c(h,d)$. Поэтому число n-вершинных графов в этом классе не превосходит

$$\sum_{i=0}^{cn}\binom{\binom{n}{2}}{i}\leq\sum_{i=0}^{cn}n^{2i}\leq cn^{2cn+1}+1\leq n^{dn},$$

где d — некоторая константа, не зависящая от n. Теорема доказана.

2. Хордальные двудольные графы

В предыдущем разделе мы рассмотрели класс двудольных графов, у которых запрещен цикл C_4, но допускаются любые другие порожденные циклы четной длины: $C_6, C_8, C_{10}, \ldots$. Рассмотрим теперь класс двудольных графов, у которых C_4 разрешен, а все остальные циклы запрещены, то есть класс $\mathcal{CB}=Free(C_6,C_8,C_{10},\ldots)\cap\mathcal{B}$. Это класс так называемых хордальных двудольных графов. Известно [7], что он является сферхфакториальным. Заметим, что если в классе хордальных двудольных графов запретить порожденный цикл $C_4=K_{2,2}$, то мы получим класс лесов, который является факториальным. Еще одним результатом данной работы является обобщение этого факта на случай произвольного полного двудольного графа с не менее чем 3 вершинами. А именно справедлива следующая теорема, приводимая здесь без доказательства.

Теорема 2. *Для любых натуральных p,q таких, что $p+q\geq 3$, класс $Free(K_{p,q})\cap\mathcal{CB}$ является факториальным.*

Список литературы

1. Алексеев В. Е. Наследственные классы и кодирование графов // В сб. Проблемы кибернетики. вып. 39. Под ред. С. В. Яблонского — М.: Наука. — 1982. — С. 151–164.
2. Алексеев В. Е. Область значений энтропии наследственных классов графов // Дискретная Математика. — 1992. — Т. 4, вып. 2. — С. 148–157.

3. Алексеев В. Е. О нижних ярусах решетки наследственных классов графов // Дискрет. анализ и исслед. операций. — 1997. — Серия 1, Т. 4. — С. 3–12.
4. Allen P. Forbidden induced bipartite graphs // Journal of Graph Theory. — 2009. — V. 60, I. 3. — P. 219–241.
5. Lozin V., Mayhill C., Zamaraev V. A note on the speed of hereditary graph properties // Electronic J. Combinatorics. — 2011. — V. 18, I. 1. — Research paper 157
6. Scheinerman E. R., Zito J. On the size of hereditary classes of graphs // J. Comb. Theory. — 1994. — V. 61, Ser. B. — P. 16–39.
7. Spinrad J. P. Nonredundant 1's in Γ-free matrices // SIAM J. Discrete Math.. — 1995. — V. 8. — P. 251–257.

О НАДЕЖНОСТИ СХЕМ В БАЗИСАХ, СОДЕРЖАЩИХ КОНСТАНТУ 1 И ФУНКЦИЮ ВИДА $x_1(x_2 \oplus x_3 \oplus c)$

Д. М. Клянчина (Пенза)

Введение

Рассматривается реализация булевых функций схемами из ненадежных функциональных элементов [1] в полном конечном базисе B, содержащем константу 1 и функцию вида $x_1(x_2 \oplus x_3 \oplus c)$ $(c \in \{0,1\})$. Считаем, что схема реализует булеву функцию $f(x_1,\ldots,x_n)$ $(n \geq 1)$, если при поступлении на входы схемы двоичного набора $\tilde{a} = (a_1,\ldots,a_n)$ при отсутствии неисправностей на выходе схемы появляется значение $f(\tilde{a})$. Допустим, что все элементы схемы независимо друг от друга с вероятностью ε $(0 < \varepsilon < 1/2)$ переходят в неисправные состояния типа 0 на выходах. Эти неисправности характеризуются тем, что в исправном состоянии функциональный элемент реализует приписанную ему булеву функцию, а в неисправном — константу 0.

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

Далее докажем, что в рассматриваемых базисах все булевы функции можно реализовать схемами, которые функционируют с ненадежностью, не больше $2\varepsilon + 149\varepsilon^2$ при $\varepsilon \in (0, 1/960]$, в то время как в тех же базисах при инверсных неисправностях на выходах элементов [3] — не больше $3\varepsilon + 293\varepsilon^2$ при $\varepsilon \in (0, 1/960]$.

1. Вспомогательные утверждения

В работе [2] введено множество G_1 — функций вида $x_1^{\sigma_1}x_2^{\sigma_2}\vee x_1^{\sigma_1}x_3^{\sigma_3}\vee x_2^{\sigma_2}x_3^{\sigma_3}$, $\sigma_i\in\{0,1\},\ i\in\{1,2,3\}$.

Обозначим через f^σ функцию f, если $\sigma=1$ и функцию $\bar{f}$, если $\sigma=0$; схему, реализующую функцию f^σ ($\sigma\in\{0,1\}$), будем обозначать S^σ.

Пусть функция $g\in G_1$ (т. е. функция g имеет вид $x_1^{\sigma_1}x_2^{\sigma_2}\vee x_1^{\sigma_1}x_3^{\sigma_3}\vee x_2^{\sigma_2}x_3^{\sigma_3}$, $\sigma_i\in\{0,1\},\ i\in\{1,2,3\}$), а схема S_g реализует функцию g. Возьмем схемы S^{σ_i}, реализующие соответственно функции $f^{\sigma_i},\ i\in\{1,2,3\}$. Соединим выход схемы S^{σ_i} с i-м входом схемы S_g ($i\in\{1,2,3\}$), построенную схему обозначим $\Phi(S^1,S^0)$. Нетрудно проверить, что схема $\Phi(S^1,S^0)$ реализует функцию f. Далее схему S^1 будем обозначать S.

Операция Φ по схемам S и S^0, реализующим булевы функции f и $\bar{f}$ соответственно, строит схему $\Phi(S,S^0)$, реализующую функцию f. Результат n-кратного применения ($n\in\mathbf{N}$) операции Φ к схемам S^1 и S^0 будем обозначать $\Phi^n(S,S^0)$. Применение операции Φ к некоторым схемам S и S^0 при некоторых условиях на их ненадежности $P(S)$ и $P(S^0)$ приводит к схемам, имеющим более высокую надежность, чем исходная схема S. В том случае, когда операция Φ применяется только к схемам S (т. е. когда все числа $\sigma_i=1$), результат ее применения будем обозначать $\Phi(S)$. Если же операция Φ применяется только к схемам S^0 (т. е. когда все числа $\sigma_i=0$), результат ее применения будем обозначать $\Phi(S^0)$.

Лемма 1 [1]. *Допустим, что произвольную функцию f можно реализовать схемой S с ненадежностью не больше p ($p\le 1/2$). Пусть S_g — схема, реализующая функцию $g\in G_1$ с ненадежностью $P(S_g)$ ($P(S_g)\le 1/2$), причем v_0 и v_1 — вероятности ошибок схемы S_g на наборах $(\sigma_1,\sigma_2,\sigma_3)$ и $(\bar\sigma_1,\bar\sigma_2,\bar\sigma_3)$ соответственно. Тогда схема $\Phi(S,S^0)$ реализует функцию f с ненадежностью $P(\Phi(S,S^0))\le\max\{v_0,v_1\}+3pP(S_g)+3p^2$.*

Лемма 2 [2]. *Любую булеву функцию f можно реализовать такой схемой S, что при всех $\varepsilon\in(0,1/960]$ верно неравенство $P(S)\le 5,2\varepsilon$.*

Пусть Ψ — множество функций, конгруэнтных одной из функций $x_1^{\sigma_1}x_2^{\sigma_2}$, $x_1^{\sigma_1}x_2^{\sigma_2}x_3^{\sigma_3}$, $x_1^{\sigma_1}(x_2^{\sigma_2}x_3^{\sigma_3}\vee x_2^{\bar\sigma_2}x_3^{\bar\sigma_3})$, $x_1^{\sigma_1}(x_2^{\sigma_2}\vee x_3^{\sigma_3})$, $\sigma_1,\sigma_2,\sigma_3\in\{0,1\}$.

Лемма 3 [3]. *Пусть $\phi\in\Psi$. Тогда подстановкой переменных из ϕ можно получить функцию $x_1^ax_2^b$ ($a,b\in\{0,1\}$).*

Лемма 4 [4]. *Пусть схема S_φ реализует функцию $\varphi=x_1^{a_1}x_2^{a_2}\oplus x_3^{a_3}$ ($a_i\in\{0,1\},i\in\{1,2,3\}$) с ненадежностью $P(S_\varphi)$, причем w_0,w_1 — вероятности ошибок схемы S_φ на наборах $(\bar a_1,\bar a_2,0),(\bar a_1,\bar a_2,1)$. Тогда можно построить схему S_g, реализующую функцию $g(x_1,x_2,x_3)=(x_1x_2\vee x_1x_3\vee x_2x_3)^{a_3}$, такую, что $P(S_g)\le P(S_\varphi)+2p_\oplus$ ($p_\oplus=\max\{P(S_1),P(S_2)\}$, S_1 — любая схема, реализующая функцию $x_1\oplus x_2$, S_2 — любая схема, реализующая функцию $x_1\oplus x_2\oplus 1$ в рассматриваемом базисе), а для вероятностей ошибок v_1 и v_0 схемы S_g на наборах $(0,0,0)$ и $(1,1,1)$ выполняются неравенства: $v_1,v_0\le\max\{w_0,w_1\}+2p_\oplus^2$.*

2. Основной результат

Теорема 1. *Пусть полный конечный базис B содержит константу 1 и функцию, конгруэнтную функции вида $\psi = x_1(x_2 \oplus x_3 \oplus c)$ $(c \in \{0,1\})$. Тогда произвольную булеву функцию f в базисе B можно реализовать такой схемой C, что при всех $\varepsilon \in (0, 1/960]$ верно неравенство $P(C) \le 2\varepsilon + 149\varepsilon^2$.*

Доказательство. Пусть полный базис B содержит константу 1 и функцию, конгруэнтную функции вида $\psi(x_1, x_2, x_3) = x_1(x_2 \oplus x_3 \oplus c)$ $(c \in \{0,1\})$. К функции $\psi = x_1(x_2 \oplus x_3 \oplus c)$ $(c \in \{0,1\})$ применима лемма 3, по которой из функции $\psi \in \Psi$ подстановкой переменных можно получить функцию $\varphi'(z_1, z_2) = z_1^a z_2^b (a, b \in \{0,1\})$. Некоторую функцию $\phi(x_1, x_2, x_3)$ вида $\phi(x_1, x_2, x_3) = x_1^{c_1} x_2^{c_2} \oplus x_3^{c_3}$ $(c_1, c_2, c_3 \in \{0,1\})$ реализуем схемой A следующим образом.

