ISBN 978-5-9624-1734-9

СИНТАКСИС И СЕМАНТИКА ЛОГИЧЕСКИХ СИСТЕМ

УДК 510.6+512+519.7
ББК 22.12+22.14+22.18
С38

Синтаксис и семантика логических систем [Электронный ресурс] : материалы 6-й Междунар. школы-семинара. Монголия, Ханх, 11–16 авг. 2019 г. / [редкол.: С. С. Гончаров [и др.]] ; ФГБОУ ВО «ИГУ». – Иркутск : Изд-во ИГУ, 2019. – 1 электрон. опт. диск (CD-ROM). – Загл. с этикетки диска.
ISBN 978-5-9624-1734-9

Сборник содержит материалы 6-й Международной школы-семинара «Синтаксис и семантика логических систем», посвященной 90-летию со дня рождения профессора А. И. Кокорина и проходившей в Ханхе (Монголия) с 11 по 16 августа 2019 г.
Для студентов, аспирантов и научных работников, специализирующихся в области математической логики и дискретной математики.

Федеральное государственное бюджетное образовательное учреждение высшего образования
«Иркутский государственный университет»
664003, г. Иркутск, ул. К. Маркса, 1; тел. (3952) 24-34-53
Издательство ИГУ, 664074, г. Иркутск, ул. Лермонтова, 124; тел. (3952) 52-18-53
Подписано к использованию 28.08.2019. Тираж 30 экз. Объем 4,1 Мб.

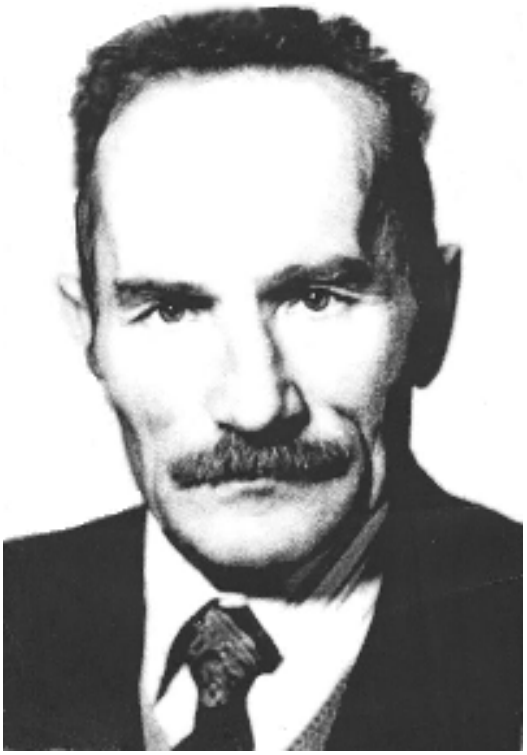
Тип компьютера, процессор, частота:	32-разрядный процессор, 1 ГГц или выше
Оперативная память (RAM):	256 МБ
Необходимо на винчестере:	320 МБ
Операционные системы:	ОС Microsoft® Windows® XP, 7, 8 или 8.1. ОС Mac OS X
Видеосистема:	Разрешение экрана 1024x768
Акустическая система:	Не требуется
Дополнительное оборудование:	Не требуется
Дополнительные программные средства:	Adobe Reader 6 или выше

ISBN 978-5-9624-1734-9

СИНТАКСИС И СЕМАНТИКА ЛОГИЧЕСКИХ СИСТЕМ

ISBN 978-5-9624-1734-9

СИНТАКСИС И СЕМАНТИКА ЛОГИЧЕСКИХ СИСТЕМ



Перед вами сборник материалов школы-семинара «Синтаксис и семантика логических систем», проходившей в пос. Ханх (Монголия) на побережье озера Хубсугул с 11 по 16 августа 2019 г. Это уже шестая школа-семинар. Первая и третья прошли в 2006 и 2010 гг. на западном берегу озера Байкал, вторая (2008 г.) — на турбазе под Владивостоком на побережье Японского моря, четвертая (2012 г.) и пятая (2017 г.) — на турбазах на восточном берегу Байкала.