Промоделируем формулу $\psi(1, \varphi'(z_1, z_2), x_3)$ и построим схему A из трех элементов. Нетрудно видеть, что $\psi(1, \varphi'(z_1, z_2), x_3) = z_1^a z_2^b \oplus x_3 \oplus c = z_1^a z_2^b \oplus x_3^{\bar{c}}$, т. е. $c_1 = a, c_2 = b, c_3 = \bar{c}$. Вычислим вероятности ошибок w_0 на наборе $(\bar{a}, \bar{b}, 0)$ и w_1 на наборе $(\bar{a}, \bar{b}, 1)$ на выходе схемы A. Получим $w_0 \le 2\varepsilon$ и $w_1 = 0$. Следовательно, $\max\{w_0, w_1\} \le 2\varepsilon$.

По условию B — полный базис, следовательно, $(x_1 \oplus x_2)^{\bar{a}}$, $(x_1 \oplus x_3)^{\bar{b}} \in [B]$. По лемме 2 реализуем эти функции такими схемами S_1 и S_2 соответственно, что $P(S_1) \le 5,2\varepsilon$ и $P(S_2) \le 5,2\varepsilon$ при всех $\varepsilon \in (0, 1/960]$.

Нетрудно проверить, что

$$\phi((x_1 \oplus x_2)^{\bar{a}}, (x_1 \oplus x_3)^{\bar{b}}, x_1) = (x_1x_2 \vee x_1x_3 \vee x_2x_3)^c = g \in G_1.$$

Моделируя формулу $\phi((x_1 \oplus x_2)^{\bar{a}}, (x_1 \oplus x_3)^{\bar{b}}, x_1)$, построим схему S_g, реализующую функцию $g \in G_1$. Очевидно, что $P(S_g) \le 2\varepsilon + 2 \cdot 5,2\varepsilon = 12,4\varepsilon$. С помощью леммы 3 оценим вероятности ошибок v_0 и v_1 схемы S_g на наборах $(0,0,0)$ и $(1,1,1)$ соответственно: $v_0, v_1 \le \max\{w_0, w_1\} + 2p_\oplus^2 \le 2\varepsilon + 2(5,2\varepsilon)^2 \le 2\varepsilon + 54,1\varepsilon^2$.

По лемме 2 произвольную булеву функцию f можно реализовать схемой S с ненадежностью $P(S) \le 5,2\varepsilon$ при всех $\varepsilon \in (0, 1/960]$.

1. Если $c = 1$, то возьмем три экземпляра схемы S, реализующей функцию f. Используя три экземпляра схемы S и схему S_g, построим схему $\Phi(S)$, которая реализует функцию f. Оценим ненадежность схемы $\Phi(S)$, используя лемму 1 и полагая $p = 5,2\varepsilon$. Получим неравенство

$$\begin{aligned} P(\Phi(S)) &\le \max\{v_0, v_1\} + 3pP(S_g) + 3p^2 \le \\ &\le 2\varepsilon + 54,1\varepsilon^2 + 3(5,2\varepsilon) \cdot 12,4\varepsilon + 3(5,2\varepsilon)^2 \le 2\varepsilon + 328,66\varepsilon^2 \le 2,34\varepsilon \end{aligned}$$

при $\varepsilon \in (0, 1/960]$.

По схеме $\Phi(S)$ построим схему $\Phi^2(S)$. По лемме 1 оценим ненадежность схемы $\Phi^2(S)$. Получим

$$P(\Phi^2(S)) \le 2\varepsilon + 54,1\varepsilon^2 + 3(2,34\varepsilon) \cdot 12,4\varepsilon + 3(2,34\varepsilon)^2 \le 2\varepsilon + 157,58\varepsilon^2 \le 2,16\varepsilon$$

при всех $\varepsilon \in (0, 1/960]$.

По схеме $\Phi^2(S)$ построим схему $\Phi^3(S)$. По лемме 1 оценим ненадежность схемы $\Phi^3(S)$. Получим

$$P(\Phi^3(S)) \le 2\varepsilon + 54,1\varepsilon^2 + 3(2,16\varepsilon)\cdot 12,4\varepsilon + 3(2,16\varepsilon)^2 \le 2\varepsilon + 149\varepsilon^2.$$

Схема $\Phi^3(S) = C$ — искомая.

2. Если $c = 0$, то возьмем три экземпляра схемы S^0, реализующей функцию $\bar{f}$. Используя три экземпляра схемы S^0 и схему S_g, построим схему $\Phi(S^0)$, которая реализует функцию f. Оценим ненадежность схемы $\Phi(S^0)$, используя лемму 1. Получим неравенство

$$\begin{aligned} P(\Phi(S^0)) &\le \max\{v_0, v_1\} + 3pP(S_g) + 3p^2 \le \\ &\le 2\varepsilon + 54,1\varepsilon^2 + 3(5,2\varepsilon)\cdot 12,4\varepsilon + 3(5,2\varepsilon)^2 \le 2\varepsilon + 328,66\varepsilon^2 \le 2,34\varepsilon \end{aligned}$$

при $\varepsilon \in (0, 1/960]$.

По схеме $\Phi(S^0)$ построим схему $\Phi^2(S^0)$. По лемме 1 оценим ненадежность схемы $\Phi^2(S^0)$. Получим

$$P(\Phi^2(S^0)) \le 2\varepsilon + 54,1\varepsilon^2 + 3(2,34\varepsilon)\cdot 12,4\varepsilon + 3(2,34\varepsilon)^2 \le 2\varepsilon + 157,58\varepsilon^2 \le 2,16\varepsilon$$

при всех $\varepsilon \in (0, 1/960]$.

По схеме $\Phi^2(S^0)$ построим схему $\Phi^3(S^0)$. По лемме 1 оценим ненадежность схемы $\Phi^3(S^0)$. Получим

$$P(\Phi^3(S^0)) \le 2\varepsilon + 54,1\varepsilon^2 + 3(2,16\varepsilon)\cdot 12,4\varepsilon + 3(2,16\varepsilon)^2 \le 2\varepsilon + 149\varepsilon^2.$$

Схема $\Phi^3(S^0) = C$ — искомая. Теорема доказана.

Работа выполнена при финансовой поддержке РФФИ, номер проекта 11-01-00212а.

Список литературы

1. Алехина М. А. Синтез асимптотически оптимальных по надежности схем (монография). — Пенза: информац.-издат. центр ПГУ, 2006. — 156 с.
2. Алехина М. А., Васин А. В. О надежности схем в базисах, содержащих функции не более чем трех переменных // Ученые записки Казанского государственного университета. Серия "Физико-математические науки". — 2009. — Т. 151, вып. 2. —С. 25–35.
3. Васин А. В. Асимптотически оптимальные по надежности схемы в полных базисах из трехвходовых элементов. — Дисс. ... кандидата физ.-мат. наук. — Пенза, 2010. — 100 с.
4. Алехина М. А., Клянчина Д. М. Достаточные условия реализации булевых функций асимптотически оптимальными схемами с тривиальной оценкой ненадежности // Труды международного симпозиума "Надёжность и качество, 2010" (Пенза, 24–31 мая 2010 г.). — Пенза: ИИЦ ПГУ, 2010. — Том 1. —С. 229–232.

О СИНТЕЗЕ СХЕМ ОГРАНИЧЕННОЙ ШИРИНЫ

В. А. Коноводов (Москва)

Рассматриваются (см., например, [5]) схемы из функциональных элементов в произвольном полном базисе Б. Под сложностью $L_{\text{Б}}(S)$ схемы S в базисе Б понимается число функциональных элементов в ней. Сложность функции алгебры логики f, т. е. минимальную из сложностей реализующих ее схем, будем обозначать через $L_{\text{Б}}(f)$, при этом соответствующую схему будем называть минимальной. В случае стандартного базиса Б_0, состоящего из функциональных элементов $\&$, $\vee$, и $\neg$, реализующих функции $x_1 \cdot x_2$, $x_1 \vee x_2$ и $\bar{x}_1$ соответственно, индекс Б_0 будет опускаться. При этом, как обычно, формулами называются те одновыходные схемы, у которых выход любого элемента либо поступает на вход одного (другого) элемента, либо является выходом схемы.

Определим понятие схемы с t, $t \in \{1, 2, \ldots\}$, регистрами. Пусть Σ — схема из функциональных элементов сложности L, все ее элементы занумерованы числами от 1 до L, и каждому элементу приписан символ из множества $R = \{r_1, \ldots, r_t\}$. Это приписывание означает, что результат выполнения операции в каждом элементе записывается в некоторый регистр с именем, которое совпадает с приписанным этому элементу символом. При этом каждый элемент берет в качестве входных значений соответствующие значения булевых переменных, подающиеся ему на вход, и значения из регистров, приписанных элементам, выходы которых являются его входами. „Срабатывания“ элементов происходят в порядке их нумерации. Элемент с номером L является выходом схемы, и результат операции в нем также записывается в один из регистров (возможно, использованный ранее), который объявляется выходным. Для корректности этой процедуры необходимо выполнение следующих условий для каждого элемента $\mathcal{E}$ схемы Σ:

1. Все элементы, выходы которых подаются на вход $\mathcal{E}$, имеют разные приписанные символы из R.

2. $\mathcal{E}$ имеет номер больший, чем те элементы, выходы которых подаются на его вход.

3. Если на вход элемента $\mathcal{E}$ с номером j, $j \in [2, L]$, подается выход элемента $\mathcal{E}'$ с номером i, $i \in [1, j-1]$, и приписанным регистром r, $r \in R$, то элементам с номерами из интервала (i, j) регистр r не приписан.

Более строгое определение и формальное построение схем с t регистрами приводится в [2].

Для схемы Σ с t, $t \in \{1, 2, \ldots\}$, регистрами число t будем называть шириной схемы Σ.[1] Для произвольной функции алгебры логики f и для любого t, $t \in \{1, 2, \ldots\}$, определим сложность $L^{(t)}_{\text{Б}}(f)$ функции f как минимальную из

[1] В работе [2] величина t называется толщиной схемы.

сложностей тех реализующих её схем в базисе Б, ширина которых не превосходит t.

В работе [3] рассматривались схемы ширины 1 — линейные суперпозиции. В отличие от них, любая функция может быть реализована схемой ширины 2 (см., например, [4, Гл. 2, § 4]). В [2] показано, что функция Шеннона (т. е. сложность самой сложной функции) для класса схем произвольной константной ширины t, $t \geqslant 3$, асимптотически равна $c_{\text{Б}} \frac{2^n}{\log_2 n}$, где $c_{\text{Б}}$ — константа, зависящая от базиса. В данной работе рассматриваются схемы ограниченной ширины в базисах Б_0 и $\{\&, \vee\}$ и исследуется существенность ослабления ограничения на ширину схемы с 2 до 3. Показывается, что ограничение ширины до 2 может менять сложность отдельных функций по порядку по сравнению с ограничением ширины до 3. Приводятся примеры схем ограниченной ширины, являющихся оптимальными в схемах без ограничений. Кроме того, приводится общая структура минимальных схем ширины 2.

Схемы с двумя регистрами

Покажем, что существуют функции, допускающие оптимальную реализацию в классе схем ширины 2, а именно линейная функция $l_n = x_1 \oplus \ldots \oplus x_n$ и её отрицание в классе схем над Б_0.

Утверждение 1. *Для любого n, $n \geqslant 2$, справедливо:*

$$L^{(2)}(l_n) = L^{(2)}(\bar{l}_n) = 4n - 4.$$

Доказательство. Нижняя оценка следует из нижней оценки в классе схем без ограничений [7]. Верхняя оценка доказывается построением оптимальных схем. На рис. 1 приведен сумматор порядка 2 с распределением регистров и нумерацией вершин. Используя суперпозицию таких блоков (и аналогичных для $\bar{l}_n$), естественным образом строятся схемы для линейных функций с указанной сложностью.

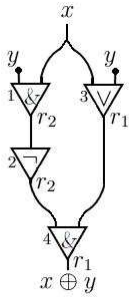

Рис. 1: Основной блок для l_n.

Лемма 1. *Пусть* Σ *— схема из функциональных элементов в базисе* $Б_0$ *с двумя регистрами, являющаяся минимальной для некоторой функции алгебры логики* f. *Тогда число исходящих дуг у любого функционального элемента схемы* Σ *не превосходит* 2.

На основе этой леммы можно показать, что любая схема ширины 2 в базисе $\{\&, \vee\}$ или в базисе $Б_0$, являющаяся минимальной для некоторой функции, представляет собой цепь из последовательно соединенных блоков, каждый из которых может быть одним из блоков, представленных на рис. 2, с точностью до замены имен регистров и сдвига нумерации.

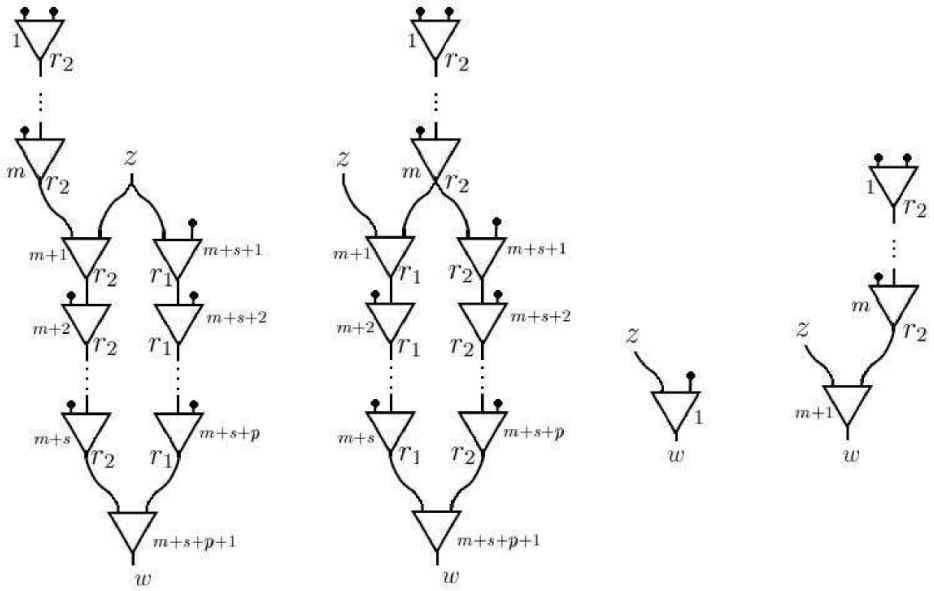

Рис. 2: Блоки схем ширины 2.

Жирными точками на рисунке показаны входы блоков, подсоединяемые к входам схемы, z и w — вход и выход блока соответственно, через которые блоки соединяются в цепь, они могут являться входом или выходом схемы соответственно. При этом для первого блока слева $m \geqslant 0$, $s \geqslant 1$, $p \geqslant 1$, для второго блока — $m \geqslant 1$, $s \geqslant 1$, $p \geqslant 1$, а для последнего — $m \geqslant 1$. В случае стандартного базиса общий вид блоков изменится только удалением некоторых входов соответствующих элементов.

Ни схемы ширины 1, ни формулы не могут иметь в качестве подсхем первые два блока на рис. 2. Такого вида подсхемы позволяют уменьшить сложность многих функций по сравнению с их сложностью в классе формул, примером этому является утверждение 1. Однако, ограничение ширины схемы до 2 является достаточно сильным, что подтверждают рассуждения ниже.

Сложность монотонной симметрической функции с порогом 2 и дешифратора

Рассмотрим монотонную симметрическую функцию с порогом 2:

$$s_n(x_1,\ldots,x_n)=\bigvee_{1\leqslant i<j\leqslant n}x_ix_j.$$

В работе [1] доказано, что сложность реализации этой функции в классе схем из функциональных элементов в базисе $\{\&,\vee\}$ без ограничений асимптотически равна $2n$. Кроме того, в [4] установлено, что в классе π-схем сложность этой функции асимптотически равна $n\log_2 n$.

Теорема 1.

$$L^{(2)}_{\{\&,\vee\}}(s_n)\asymp n\log_2 n.$$

В доказательстве этой теоремы устанавливается, что любая схема ширины 2 в базисе $\{\&,\vee\}$ для некоторой функции f имеет сложность не меньшую, чем $\frac{1}{2}L^{\Phi}(f)$, где $L^{\Phi}(f)$ — сложность функции f в классе формул.

Ослабление ограничения ширины с 2 до 3 позволяет добиться линейной сложности для этой функции, т. е. оптимальной по порядку.

Утверждение 2. *Для любого* n, $n\geqslant 2$, *справедлива оценка*

$$L^{(3)}_{\{\&,\vee\}}(s_n)\leqslant 3n-5.$$

Это утверждение доказывается построением схемы, в которой элементы с номерами $1,4,7,10,\ldots,3n-5$ реализуют функции $s_2,s_3,s_4,s_5,\ldots,s_n$ соответственно. Заметим, что применение конструкции, предложенной в работе [1], здесь невозможно, так как соответствующая схема не является схемой константной ширины.

Система функций Q_n, $Q_n=\{\bar{x}_1\cdots\bar{x}_{n-1}\bar{x}_n,\bar{x}_1\cdots\bar{x}_{n-1}x_n,\ldots,x_1\cdots x_{n-1}x_n\}$, состоящая из всех элементарных конъюнкций ранга n, называется дешифратором порядка n. Известно (см., например, [5]), что его сложность[2] в классе схем из функциональных элементов в стандартном базисе без ограничений асимптотически равна 2^n. Можно показать, что ограничение ширины до 3 не изменит эту асимптотику[3].