Настоящая школа-семинар посвящена памяти основателя научной алгебро-логической школы в Иркутске Али Ивановича Кокорина, 90 лет со дня рождения которого исполняется в ноябре 2019 г. Организаторами семинара являлись Иркутский государственный университет и Институт математики им. С. Л. Соболева Сибирского отделения РАН. Тематика сборника отражает широту научных интересов Али Ивановича и представляет те области исследований, в которых сегодня работают его ученики.

В.И. Пантелеев,
Н.А. Перязев

Содержание

УДК 519.718

Асимптотически оптимальные по надежности схемы в базисе, состоящем из функции Вебба, при неисправностях типа 0 на выходах элементов

Алехина Марина Анатольевна[1], **Барсукова Оксана Юрьевна**[2]

[1] Пензенский государственный технологический университет, e-mail: alekhina@penzgtu.ru
[2] Пензенский государственный университет, e-mail: oksana.barsukova.71@gmail.com

Рассматривается реализация функций k-значной логики ($k \geqslant 3$) схемами из ненадежных функциональных элементов в полном базисе, состоящем из функции Вебба. Предполагается, что элементы схемы переходят в неисправные состояния независимо друг от друга, подвержены однотипным константным неисправностям типа 0 на выходах. Показано, что при неисправностях типа 0 почти любую функцию k-значной логики можно реализовать асимптотически оптимальной по надежности схемой, функционирующей с ненадежностью асимптотически равной ненадежности одного базисного элемента. Полученный результат справедлив в двойственном (относительно перестановки, порождаемой функцией Лукашевича) базисе при однотипных константных неисправностях типа $k-1$ соответственно.

Ключевые слова: функции k-значной логики, ненадежные функциональные элементы, надежность и ненадежность схемы, синтез схем из ненадежных элементов, неисправности на выходах элементов.

Рассматривается реализация функций k-значной логики ($k \geqslant 3$) схемами из ненадежных элементов в полном базисе B, состоящем из функции Вебба $V_k(x_1, x_2) = \max\{x_1, x_2\} + 1 \ (mod\ k)$, а также в двойственном (относительно перестановки, порождаемой функцией $N(x) = k - 1 - x$, которую называют отрицанием Лукашевича) базисе B^*, состоящем из функции $\min\{x_1, x_2\} + k - 1 \ (mod\ k)$.

Задача синтеза надежных схем в этих базисах была решена в [1] при инверсных неисправностях на выходах базисных элементов (когда на каждом входном наборе любого из базисных элементов вероятность появления неверного значения на выходе элемента одинакова) и $k = 3$, причем были применены два различных метода синтеза и найдены условия, при которых один метод дает лучшую оценку надежности схем чем другой. В отличие от [1] будем исследовать однотипные константные неисправности типа 0 на выходах элементов и произвольном $k \geqslant 3$. Предполагается, что элементы схемы переходят в неисправные состояния с вероятностью $\varepsilon \in (0, 1/2)$, независимо друг от друга.

Пусть $k, n \in \mathbf{N}$, $k \geqslant 3$. Обозначим через $E_k = \{0, 1, 2, ..., k-1\}$, а через P_k — множество всех функций k-значной логики, т.е. функций $f(x_1, ..., x_n) : (E_k)^n \to E_k$. Используемые в этой работе понятия и определения можно найти в [1], [2].

Справедливы следующие теоремы.

Теорема 1. *Любую функцию* $f \in P_k$ *можно реализовать такой схемой* S, *что* $P(S) < \varepsilon + c_1(k)\varepsilon^2$ *при всех* $\varepsilon \in (0, \varepsilon_1]$, *где* $\varepsilon_1 = 2^{-2^k}/(27k^8)$, $c_1(k) = 5 \cdot 2^{2^k}$.

Из теоремы 1 следует, что любую функцию из P_k можно реализовать схемой, ненадежность которой асимптотически (при $\varepsilon \to 0$) не больше ε.

Пусть $K(n)$ — множество функций k-значной логики, каждая из которых зависит от переменных $x_1, ..., x_n$ $(n \geqslant 1)$ и отлична от функций 0, $x_1, ...,$ x_n $(n \geqslant 1)$. Обозначим $K = \bigcup\limits_{n=1}^{\infty} K(n)$. Очевидно, что $|K(n)| = k^{k^n} - n - 1$, а значит, класс $K(n)$ содержит почти все функции из множества $P_k(n)$ (поскольку $\lim\limits_{n\to\infty} \frac{k^{k^n}-n-1}{k^{k^n}} = 1$).