Теорема 2.

$$L^{(3)}(Q_n)\sim 2^n.$$

Это утверждение доказывается с использованием техники разбиений булева куба на регулярные компоненты [6]. С помощью усложнения применяемого метода можно доказать следующую оценку.

[2] Под сложностью системы функции F понимается минимальная сложность схемы с $|F|$ выходами, реализующей систему F.

[3] В схемах ограниченной ширины с m, $m>1$, выходами выделены m элементов $\mathcal{E}_1,\ldots,\mathcal{E}_m$ и имеются m дополнительных выходных регистров $r'_1,\ldots,r'_m\notin R$. После срабатывания $\mathcal{E}_i$, $i=1,\ldots,m$, в регистр r'_i записывается значение из регистра, приписанного элементу $\mathcal{E}_i$. Кроме того, значения в выходных регистрах не могут подаваться на входы элементов схемы.

Утверждение 3.

$$L^{(2)}(Q_n) = O(2^n).$$

Список литературы

1. Гринчук М. И. О монотонной сложности пороговых функций // Методы дискретного анализа в синтезе управляющих систем. — 1992. — Вып. 52. — С. 41–48.
2. Карпова Н. А. О вычислениях с ограниченной памятью // Математические вопросы кибернетики. — 1989. — Вып. 2. — С. 131–144.
3. Карпова Н. А. О сложности представлений функций алгебры логики линейными суперпозициями // Методы дискретного анализа в теории графов и логических функций. — 1986. — Вып. 43. — С. 40–46.
4. Кричевский Р. Е. Минимальная схема из замыкающих контактов для одной булевой функции от n аргументов // Методы дискретного анализа в синтезе управляющих систем. — 1965. — Вып. 5. — С. 89–92.
5. Ложкин С. А. Лекции по основам кибернетики: Учебное пособие. — М.: Издательский отдел Факультета ВМиК МГУ им. М. В. Ломоносова, 2004.
6. Ложкин С. А. О синтезе формул, сложность и глубина которых не превосходят асимптотически наилучшие оценки высокой степени точности // Вестник Московского университета. Сер. 1. Математика. Механика. — 2007. — № 3. — С. 19–25.
7. Редькин Н. П. Доказательство минимальности некоторых схем из функциональных элементов // Проблемы кибернетики. — 1970. — Вып. 23. — С. 83–102.

НАДСТРУКТУРА КЛАССОВ КВАЗИСАМОДВОЙСТВЕННЫХ ФУНКЦИЙ

В. Б. Ларионов, В. С. Федорова (Москва)

Обозначим через E_k множество $\{0, 1, \ldots, k-1\}$. Функция $f(x_1, \ldots, x_n)$ называется *функцией k-значной логики* ($k \geqslant 2$), если она определена на E_k^n и все ее значения принадлежат E_k.

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

Яновым и Мучником в [7] было показано, что при $k \geqslant 3$ множество всех замкнутых классов функций из P_k имеет мощность континуум. В связи с этим особенный интерес представляет изучение именно фрагментов решетки замкнутых классов функций из P_k.

Для данного класса A *надструктурой* будем называть множество классов, строго содержащих класс A.

Ранее авторами была полностью описана надструктура замкнутых классов самодвойственных функций [3], которые по своим свойствам близки к предполным классам [5]. В данной работе рассматривается новое семейство квазисамодвойственных функций и строится их надструктура, конечность которой была доказана одним из авторов в работе [2].

Пусть $p(x_1, \ldots, x_m)$ – некоторый предикат, определенный на множестве E_k^m, $f(y_1, \ldots, y_n)$ — функция из P_k. Будем говорить, что *функция f сохраняет предикат p*, если для любых n наборов $\tilde{a}_i = (a_{i1}, \ldots, a_{im})$, $i \in \{1, \ldots, n\}$, удовлетворяющих предикату p, набор $f(a_{11}, \ldots, a_{n1}), \ldots, f(a_{1m}, \ldots, a_{nm})$ также удовлетворяет предикату p. По определению будем считать, что тождественно ложный предикат сохраняет любая функция.

Обозначим через $\mathrm{Pol}(p)$ множество функций, сохраняющих предикат p. Для произвольного множества функций A через $\mathrm{Inv}A$ обозначим множество предикатов, каждый из которых сохраняет любая функция из A.

На множестве предикатов вводятся следующие операции: отождествление переменных, конъюнкция, добавление квантора существования по какой-либо переменной (проекция). Для произвольного множества предикатов P через $[P]$ будем обозначать его замыкание относительно указанных операций. Подробное определение этих операций можно найти в [1] и [4].

Лемма 1 [1]. *Если $p_1 \in [p_2]$, то* $\mathrm{Pol}(p_2) \subseteq \mathrm{Pol}(p_1)$.

Лемма 2 [6]. *Пусть $p = p_1 \& \ldots, \& p_m$, где предикаты $p_1, \ldots, p_m$ не имеют общих переменных. Тогда*

$$\mathrm{Pol}p = \bigcap_{i=1}^{m} \mathrm{Pol}p_i.$$

Пусть A и B — произвольные непустые подмножества E_k, имеющие равную мощность. Обозначим через F_{AB} множество всех различных взаимнооднозначных отображений множества A во множество B, а через F_k — объединение множеств F_{AB} для всевозможных пар подмножеств A и B указанного вида. Для $f \in F_{AB}$ обозначим $D_f = A$, $T_f = A \bigcup B$.

Для произвольного отображения $f \in F_k$ обозначим через $R_f(x_1, x_2)$ предикат, истинный на всех парах $(a, f(a))$, где $a \in D_f$, и только на них.

Замкнутые классы функций $S_f = \mathrm{Pol}(R_f)$, где $f \in F_k$, $D_f \subseteq E_k$, будем называть *классами квазисамодвойственных функций*, а сами функции, входящие в указанные классы, — *квазисамодвойственными функциями*.

Отметим, что, если в последнем определении положить $D_f = E_k$, мы получим определение самодвойственных функций [5], а если $f(a) = a$ для любого $a \in D_f$ и $D_f \subset E_k$, то S_f — предполный центральный класс [6].

Для произвольного отображения $f \in F_k$ обозначим через $L_1(f)$ множество элементов $a \in E_k$ таких, что $a \in D_f$, и существует число n такое, что справедливо $f^n(a) = a$. Пусть $L_2(f) = T_f \setminus L_1(f)$.

Пусть предикат p реализуется над $\{R_f\}$ формулой F. Везде далее будем считать, что в формуле F вынесены вперед все кванторы существования. Сопоставим F ориентированный граф $G(F)$ по следующему правилу: между множеством вершин $G(F)$ и множеством переменных F (учитываем и свободные и связанные) существует взаимно однозначное соответствие. Вершину, соответствующую переменной x, пометим символом "x", если переменная x свободная и "$\exists x$", если связанная, и будем обозначать v_x. В графе $G(F)$ есть ориентированное ребро (v_x, v_y) тогда и только тогда, когда в формуле F содержится запись $R_f(y, x)$.

Отметим, что по графу формулы $G(F)$ формула F с вынесенными вперед кванторами существования восстанавливается однозначно.

Путем из вершины v_1 в вершину v_2 в ориентированном графе G будем называть любую последовательность ребер вида $\{(v_1, w_1), (w_1, w_2), (w_2, w_3), \ldots, (w_m, v_2)\}$ (вершины и ребра в последовательности могут повторяться). Ориентация ребер указанной последовательности может быть любая. *Замкнутым путем* называется путь, в котором первая и последняя вершины совпадают. *Простым циклом* называется замкнутый путь, в котором каждая вершина (кроме первой и последней) встречается не более одного раза. *Длиной пути* будем называть разность количества ребер, пройденных в прямом направлении, и количества ребер, пройденных в обратном.

Обозначим через $c(G)$ наибольший общий делитель длин всех простых циклов графа G. Если в G нет циклов, положим $c(G) = 0$.

Лемма 3 [3]. *Пусть в связном орграфе G из вершины v в вершину w существует путь длины l. Тогда любой путь из вершины v в вершину w имеет длину $l + \alpha c(G)$, где α — некоторое целое число.*

Обозначим через $d(v, w)$ минимальное по модулю расстояние в графе G от вершины v до вершины w.

Пусть снова предикат p реализуется над $\{R_f\}$ формулой F со связным графом G_F. Пусть $y_1, \ldots, y_N$ — все переменные формулы F, первые n из которых являются свободными (обозначим их $x_1, \ldots, x_n$), $d(v_{y_i}, v_{y_j}) = d_{i,j}$. Для произвольной вершины v_y обозначим

$$d_p(y) = \max_{w \in G(F)} d(v_y, w), \quad d_n(y) = \min_{w \in G(F)} d(v_y, w),$$

$$D(v_y) = \{a \in E_k : \exists f^{d_p(y)}(a), f^{-d_n(y)}(a)\}.$$

Обозначим также множество $M_c = \{a \in E_k : f^c(a) = a\}$. Докажем основную лемму, являющуюся обобщением леммы из [3].

Лемма 4. *Пусть G_F — связный граф. Тогда $p(\tilde{a}) =$ TRUE тогда и только тогда, когда для любого $i \in \{1, \ldots, n\}$ справедливо $a_i \in M_{c(G_F)} \bigcap D(v_{x_i})$, $a_j = f^{d_{i,j}}(a_i)$ для любого $j \neq i$.*

Доказательство. Пусть набор $\tilde{a}$ таков, что $p(\tilde{a}) =$ TRUE. Предположим, что для некоторого i справедливо $a_i \notin M_{c(G_F)} \bigcap D(v_{x_i})$.

Предположим вначале, что $a_i \in L_1(f)$. Если в графе G_F нет циклов, то $c(G_F) = 0$, $M_{c(G_F)} = E_k$, откуда $a_i \in M_{c(G_F)}$. Пусть теперь $c(G_F) > 0$. Поскольку граф G_F связный, то существует замкнутый путь L длины $c(G_F)$, проходящий через вершину v_{x_i} (мы можем пройти в графе из v_{x_i} до цикла, пройти один раз по циклу и вернуться в v_{x_i} тем же путем). Из $p(\tilde{a}) = \text{TRUE}$ следует, что существуют корректные значения для всех переменных формулы F, соответствующие которым вершины графа G_F входят в L. Следовательно, должно выполняться $f^{c(G_F)}(a_i) = a_i$, то есть $a_i \in M_{c(G_F)}$. Получаем противоречие.

Пусть теперь $a_i \notin L_1(f)$. Поскольку $a_i \in T_f$, то $a_i \in L_2(f)$. В графе G_F из вершины v_{x_i} существует путь длины $d_p(x_i)$ $(-d_n(x_i)))$ в некоторую вершину w_1 (соответственно, w_2). Поскольку $p(\tilde{a}) = \text{TRUE}$, то существуют корректные значения переменных формулы F, соответствующих вершинам w_1 и w_2. Получаем, что существуют значения $f^{d_p(y)}(a_i)$ и $f^{-d_n(y)}(a_i)$, откуда $a_i \in D(v_{x_i})$. Опять получаем противоречие.

Пусть опять $p(a_1, \ldots, a_n) = \text{TRUE}$. По определению между вершинами v_{x_i} и v_{x_j} существует путь длины $d_{i,j}$. Следовательно, должно выполняться соотношение $a_j = f^{d_{i,j}}(a_i)$. Необходимость доказана.

Покажем достаточность. Пусть набор $\tilde{a}$ удовлетворяет условиям из формулировки леммы. Зафиксируем некоторое число $i \in \{1, \ldots, n\}$ и обозначим $a_i = b$. Присвоим каждой переменной y_j предиката p (свободной и связанной) значение, равное $f^{d_{i,j}}(b)$. В силу $a_i \in D(v_{x_i})$ для каждой переменной найдется подходящее значение. Покажем далее, что $p(\tilde{a}) = \text{TRUE}$.

Рассмотрим произвольное вхождение сомножителя $R_f(y_j, y_q)$ в формулу F, задающую предикат p над $\{R_f\}$. Переменные y_j и y_q примут соответственно значения $a_j = f^{d_{i,j}}(b)$ и $a_q = f^{d_{i,q}}(b)$. По определению графа формулы в $G(F)$ существует ребро (v_{y_q}, v_{y_j}). Значит, в графе $G(F)$ существуют пути от вершины v_{y_i} к вершинам v_{y_q} и v_{y_j} с длинами соответственно $d_{i,q}$ и $d_{i,j}$. Составим новый путь из вершины v_{y_i} в вершину v_{y_j} через v_{y_q} длины $d_{i,q} + 1$. По лемме 3 существует целое число α такое, что $d_{i,j} = d_{i,q} + 1 + \alpha c(G_F)$.

С учетом $a_i \in M_{c(G_F)}$ получаем

$$a_j = f^{d_{i,j}}(b) = f^{d_{i,q}+1+\alpha c(G_F)}(b) = f^{d_{i,q}+1}(b) = f(a_q),$$

откуда $R_f(a_j, a_q) = \text{TRUE}$. Таким образом, существует набор значений, на котором произвольно взятый сомножитель в формуле F истинен, откуда $p(\tilde{a}) = \text{TRUE}$. Лемма 4 доказана.

Теорема. *Надструктура произвольного класса квазисамодвойственных функций S_f состоит только из классов самодвойственных, квазисамодвойственных функций, их пересечений и P_k.*

Доказательство. Рассмотрим произвольный класс A, содержащий S_f. Из [1] имеем $\text{Inv}A \subseteq \text{Inv}S_f = \text{InvPol}R_f = [R_f, d]$, где $d(x_1, x_2)$ — диагональ ($d(a, b) = \text{TRUE}$ тогда и только тогда, когда $a = b$). Для любого $p \in \text{Inv}A$ справедливо $p \in [R_f, d]$. Рассмотрим формулу F, реализующую предикат p

над $\{R_f, d\}$. Для произвольного вхождения $d(z_1, z_2)$ в F отождествим переменные z_1 и z_2, что позволит вычеркнуть сомножитель $d(z_1, z_2)$. В результате мы получим формулу F_1, реализующую предикат p_1 над $\{R_f\}$. Из [1] следует $\mathrm{Pol}p = \mathrm{Pol}p_1$.

В силу проведенных рассуждений достаточно показать, что для произвольного предиката $p \in [R_f]$ класс $\mathrm{Pol}p$ совпадает с одним из перечисленных в теореме.

Пусть снова F — формула, реализующая p над $\{R_f\}$, G_F — ее граф. Предположим вначале, что G_F — связный граф.

Если местность n предиката p равна единице, то по лемме 4 получаем $p(a) = \mathrm{TRUE}$ тогда и только тогда, когда $a \in T = M_{c(G_F)} \bigcap D(v_x)$. Если $T = E_k$ или $T = \emptyset$, то $\mathrm{Pol}p = P_k$, в противном случае $\mathrm{Pol}p$ является предполным центральным классом, при этом $\mathrm{Pol}p = \mathrm{Pol}R_{f_0}$, где f_0 — тождественная перестановка на множестве T.

Пусть теперь $n = 2$. По лемме 4 получаем $p(a, b) = \mathrm{TRUE}$ тогда и только тогда, когда $a \in T = M_{c(G_F)} \bigcap D(v_x)$ и $b = f^d(a)$. Если $T = E_k$, то $\mathrm{Pol}p$ — класс самодвойственных функций (или P_k, если f — тождественная перестановка), в противном случае $\mathrm{Pol}p$ — класс квазисамодвойственных функций.

Остается случай $n > 2$. Обозначим предикаты

$$p_i(x_1, x_i) = \exists y_1 \ldots, y_{n-2} p(x_1, y_1, \ldots, y_{i-2}, x_i, y_{i-1}, \ldots, y_{n-2}),$$

где $i \in \{2, \ldots, n\}$. Получаем, что $p_i \in [p]$, откуда $p_i \in [R_f]$. Предикаты p_i попадают в уже рассмотренный случай. Несложно показать, что выполняется равенство $p(x_1, \ldots, x_n) = p_2(x_1, x_2) \& p_3(x_1, x_3) \& \ldots \& p_n(x_1, x_n)$, то есть $p \in [\{p_2, \ldots, p_n\}]$.

Обозначим через t предикат, равный конъюнкции предикатов $p_2, \ldots, p_n$ без отождествления переменных. Из последнего соотношения следует, что $p \in [t]$ (p получается из t отождествлением переменных). С другой стороны, из $p_i \in [p]$ следует, что $t \in [p]$. По лемме 1 получаем, что $\mathrm{Pol}p = \mathrm{Pol}t$. По лемме 2 класс $\mathrm{Pol}t$, а значит и $\mathrm{Pol}p$, является пересечением классов $\mathrm{Pol}p_i$, т. е. классов самодвойственных и квазисамодвойственных функций.

Пусть теперь G_F — несвязный граф. Каждая компонента связности G_F очевидным образом задает свой предикат, для которого справедливы проведенные выше рассуждения. Предикат p является конъюнкцией (без отождествления переменных) указанных предикатов. Опять получаем, что $\mathrm{Pol}p$ — некоторое пересечение классов самодвойственных и квазисамодвойственных функций. Теорема доказана.

Список литературы

1. Бондарчук В. Г., Калужнин В. А., Котов В. Н., Ромов Б. А. Теория Галуа для алгебр Поста // Кибернетика. — 1969. — № 3. — С. 1–10. — № 5. — С. 1–9.

2. Ларионов В. Б. О надструктуре некоторых классов функций k-значной логики // XVI международная конференция "Проблемы теоретической кибернетики" (Нижний Новгород, 20-25 июня 2011 г.). — Н. Новгород: изд-во Нижегородского гос. университета. — 2011. — С. 263–266.
3. Ларионов В. Б., Федорова В. С. Надструктура классов самодвойственных k-значных функций // Известия Иркутского государственного университета. Серия Математика. — 2011. — Т. 4, № 3. — С. 83–98.
4. Марченков С. С. Замкнутые классы булевых функций. — М.: Физматлит, 2000.
5. Яблонский С. В. Функциональные построения в k-значной логике // Тр. МИАН им. В. А. Стеклова. — 1958. — Т. 51. — С. 5–142.
6. Яблонский С. В., Гаврилов Г. П., Набебин А. А. Предполные классы в многозначных логиках. — М.: Изд. дом МЭИ, 1997.
7. Янов Ю. И., Мучник А. А. О существовании k-значных замкнутых классов, не имеющих конечного базиса // Доклады АН СССР. — 1959. — Т. 127, № 1. — С. 44–46.