Справедлива теорема 2 о нижней оценке ненадежности схем, реализующих функции из класса K.

Теорема 2. *Пусть функция* $f \in K$. *Тогда для любой схемы* S, *реализующей* f, *верно неравенство* $P(S) \geqslant \varepsilon$ *при всех* $\varepsilon \in (0, 1/2)$.

Для доказательства теоремы 2 достаточно выделить подсхему из одного элемента, выход которого является выходом схемы, и оценить вероятность появления 0 на любом ненулевом входном наборе схемы.

Из теоремы 2 следует, что любая схема, реализующая функцию $f \in K$, функционирует с ненадежностью, которая не меньше ε. Это означает, что схема, реализующая функцию $f \in K$ и удовлетворяющая условиям теоремы 1, является асимптотически оптимальной по надежности и функционирует с ненадежностью, асимптотически равной ε при $\varepsilon \to 0$.

Поскольку ненадежности двойственных (относительно перестановки, порождаемой функцией $N(x) = k - 1 - x$, которую называют отрицанием Лукашевича) схем равны [3], утверждение, доказанное в базисе B для ненадежности схемы, реализующей функцию f, при неисправностях типа 0 на выходах элементов верно в базисе B^* для ненадежности двойственной схемы, реализующей функцию f^*, при неисправностях типа $k - 1$ на выходах элементов. Следовательно, в базисе B^* при неисправностях типа $k - 1$ на выходах элементов почти любую функцию k-значной логики можно реализовать асимптотически оптимальной по надежности, которая функционирует с ненадежностью, асимптотически равной ε при $\varepsilon \to 0$.

Работа выполнена при поддержке РФФИ (проект № 17-01-00451-а).

Список литературы

[1] Алехина М. А., Барсукова О. Ю. Верхняя оценка схем в базисе, состоящем из функции Вебба // Известия высших учебных заведений. Математика. 2015. № 3. С. 15–27.

[2] Алехина М. А. Рекуррентные соотношения для ненадежностей схем при однотипных константных неисправностях типов 0 и k-1 в базисе, состоящем из функции Вебба, в P_k // Известия высших учебных заведений. Поволжский регион. Физико-математические науки. 2018. № 4. С. 25–30.

[3] Алехина М. А. Надежность двойственных схем в P_k // Известия высших учебных заведений. Поволжский регион. Физико-математические науки. 2017. № 1. С. 3–13.

Asymptotically optimal in reliability curcuits in a basis consisting of the Webb function with the faults of type 0 at the outputs of gates.

Alekhina Marina Anatol'evna [1], Barsukova Oksana Yur'evna [2]

[1] Penza State Technological University , e-mail: alekhina@penzgtu.ru

[2] Penza State University , e-mail: oksana.barsukova.71@gmail.com

We consider the problem of the implementation of k-valued logics ($k \geqslant 3$) by circuits from unreliable gates in full basis consisting of the Webb function. We assume that gates of the circuit pass to fault states independently of each other, and they are exposed to single-type constant faults of type 0 at the outputs. It is shown that with faults of type 0 almost any function of k-valued logics can be implemented by an asymptotically optimal in reliability circuit functioning with the unreliability which is asymptotically equal to unreliability of one basis element. The obtained result is valid in a dual (with respect to the permutation which is generated by the Lukashevich function) basis with single-type constant faults of type $k-1$ respectively.

Keywords: unreliable functional gates, reliability and unreliability of circuit, synthesis of circuits from unreliable gates, faults at outputs of gates.