О ВЕРОЯТНОСТНОМ ВЫБОРЕ СЛАЙДОВЫХ ПАР В КОРРЕЛЯЦИОННОМ КРИПТОАНАЛИЗЕ ШИФРА KeeLoq

О. Н. Лебедева (Новосибирск)

Введение

KeeLoq — блочный шифр, широко используемый в системах удалённого доступа, дистанционного управления и т.д. Шифр был разработан профессором Каном Г. и запатентован Южно-Африканской компанией Nanoteq в середине 80-х. В 1995 г. фирма MICROCHIP приобрела *KeeLoq* у фирмы Nanoteq вместе с лицензионными правами.

В данной работе предлагается усовершенствовать метод криптоанализа шифра *KeeLoq* Богданова А. [1]. Улучшение основано на проверке некоторых вероятностных соотношений, используемых для отсеивания неподходящих пар — претендентов на слайдовую пару.

Первый криптоанализ *KeeLoq* был опубликован только в феврале 2007 г. Богдановым А. [1]. Эта атака основана на слайдовой технике и линейном приближении нелинейной булевой функции, использующейся в *KeeLoq*. Криптоанализ имеет временную сложность 2^{52} циклов шифрования *KeeLoq* и требует 16 ГБ памяти. Позднее Богданов обновил свой метод, используя алгебраический криптоанализ [2]. Улучшение привело к уменьшению временной сложности до $2^{50,6}$. Courtois N., Bard V. и Wagner D. [3] применили алгебраическую технику в криптоанализе *KeeLoq*. В 2011 году их криптоанализ был усовершенствован [4] как в среднем, так и в самом лучшем случае.

Biham E. и другие также представили криптоанализ $KeeLoq$ [5, 6], который использует 2^{16} открытых текстов. Его временная сложность составляет 2^{45}, а в случае обобщения $2^{44,5}$.

В статье [7] Kasper M., Kasper T., Moradi A. и Paar C. применили атаку по сторонним каналам, а именно простую атаку по энергопотреблению SPA(simple power analysis).

1. Описание Алгоритма

Алгоритм $KeeLoq$ [1, 8] имеет 64-битный ключ и осуществляет шифрование 32-битных блоков открытого текста. В нём используются два регистра сдвига: один — длины 64 без функции обратной связи (для выработки подключа), другой — регистр сдвига длины 32 с нелинейной функцией обратной связи NLF от пяти переменных (непосредственно для шифрования). Ей соответствует следующая АНФ:

$$NLF(y_4, y_3, y_2, y_1, y_0) = y_0 \oplus y_1 \oplus y_0y_1 \oplus y_1y_2 \oplus y_2y_3 \oplus y_0y_4 \oplus y_0y_3 \oplus \\ \oplus y_2y_4 \oplus y_0y_1y_4 \oplus y_0y_2y_4 \oplus y_1y_3y_4 \oplus y_2y_3y_4$$

Блок открытого текста помещается в текстовый регистр. Шифртекстом является состояние регистра после 528 циклов с использованием регистра ключа. Пусть $V_n = \mathbb{Z}_2^n$ — множество всех n-битных слов; $Y^{(i)}$ и $K^{(i)}$ — соответственно состояния текстового регистра и регистра ключа после i циклов, $Y^{(i)} = (y_{31}^{(i)}, \ldots, y_0^{(i)}) \in V_{32}$, $K^{(i)} = (k_{63}^{(i)}, \ldots, y_0^{(i)}) \in V_{64}$. Каждый цикл шифрования может быть описан следующим образом:

— вычисление очередного бита:

$$\varphi = NLF(y_{31}^{(i)}, y_{26}^{(i)}, y_{20}^{(i)}, y_9^{(i)}, y_1^{(i)}) \oplus y_{16}^{(i)} \oplus y_0^{(i)} \oplus k_0^{(i)};$$

— сдвиг состояния текстового регистра:

$$R^{(i+1)} = (\varphi, y_{31}^{(i)}, \ldots, y_1^{(i)});$$

— сдвиг состояния регистра ключа:

$$K^{(i+1)} = (k_0^{(i)}, k_{63}^{(i)}, \ldots, k_1^{(i)}).$$

528 циклов шифрования $KeeLoq$ можно представить в виде 8+1/4 раундов, где каждый раунд имеет длину 64 цикла. Один раунд использует весь 64-битный ключ, а 1/4 раунда — первые 16 бит ключа. На этом основана первая слабость алгоритма, которая позволяет применить слайдовую атаку. Вторая слабость связана с наличием достаточно хорошего линейного приближения нелинейной функции NLF. А именно, справедлива следующая лемма [1].

Лемма. *Для равномерно распределённых $y_4, y_3, y_2 \in GF(2)$ верно следующее:*

$$-Pr\{NLF(y_4, y_3, y_2, y_1, y_0) = 0 \mid y_0 \oplus y_1 = 0\} = 5/8,$$
$$-Pr\{NLF(y_4, y_3, y_2, y_1, y_0) = 1 \mid y_0 \oplus y_1 = 1\} = 5/8.$$

2. Криптоанализ Богданова А.

В своей работе [1] Богданов описывает следующие шаги. Для каждого подключа $K' = (k_{15}, \ldots, k_0)$ и случайного 32-битного входа $I_0 \in V_{32}$ с помощью парадокса дней рождения угадывается промежуточный шифртекст $O_0 \in V_{32}$ после 64 циклов шифрования. Такая пара (I_0, O_0) называется *слайдовой парой*. Используя периодическую структуру ключа, в $KeeLoq$ генерируются другие пары $(I_i, O_i) \in (V_{32})^2, i = 1, \ldots, N-1$. Для успешной атаки их число должно быть около 2^8. Для каждого такого набора пар получаются линейные соотношения для неизвестных битов ключа с высокой вероятностью в связи с тем, что нелинейная функция обратной связи, использующаяся в $KeeLoq$, не является 2-устойчивой. Таким образом, можно определить $(k_{47}, \ldots, k_{16})$ бит за битом. После этого решается треугольная система линейных уравнений для оставшихся битов ключа $(k_{63}, \ldots, k_{48})$.

Отметим, что в методе Богданова для каждого подключа $K' = (k_{15}, \ldots, k_0)$ по сути происходит полный перебор всевозможных пар (кандидатов на слайдовую пару (I_0, O_0)) из случайного подмножества мощности 2^{16} множества всех двоичных векторов длины 32 и для каждой такой пары (I_0, O_0) выполняется корреляционный криптоанализ.

3. Усовершенствование метода Богданова А.

В данной работе предлагается на каждом шаге корреляционного криптоанализа использовать найденные биты ключа для отсеивания неподходящих пар. А именно, можно найти вероятностное соотношение между битами из правильной слайдовой пары и битами ключа, проверка которого позволяет для части неправильных пар остановить выполнение корреляционного криптоанализа уже на этом шаге. В этом соотношении используется линейное приближение нелинейной функции NLF, выполняющееся с вероятностью 5/8.

Например, связь бита $y_0^{(64)}$ с битами на 16-м раунде выражается так:

$$y_0^{(64)} = y_{31}^{(33)} = NLF(y_{31}^{(32)}, y_{26}^{(32)}, y_{20}^{(32)}, y_9^{(32)}, y_1^{(32)}) \oplus y_{16}^{(32)} \oplus y_0^{(32)} \oplus k_{32} =$$
$$= y_1^{(32)} \oplus y_9^{(32)} \oplus y_{16}^{(32)} \oplus y_0^{(32)} \oplus k_{32} = y_{17}^{(16)} \oplus y_{25}^{(16)} \oplus y_{31}^{(17)} \oplus y_{16}^{(16)} \oplus k_{32} =$$
$$= y_{17}^{(16)} \oplus y_{25}^{(16)} \oplus (NLF(y_{31}^{(16)}, y_{26}^{(16)}, y_{20}^{(16)}, y_9^{(16)}, y_1^{(16)}) \oplus y_{16}^{(16)} \oplus y_0^{(16)} \oplus$$
$$\oplus k_{16}) \oplus y_{16}^{(16)} \oplus k_{32} =$$
$$= y_{17}^{(16)} \oplus y_{25}^{(16)} \oplus y_9^{(16)} \oplus y_1^{(16)} \oplus y_0^{(16)} \oplus k_{16} \oplus k_{32}$$

Это соотношение выполняется с вероятностью 17/32.

Таким образом, после того как будут найдены k_{16} и k_{32} на первом шаге корреляционной атаки, для отсеивания неправильных слайдовых пар используются биты ключа $(k_{16}, k_{15}, \ldots, k_0)$ и k_{32}.

На каждом шаге корреляционной атаки используется дополнительное соотношение для битов входного и выходного текста, что позволяет останавливать криптоанализ для пары, которая не удовлетворяет полученным со-

отношениям. Можно построить 9 таких соотношений. Следующая таблица иллюстрирует процесс.

шаг	0	1	2	...	9
количество слайдовых пар	2^{32}	2^{31}	2^{30}	...	2^{23}
найденные биты ключа	$k_{15}, \ldots, k_0$	k_{16}, k_{32}	k_{17}, k_{33}	...	k_{24}, k_{40}

Во второй строке указано количество пар, для которых будет выполняться следующий шаг корреляционного анализа. Например, изначально понадобится перебор 2^{32} пар. Затем находятся биты ключа k_{16} и k_{32} на первом шаге корреляционной атаки, которые используются в соотношении между $y_0^{(64)}$ и битами шифртекста после 16 циклов. Значит, можно не рассматривать пары, не удовлетворяющие этому соотношению. Следовательно, число пар, для которых будет выполняться следующий шаг криптоанализа, сократится.