УДК 519.718

О надежности схем в базисе, содержащем особенную функцию

Алехина Марина Анатольевна, Гусынина Юлия Сергеевна, Шорникова Татьяна Александровна

Пензенский государственный технологический университет, e-mail: alekhina@penzgtu.ru, gusynina@mail.ru, shornikovat@mail.ru

Рассматривается реализация булевых функций схемами из ненадежных функциональных элементов в полном конечном базисе, содержащем особенную функцию. Предполагается, что все элементы схемы независимо друг от друга с вероятностью $\varepsilon \in (0, 1/2)$ подвержены неисправностям типа 0 на выходах. Показано, что почти любую булеву функцию можно реализовать асимптотически оптимальной по надежности схемой, функционирующей с ненадежностью, асимптотически равной ε при $\varepsilon \to 0$.

Ключевые слова: ненадежные функциональные элементы, надежность и ненадежность схемы, синтез схем из ненадежных элементов.

Рассмотрим реализацию булевых функций схемами из ненадежных функциональных элементов в полном конечном базисе. Известно, что любой полный базис содержит нелинейную функцию [1], а из всякой нелинейной функции от трех или более переменных подстановкой (т. е. отождествлением и/или переименованием) переменных можно получить либо нелинейную функцию двух переменных $\phi(x_1, x_2) = x_1x_2 \oplus \alpha_1x_1 \oplus \alpha_2x_2 \oplus \alpha_0$, либо особенную функцию, т. е. функцию вида $\varphi(x_1, x_2, x_3) = x_1x_2 \oplus x_1x_3 \oplus x_2x_3 \oplus \beta_1x_1 \oplus \beta_2x_2 \oplus \beta_3x_3 \oplus \beta_0$, где $\alpha_0,\ \alpha_1,\ \alpha_2,\ \beta_0,\ \beta_1,\ \beta_2,\ \beta_3 \in \{0,\ 1\}$ [2]. В этой работе будем рассматривать базисы, в каждом из которых содержится нелинейная функция, из которой можно получить особенную функцию. Поэтому без ограничения общности будем считать, что базис содержит особенную функцию, зависящую от переменных $x_1,\ x_2,\ x_3$.

С точностью до переименования переменных $x_1,\ x_2,\ x_3$ для особенной функции (в зависимости от коэффициентов $\beta_0,\ \beta_1,\ \beta_2,\ \beta_3$) возможны 8 случаев:

1) $\varphi_1(x_1,\ x_2,\ x_3) = x_1x_2 \oplus x_2x_3 \oplus x_1x_3 \oplus x_1 \oplus x_2 \oplus x_3 \oplus 1$;
2) $\varphi_2(x_1,\ x_2,\ x_3) = x_1x_2 \oplus x_2x_3 \oplus x_1x_3 \oplus x_1 \oplus 1$;
3) $\varphi_3(x_1,\ x_2,\ x_3) = x_1x_2 \oplus x_2x_3 \oplus x_1x_3 \oplus x_1$;
4) $\varphi_4(x_1,\ x_2,\ x_3) = x_1x_2 \oplus x_2x_3 \oplus x_1x_3 \oplus x_1 \oplus x_2 \oplus x_3$;
5) $\varphi_5(x_1,\ x_2,\ x_3) = x_1x_2 \oplus x_2x_3 \oplus x_1x_3 \oplus x_1 \oplus x_2 \oplus 1$;
6) $\varphi_6(x_1,\ x_2,\ x_3) = x_1x_2 \oplus x_2x_3 \oplus x_1x_3 \oplus x_1 \oplus x_2$;
7) $\varphi_7(x_1,\ x_2,\ x_3) = x_1x_2 \oplus x_2x_3 \oplus x_1x_3 \oplus 1$;
8) $\varphi_8(x_1,\ x_2,\ x_3) = x_1x_2 \oplus x_2x_3 \oplus x_1x_3$.

Обозначим через G множество функций, зависящих от переменных $x_1,\ x_2,\ x_3$ и имеющих вид $x_1^{\sigma_1}x_2^{\sigma_2} \vee x_1^{\sigma_1}x_3^{\sigma_3} \vee x_2^{\sigma_2}x_3^{\sigma_3}$ $(\sigma_i \in \{0, 1\},\ i \in \{1,\ 2,\ 3\})$. Отметим, что функции $\varphi_5, \varphi_6, \varphi_7, \varphi_8 \in G$.