По парадоксу дней рождения достаточно рассмотреть подмножество A векторов длины 32 мощности 2^{16}. Вероятность того, что среди элементов этого подмножества найдутся как минимум два, составляющие слайдовую пару, равна $1-(1-2^{-32})^{2^{32}} \approx 0,63$. Это множество будем выбирать таким образом, чтобы каждому вероятностному соотношению удовлетворяла ровно половина векторов из этого множества. За счёт этого после каждого шага корреляционного анализа далее используется только половина пар.

4. Построение множества A

Рассмотрим множество A. Оно состоит из векторов $a = (a_0, \ldots, a_{31})$ длины 32. Его мощность равна 2^{16}.

Пусть биты $a_0, a_1, \ldots, a_{23}$ для каждого вектора $a \in A$ принимают произвольные значения.

Введём следующее обозначение. Пусть $A_{i_0,\ldots,i_k}^{\delta_0,\ldots,\delta_k}$ — множество всех векторов из A таких, что биты на позициях $i_0, \ldots, i_k$ принимают значения $\delta_0, \ldots, \delta_k$.

Рассмотрим ограничения на множество A, исходя из которых в корреляционном криптоанализе ровно половина пар — кандидатов на слайдовую — перестанет удовлетворять полученным выше соотношениям.

1) $a_{25} = a_{17} \oplus a_9 \oplus a_1$; $\quad |A_0^{\delta}| = 2^{15}\ \forall \delta \in \{0,1\}$

2) $a_{26} = a_{18} \oplus a_{10} \oplus a_2$; $\quad |A_{0,1}^{\delta_0,\delta_1}| = 2^{14}\ \forall \delta_0, \delta_1 \in \{0,1\}$

3) $a_{27} = a_{19} \oplus a_{11} \oplus a_3$; $\quad |A_{0,1,2}^{\delta_0,\delta_1,\delta_2}| = 2^{13}\ \forall \delta_0, \delta_1, \delta_2 \in \{0,1\}$

4) $a_{28} = a_{20} \oplus a_{12} \oplus a_4$; $\quad |A_{0,1,2,3}^{\delta_0,\delta_1,\delta_2,\delta_3}| = 2^{12}\ \forall \delta_0, \delta_1, \delta_2, \delta_3 \in \{0,1\}$

5) $a_{29} = a_{21} \oplus a_{13} \oplus a_5$; $\quad |A_{0,1,2,3,4}^{\delta_0,\delta_1,\delta_2,\delta_3,\delta_4}| = 2^{11}\ \forall \delta_0, \delta_1, \delta_2, \delta_3, \delta_4 \in \{0,1\}$

6) $a_{30} = a_{22} \oplus a_{14} \oplus a_6$; $\quad |A_{0,1,2,3,4,5}^{\delta_0,\delta_1,\delta_2,\delta_3,\delta_4,\delta_5}| = 2^{10}\ \forall \delta_0, \delta_1, \delta_2, \delta_3, \delta_4, \delta_5 \in \{0,1\}$

7) $a_{31} = a_{23} \oplus a_{15} \oplus a_7$; $\quad |A_{0,1,2,3,4,5,6}^{\delta_0,\delta_1,\delta_2,\delta_3,\delta_4,\delta_5,\delta_6}| = 2^{9}\ \forall \delta_0, \delta_1, \delta_2, \delta_3, \delta_4, \delta_5, \delta_6 \in \{0,1\}$

8) $a_{24} = a_8 \oplus a_0 \oplus NLF(a_{31}, a_{26}, a_{20}, a_9, a_1)$;

$|A^{\delta_0,\delta_1,\delta_2,\delta_3,\delta_4,\delta_5,\delta_6,\delta_7}_{0,1,2,3,4,5,6,7}| = 2^8 \ \forall \delta_0, \delta_1, \delta_2, \delta_3, \delta_4, \delta_5, \delta_6, \delta_7 \in \{0,1\}$

9) $a_{25} = a_9 \oplus a_1 \oplus NLF(NLF(a_{31}, a_{26}, a_{20}, a_9, a_1) \oplus a_0 \oplus a_{16}, a_{27}, a_{21}, a_{10}, a_2)$;

$|A^{\delta_0,\delta_1,\delta_2,\delta_3,\delta_4,\delta_5,\delta_6,\delta_7,\delta_8}_{0,1,2,3,4,5,6,7,8}| = 2^7 \ \forall \delta_0, \delta_1, \delta_2, \delta_3, \delta_4, \delta_5, \delta_6, \delta_7, \delta_8 \in \{0,1\}$

Далее подобные ограничения не рассматриваются, так как в первой части каждого ограничения зависимый бит будет стоять как слева, так и справа от знака равенства.

Способов выбора множества A существует $\approx 2^{914759,68}$. Это позволяет считать множество A вполне случайным, что необходимо для парадокса дней рождения.

5. Временная сложность, память

По методу Богданова А. криптоанализа шифра *KeeLoq* была осуществлена практическая реализация. Также она выполнена для усовершенствования метода. В обоих случаях верный ключ находится. По псевдокоду написанной программы для метода криптоанализа Богданова А. была подсчитана средняя временная сложность. Она составляет $\approx 2^{57}$ циклов шифрования *KeeLoq*. Аналогичным способом подсчитана временная сложность для усовершенствования метода Богданова А. Она составила $\approx 2^{51}$ циклов шифрования *KeeLoq*.

В обоих случаях: как для реализации метода Богданова А., так и для реализации усовершенствования требуется константная память, примерно 2^{21} битов.

Список литературы

1. Bogdanov A. Cryptanalysis of the KeeLoq Block Cipher // Cryptology ePrint Archive, Report 2007/055, 16 February 2007, http://eprint.iarc.org/2007/055
2. Bogdanov A. Attacks on the KeeLoq Block Cipher and Authentication Systems // 3rd Conference on RFID Security 2007, RFIDSec 2007, http://rfidsec07.etsit.uma.es/slides/papers/paper-22.pdf
3. Courtois N., Bard V., Wagner D. Algebraic and Slide Attacks on KeeLoq // Fast Software Encryption: 15th International Workshop, FSE 2008. (Lausanne, Switzerland, February 10–13, 2008), eprint.iacr.org/2007/062
4. Courtois N., Bard V., Wagner D. Random Permutation Statistics and An Improved Slide-Determine Attack on KeeLoq // Festschrift Jean-Jacques Quisquater, 2011, http://www-users.math.umd.edu/ bardg/keeloq_new_paper.pdf

5. Indesteege S., Keller N., Dunkelman O., Biham E., Preneel B. A Practical Attack on KeeLoq // EUROCRYPT 2008, 27th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Istanbul, Turkey, April 13–17, 2008.
6. Aerts W., Biham E., De Moitie D., De Mulder E., Dunkelman O., Indesteege S., Keller N., Preneel B, Vandenbosch G., Verbauwhede I. A Practical Attack on KeeLoq // Journal of Cryptology (2010): November 03, 2010.
7. Kasper M., Kasper T., Moradi A., Paar C. Breaking KeeLoq in a Flash // Progress in Cryptology - AFRICACRYPT 2009, Second International Conference on Cryptology in Africa, Gammarth, Tunisia, June 21-25, 2009.
8. Wikipedia. KeeLoq // http://en.wikipedia.org/wiki/KeeLoq.

ПОВЕДЕНИЕ ФУНКЦИИ ШЕННОНА ДЛЯ ГЛУБИНЫ В МОДЕЛИ СХЕМ ДОПУСКАЮЩЕЙ РАЗЛИЧИЕ ЗАДЕРЖЕК ФУНКЦИОНАЛЬНЫХ ЭЛЕМЕНТОВ ПО ВХОДАМ

С. А. Ложкин, Б. Р. Данилов (Москва)

1. Введение

Рассматриваются формулы и схемы из функциональных элементов (СФЭ) над произвольным конечным полным базисом Б, Б $= \{E_1, E_2, \ldots, E_b\}$, где функциональный элемент (ФЭ) E_i, $i = 1, \ldots, b$, имеет k_i, $k_i \geq 1$, входов и реализует функцию алгебры логики (ФАЛ) $\varphi_i(x_1, \ldots, x_{k_i})$, которая в случае $k_i \geq 2$ существенно зависит от всех своих булевых переменных (БП). При этом, как обычно, формулами считаются те одновыходные СФЭ, в которых выход любого ФЭ либо поступает на вход ровно одного (другого) ФЭ, либо является выходом схемы. Для натурального n множество всех двоичных наборов длины n будем обозначать через B^n.