Известно, что если полный конечный базис содержит функцию из множества G, то как при инверсных неисправностях на выходах элементов [3], так и при неисправностях типа 0 на выходах [4] элементов любую булеву функцию можно реализовать асимптотически оптимальной по надежности схемой (необходимые определения также можно найти в [4]), функционирующей с тривиальной оценкой ненадежности, асимптотически равной ε при $\varepsilon \to 0$. Ранее доказано [5], что этот же результат имеет место для базисов, содержащих функции φ_1, φ_3. В этой работе показано, что при неисправностях типа 0 на выходах элементов утверждение верно и для полных конечных базисов, содержащих функции φ_2, φ_4.

Далее будем считать, что все элементы полного конечного базиса B ненадежны, 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. То есть при этих неисправностях функциональный элемент на единичных наборах с вероятностью $1 - \varepsilon$ выдает 1, с вероятностью ε выдает 0, а на нулевых наборах элемент работает абсолютно надежно (с вероятностью 1 выдает 0, с вероятностью 0 выдает 1).

Теорема 1. *Пусть полный конечный базис содержит функцию* $\varphi_2(x_1, x_2, x_3) = x_1x_2 \oplus x_2x_3 \oplus x_1x_3 \oplus x_1 \oplus 1$ *или функцию* $\varphi_4(x_1, x_2, x_3) = x_1x_2 \oplus x_2x_3 \oplus x_1x_3 \oplus x_1 \oplus x_2 \oplus x_3$. *Тогда в этом базисе любую булеву функцию* f *можно реализовать такой схемой* A, *что* $P(A) \leqslant \varepsilon + 16\varepsilon^2$ *при всех* $\varepsilon \in (0, 1/480]$.

Из теоремы 1 следует, что в базисах, содержащих φ_2 или φ_4, любую булеву функцию можно реализовать схемой, ненадежность которой асимптотически не больше ε при $\varepsilon \to 0$.

Отметим, что 1) любая схема, содержащая хотя бы один функциональный элемент и реализующая отличную от константы 0 функцию, имеет ненадежность, не меньше ε [4]; 2) функции x_i $(i \in \mathbf{N})$ можно реализовать абсолютно надежно (не используя функциональных элементов). Следовательно, любую булеву функцию $f(x_1, x_2, ..., x_n)$ $(n \in \mathbf{N})$, исключая $x_1, x_2, ..., x_n$ и константу 0, можно реализовать схемой (см. теорему 1), которая является асимптотически оптимальной по надежности и функционирует с ненадежностью, асимптотически равной ε при $\varepsilon \to 0$.

Таким образом, из теоремы 1 и ранее полученных результатов [4; 5] следует, что если полный конечный базис содержит особенную функцию, то почти любую булеву функцию $f(x_1, x_2, ..., x_n)$ можно реализовать асимптотически оптимальной по надежности схемой, функционирующей с ненадежностью, асимптотически равной ε при $\varepsilon \to 0$.

Этот результат отличается от ранее известного результата для инверсных неисправностей на выходах элементов [3], поскольку для базиса, содержащего одну из функций $\varphi_1, \varphi_2, \varphi_3, \varphi_4$ и не содержащего ни одну из функций множества G, доказано, что почти любую булеву функцию можно реализовать асимптотически оптимальной по надежности схемой, функционирующей с ненадежностью, асимптотически равной 2ε при $\varepsilon \to 0$, т. е. в случае неисправностей типа 0 на выходах элементов имеем лучшую (в 2 раза) асимптотическую оценку ненадежности схем.

Работа выполнена при поддержке РФФИ (проект № 17-01-00451-а).

Список литературы

[1] Яблонский С. В. Введение в дискретную математику: учебное пособие для вузов / под ред. В. А. Садовничего. 3-е изд., стер. М. : Высш. шк., 2001. 384 с.

[2] Редькин Н. П. О полных проверяющих тестах // Математические вопросы кибернетики. 1989. Вып. 2. С. 198–222.

[3] Васин А. В. Асимптотически оптимальные по надежности схемы в полных базисах из трехвходовых элементов : дис. ... канд. физ.-мат. наук. Пенза, 2010. 100 с.

[4] Алехина М. А. Синтез асимптотически оптимальных по надежности схем : монография. Пенза : ИИЦ ПГУ, 2006. 156 с.