Введём модель задержки СФЭ над Б, которая обобщает рассматриваемые в работах [1–4] модели задержки. Будем считать, что для каждого ФЭ E_i и каждого j, $j = 1, \ldots, k_i$, определена положительная *задержка* T_i^j *ФЭ* E_i *по входу* x_j. *Цепью* ω называется, как обычно, СФЭ, которая составлена из цепочки последовательно соединённых ФЭ $E_{i_1}, \ldots, E_{i_w}$. *Инициальной цепью* назовём цепь, у которой выделен один из входов первого ФЭ цепи E_{i_1}. *Задержкой* $T(\omega)$ *инициальной цепи* ω *СФЭ* Σ, $\Sigma = \Sigma(x_1, \ldots, x_n)$, назовём сумму задержек ФЭ цепи по соединяющим их входам и выделенному входу первого ФЭ. По аналогии с $T(\omega)$ определим величину $\widehat{T}(\omega)$, где в сумму включим только слагаемые, отвечающие ФЭ с более чем одним входом, и которая равна нулю в случае, когда цепь ω составлена только из одновходовых элементов. Подсхему Σ, являющуюся инициальной цепью, выделенный вход которой яв-

ляется входом Σ и оканчивающуюся на одном из её выходных ФЭ (т. е. ФЭ, выход которых поступает на выход схемы), будем называть *главной цепью СФЭ* Σ.

Под *задержкой* $T(\Sigma)$ *схемы* Σ в рассматриваемой модели понимается величина равная максимуму из задержек её инициальных цепей. Величину $\widehat{T}(\Sigma)$ определим по аналогии $T(\Sigma)$ на основе $\widehat{T}(\omega)$. *Задержка ФАЛ* и *функция Шеннона* $T_{\text{Б}}(n)$ *для задержки ФАЛ от* n *БП в классе СФЭ над* Б определяются обычным образом.

В описанной модели поднятие ветвлений выходов ФЭ к входам схемы не изменяет её задержки. Отсюда, аналогично [5], следует, что для каждой СФЭ найдётся формула (система формул) в том же базисе, задержка которой совпадёт с задержкой исходной СФЭ, поэтому в дальнейшем ограничимся рассмотрением формул в базисе Б. Множество формул над Б обозначим через $U^{\Phi}_{\text{Б}}$, а через U^{Φ} обозначим множество формул над базисом $\{\&, \vee, \neg\}$.

Рассмотрим не пустое (в силу полноты Б) множество $\widehat{\text{Б}}$, состоящее из ФЭ базиса Б, имеющих не менее двух входов. Без ограничения общности предположим, что $\widehat{\text{Б}} = \{E_1, \ldots, E_{b'}\}$. Для ФЭ E_i, $i = 1, \ldots, b'$, определим его *приведённую задержку* τ'_i равенством $\tau'_i = 1/\log_2 x_i$, где x_i, $x_i > 1$, — единственный корень характеристического уравнения

$$\sum_{j=1}^{k_i} x^{-T_i^j} = 1,$$

рассматриваемого на положительной полуоси. Определим *приведённую задержку базиса* Б равенством $\tau'_{\text{Б}} = \min_{1 \le i \le b'} \tau'_i$.

2. Нижняя оценка функции Шеннона

Нижняя оценка функции Шеннона может быть получена аналогично тому, как это делается в [5] на основе следующих лемм.

Лемма 1. *Для любого* n *и всякой формулы* $\mathcal{F} = \mathcal{F}(x_1, ..., x_n) \in U^{\Phi}_{\text{Б}}$, *верно*

$$R(\mathcal{F}) \le 2^{\widehat{T}(\mathcal{F})/\tau'_{\text{Б}}}.$$

Лемма 2. *Для любого действительного* $T \ge 0$ *и любого натурального* n *число попарно не эквивалентных формул над* Б, *которые зависят от* n *БП и задержка которых не больше* T, *не превосходит*[4] $(c_1 n)^{2^{T/\tau'_{\text{Б}}}}$.

Теорема 1. *Для всех натуральных* n *выполняется неравенство*

$$T_{\text{Б}}(n) \ge \tau'_{\text{Б}}(n - \log\log n) - c_2.$$

[4]Буквой c с индексами обозначаются различные константы зависящие от базиса Б.

3. Верхняя оценка функции Шеннона

Назовём *альтернированием набора* $\alpha \in B^n$ $(n \geq 1)$ минимальное число отрезков постоянства, на которые он распадается, уменьшенное на единицу, и обозначим его через $\mathrm{alt}(\alpha)$. Определим *альтернирование ФАЛ* f как альтернироване столбца её значений и обозначим через $\mathrm{alt}(f)$. Назовём монотонную (антимонотонную) ФАЛ h *монотонной* (соответственно *антимонотонной*) *ступенчатой ФАЛ*, если $\mathrm{alt}(h) \leq 1$. ФАЛ h_i, $h_i \in P_2(n)$, назовём *i-ой монотонной ступенчатой* ФАЛ $(0 \leq i \leq 2^n)$, если для всякого $\beta \in B^n$ она равна нулю, когда число двоичной записью которого является набор β меньше i и равна единице в противном случае.

Лемма 3. *Для натурального n и любой i-ой монотонной ступенчатой ФАЛ h_i, $h_i \in P_2(n)$, $(1 \leq i \leq 2^n - 1)$ найдётся формула $\mathcal{F}_i$, $\mathcal{F}_i \in U^{\Phi}$, реализующая h_i для которой верно*

$$D(\mathcal{F}_i) \leq 2 \lceil \log n \rceil .$$

Лемма 4. *Для натурального n и любой ФАЛ g, $g \in P_2(n)$, отличной от константы найдётся формула $\mathcal{F}$, $\mathcal{F} \in U^{\Phi}$, реализующая g для которой верно*

$$D(\mathcal{F}) \leq 2 \lceil \log n \rceil + \lfloor \log \mathrm{alt}(g) \rfloor + 2.$$

Следующая лемма позволяет построить формулу в виде квазиполного дерева с минимальной при данном числе входов задержкой.

Лемма 5. *Если $\tau'_{\text{Б}}$ достигается на ФЭ E_t, т. е. $\tau'_t = \tau'_{\text{Б}}$, то для всяких натуральных чисел p и r, связанных соотношением $p = r(k_t - 1) + 1$, существует бесповторная формула $\mathcal{F}$, $\mathcal{F} \in U^{\Phi}_{\text{Б}}$, с p входами, состоящая из r ФЭ E_t, для которой справедливо $T(\mathcal{F}) \leq \tau'_{\text{Б}} \log p + c_3$.*

Леммы 6 и 7 позволяют конструировать мультиплексорную ФАЛ на основе произвольной ФАЛ.

Лемма 6. *Для любой существенной ФАЛ $\varphi(y_1, \ldots, y_p)$ и любого разбиения $\Delta = (\delta_1, \ldots, \delta_p)$ куба B^n от БП $x = (x_1, \ldots, x_n)$ существуют ФАЛ $g_i(x, y_i)$, $i = 1, \ldots, p$, которые монотонно или антимонотонно зависят от БП $y_1, \ldots, y_p$, такие что $\varphi(g_1, \ldots, g_p) = \mu_{\Delta}(x, y_1, \ldots, y_p)$.*

Лемма 7. *Для любой существенной ФАЛ $\varphi(y_1, \ldots, y_p)$ и любого разбиения Δ, $\Delta = (\delta_1, \ldots, \delta_p)$, куба B^n от БП $x = (x_1, \ldots, x_n)$ существуют ФАЛ $g_i(x, y_i)$, $i = 1, \ldots, p$, которые монотонно или антимонотонно зависят от БП $y_1, \ldots, y_p$, такие, что $\varphi(g_1, \ldots, g_p) = \mu_{\Delta}(x, y_1, \ldots, y_p)$, где μ_{Δ} — это обобщённая мультиплексорная ФАЛ, соответствующая разбиению Δ, равная y_i, когда $x \in \delta_i$.*

Теоремы 2 и 3 могут быть доказаны на основе лемм 3–7.

Теорема 2. *Для любого натурального n ФАЛ $\mu_n(x, y_0, \ldots, y_{2^n-1})$ можно реализовать бесповторной по информационным БП формулой $\mathcal{M}_n$ в базисе* Б, *для которой*

$$T(\mathcal{M}_n) \leq \tau_{\text{Б}} n + c_4.$$

Теорема 3. *Для натурального n и любой ФАЛ f, $f \in P_2(n)$, существует реализующая её формула $\mathcal{F}$ в базисе* Б *такая, что*

$$T(\mathcal{F}) \leq \tau'_{\text{Б}}(n - \log\log n) + c_5.$$

Теоремы 1 и 3 дают асимптотику функции Шеннона для глубины формул в произвольном базисе в рассматриваемой модели на уровне асимптотических оценок высокой степени точности.

Следствие.

$$T(n) = \tau'_{\text{Б}}(n - \log\log n) \pm O(1).$$

Список литературы

1. Лупанов О. Б. О схемах функциональных элементов с задержками // Проблемы кибернетики. — Вып. 23 — М.: Наука, 1970. — С. 43–82.
2. Ложкин С. А. О глубине функций алгебры логики в произвольном полном базисе // Вестник МГУ. Математика. Механика. — 1996. — № 2 — С. 80–82.
3. Ложкин С. А. О задержке мультиплексорной функции в произвольном базисе // Проблемы теоретической кибернетики. Тезисы докладов XV международной конференции (Казань, 2–7 июня 2008 г.). — Казань: Отечество, 2008. — С. 75.
4. Ложкин С. А. Поведение функции Шеннона для задержки схем из функциональных элементов в некоторых моделях // Проблемы теоретической кибернетики. Тезисы докладов XII международной конференции (Нижний Новгород, 17–22 мая 1994 г.). — М.: Изд-во механико-математического факультета МГУ, 1999. — С. 139.
5. Ложкин С. А. Основы кибернетики. — М.: Издательский отдел ф-та ВМиК МГУ, 2004. — 251 с.