[5] 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» г. Пенза, 24–31 мая 2010 г.). Пенза : ИИЦ ПГУ, 2010. Т. 1. С. 229–232.

About the reliability of circuits in the basis containing a special function

Alekhina Marina Anatol'evna, Gusynina Yulia Sergeevna, Shornikova Tat'ana Aleksandrovna

Penza State Technological University, e-mail: alekhina@penzgtu.ru, gusynina@mail.ru, shornikovat@mail.ru

We consider the realization of Boolean functions by the circuits from unreliable gates in a complete final basis B, containing a special function. We assume that all gates of a circuit are exposed to the faults type 0 at the outputs with probability $\varepsilon \in (0, 1/2)$ independently of each other. We show that almost any Boolean function can be implemented by an asymptotically optimal in reliability circuit functioning with the unreliability which is asymptotically equal to ε with $\varepsilon \to 0$.

Keywords: unreliable functional gates, reliability and unreliability of circuit, synthesis of circuits composed of unreliable gates.

УДК 519.7

Применение метаэвристических алгоритмов псевдобулевой оптимизации к поиску линеаризующих множеств в криптоанализе криптографических генераторов

Антонов Кирилл Валентинович[1], **Семенов Александр Анатольевич**[2]

[1] Иркутский государственный университет, e-mail: aknitr@mail.ru

[2] Институт динамики систем и теории управления им. В. М. Матросова СО РАН, e-mail: biclop@rambler.ru

В статье рассматривается новый подход к построению атак типа «угадывай и определяй» на генераторы ключевого потока, основанный на понятии линеаризующего множества. Сложность атаки для конкретного линеаризующего множества оценивается как значение специально определённой псевдобулевой функции. Для решения задачи оптимизации псевдобулевой функции реализованы метаэвристические алгоритмы поиска: tabu search, генетический алгоритм, (1 + 1) эволюционный алгоритм, GBFS. Приведены оценки сложности атак указанного типа, которые были построены для поточных шифров A5/1 и ASG.

Ключевые слова: алгебраический криптоанализ, атаки из класса «угадывай и определяй», псевдобулева оптимизация, метаэвристические алгоритмы.

Понятие линеаризационного множества ввёл в 2003 году Г. П. Агибалов в работе [1]. Атаки на криптографические функции, использующие данное понятие, относятся к области, известной как алгебраический криптоанализ [2]. В алгебраическом криптоанализе задача обращения криптографической функции сводится к поиску решения системы алгебраических уравнений над некоторым конечным полем (чаще всего над $GF(2)$). Хорошо известно (см., например, [3]), что задача проверки совместности даже квадратичной системы уравнений над $GF(2)$ является NP-полной. Соответственно, в любом случае при решении таких систем приходится использовать переборную стратегию. Техника линеаризационных множеств, предложенная в [1], подразумевает ослабление систем уравнений, кодирующих криптоанализ рассматриваемой функции, до линейных систем засчёт подстановки угаданных значений некоторых переменных. Таким образом, атаки из [1] относятся к атакам типа «угадывай и определяй» (guess and determine) [2]. В целом ряде случаев множество угадываемых бит можно подобрать так, что трудоёмкость соответствующей атаки будет существенно ниже, чем при полном переборе вариантов секретного ключа.

Криптографический генератор ключевого потока — это дискретная функция вида

$$g : \{0,1\}^n \to \{0,1\}^*, \tag{1}$$

которая задаётся некоторым эффективным алгоритмом. Рассматриваются всюду определённые функции вида (1). Произвольный $\gamma \in \{0,1\}^m$ такой, что $\gamma = g(\alpha)$ для некоторого $\alpha \in \{0,1\}^n$, называется фрагментом ключевого потока длины m генератора g. С функцией (1) естественным образом связывается функция

$$f : \{0,1\}^n \to \{0,1\}^m, \tag{2}$$

область значений ($Range\ f$) которой совпадает с множеством всех возможных фрагментов ключевого потока длины m, порождаемых генератором (1). Задача обращения ключевого потока длины m генератора g ставится следующим образом: по известному $\gamma \in Range\ f$ требуется найти такой $\alpha \in \{0,1\}^n$, что $f(\alpha) = \gamma$.

Известно, что по алгоритму, задающему f, можно эффективно построить систему алгебраических уравнений степени не более 2 над полем $GF(2)$. Для этой цели можно использовать техники сводимости, подобные тем, которые были описаны в [4]. Пусть E_f — результирующая система и X — множество фигурирующих в ней булевых переменных. В X выделим два подмножества: $X^{in}, \left|X^{in}\right| = n$ и $Y, |Y| = m$. Переменные, образующие X^{in}, соответствуют входу f, а переменные из Y — её выходу. Результат подстановки в E_f известного $\gamma \in Rangef$ обозначим через $E_f(\gamma)$ (подстановка определяется стандартным способом — см., например [5]).

В соответствии с [1] назовём множество $X', X' \subset X$ линеаризационным, если для любого $\gamma \in Rangef$ и любого набора значений переменных из X' (используем обозначение $\beta \in \{0,1\}^{|X'|}$) подстановка β в $E_f(\gamma)$ даёт линейную систему. Таким образом, если X' — линеаризационнное множество, то задачу обращения произвольного $\gamma \in Rangef$ можно эффективно свести к решению $2^{|X'|}$ систем линейных уравнений над $GF(2)$. Известен целый ряд примеров, когда такая атака оказывается более эффективной, чем опробование всех 2^n возможных входов рассматриваемой функции.

Приведём один пример такого типа. Речь идёт об атаке, предложенной Россом Андерсоном [6] на известный генератор ключевого потока A5/1, который долгое время использовался для шифрования траффика в сетях сотовой связи. Данный алгоритм состоит из 3 несинхронно сдвигаемых регистров сдвига с линейной обратной связью (LFSR, [7]), детали его работы можно найти в многочисленных статьях, в том числе в Wikipedia. Р. Андерсон заметил, что угадывание 53 бит (все биты первого и третьего регистров и младшие 11 бит второго регистра) позволяет эффективно восстановить значения оставшихся 11 бит секретного ключа для любого фрагмента ключевого потока длины не менее 64. Несложно показать, что множество Андерсона — это линеаризационное множество в смысле [1].

В настоящей работе рассматривается одно обобщение понятия линеаризационного множества, которое можно построить, отталкиваясь от результатов

статьи [8]. В этой статье были введены т. н. «инверсные множества с лазейками» (Inverse Backdoor Sets, IBS). Концептуально, IBS — это (так же, как и линеаризационное множество) множество угадываемых бит в некоторой атаке типа «угадывай и определяй». Однако для решения ослабленных систем можно использовать алгоритм A решения какой-либо NP-трудной задачи, который работает быстро на значительной доле входов. В [8] для этой цели использовались алгоритмы решения задачи булевой выполнимости (SAT). Главная особенность описанных в [8] атак состоит в том, что не все ослабленные задачи должны быть простыми для алгоритма A. Эффективные IBS-атаки можно строить и для ситуаций, когда простой оказывается лишь некоторая доля от всех возможных ослабленных задач. Мы переносим эту идею на ситуацию, когда в роли A используется произвольный алгоритм решения линейных уравнений над $GF(2)$ (например, метод Гаусса). Получаемое в результате понятие отличается от понятия линеаризационного множества требованием, чтобы система вида $E_f(\gamma)$ линеаризовалась не любыми, а лишь некоторыми наборами значений переменных из X'.

С этой целью мы вводим специальную оценочную функцию, значения которой оценивают долю наборов из $\{0,1\}^{|X'|}$, линеаризующих системы вида $E_f(\gamma)$. Более точно, нам требуется оценить долю булевых векторов из $\{0,1\}^{|X'|}$ подстановка которых в $E_f(\gamma)$ обращает эту систему в линейную. Если эта доля относительно велика, то мы можем повторить нашу атаку применительно к нескольким различным выходам γ. В роли лазеек X' рассматриваются подмножества множества X^{in}. Каждое $X' \in 2^{X^{in}}$ можно задать булевым вектором длины n, в котором единицы отмечают те переменные из X^{in}, которые попадают в X'.

Рассмотрим N случайных входов функции f $\alpha_1, \ldots, \alpha_N$, выбранных из $\{0,1\}^n$ в соответствии с равномерным распределением. Построим выходы $\gamma_1, \ldots, \gamma_N : \gamma_j = f(\alpha_j), j \in \{1, \ldots, N\}$. Рассмотрим произвольное множество $X', X' \in X^{in}$. Тогда, входам α_j соответствуют наборы значений переменных из X', которые будем обозначать через $\beta_j, j \in \{1, \ldots, N\}$. Для входов $\alpha_1, \ldots, \alpha_N$ рассмотрим системы $E_f(\gamma_j, \beta_j), j \in \{1, \ldots, N\}$: каждая такая система получается в результате подстановки γ_j, β_j, порождённых α_j. Обозначим через δ долю систем вида $E_f(\gamma_j, \beta_j)$, которые являются линейными. Рассуждая по аналогии с [8], можем заключить, что δ — оценка вероятности следующего события: результат подстановки векторов γ_j и β_j, порождённых случайным входом $\alpha_j \in \{0,1\}^n$, в E_f — линейная система над $GF(2)$. Для фиксированного X' обозначим эту вероятность через $p_{X'}$.

Определение 1. *В контексте задачи обращения функции (2) назовём множество X' линеаризующим с вероятностью линеаризации $p_{X'}$.*

Таким образом, линеаризационное множество из [1] — это линеаризующее множество с вероятностью линеаризации 1.

С использованием $p_{X'}$ можно построить атаку из класса «угадывай и определяй» по смыслу близкую к атакам, описанным в [8] с той лишь разницей, что успехом в соответствующей последовательности испытаний Бернулли считается ситуация, когда выбран такой вход $\alpha \in \{0,1\}^n$, что $E_f(\gamma, \beta)$ — линейная система над $GF(2)$. Трудоёмкость такой атаки оценивается через оценку вероятности $p_{X'}$. С этой целью рассматривается специальная функция следующего вида:

$$\Phi : \{0,1\}^n \to \mathbb{R} \tag{3}$$

Функция (3) задаётся следующим образом. На вход она получает произвольный вектор $\chi \in \{0,1\}^n$, который задаёт множество X' (единицы в χ соответствуют переменным из X^{in}). Затем строится случайная выборка $\alpha_1, \ldots, \alpha_N$, по которой вычисляется величина δ. Данная величина принимается за оценку вероятности $p_{X'}$, на основании которой строится оценка трудоёмкости атаки из класса «угадывай и определяй», использующей множество угадываемых бит X'. Полученная оценка — значение функции (3).

Всё сказанное означает, что (3) — это псевдобулева функция [9]. Минимальное её значение на гиперкубе $\{0,1\}^n$ — это оценка трудоёмкости наиболее эффективной атаки. Для минимизации (3) мы использовали следующие метаэвристические алгоритмы: алгоритм, использующий поиск с запретами (tabu search, [10]) в том виде, как он описан в [11]; алгоритм, использующий стратегию GBFS (Greedy Best First Search, [11]), а также генетический алгоритм в варианте, который был использован в [13].

В вычислительных экспериментах рассматривались задачи построения линеаризующих множеств и соответствующих атак на следующие криптографические генераторы: A5/1, ASG96 и ASG192 (ASG — alternating step generator). У A5/1 анализировалось 114 бит выходного потока, у ASG92 — 112 бит, у ASG192 — 200 бит. Лучшие результаты экспериментов приведены в следующей таблице.

Таблица 1: Результаты экспериментов. GA — генетический алгоритм, TS — tabu search

Шифр	Алгоритм	Мощность множества	Сложность атаки (число решаемых систем ЛУ)	Вероятность
A5/1	GA	47	5.32e+15	0.0793
ASG96	GA, TS	31	6.44e+9	1
ASG192	GA, TS	65	1.11e+20	1

Из таблицы 1 видно, что лучшие результаты показали алгоритмы GA и TS. В случаях ASG96 и ASG192 эти алгоритмы в качестве множества X' построили множество переменных, которое кодирует управляющий регистр. Данный факт соответствует известной атаке на ASG. Для алгоритма A5/1 с использованием GA была построена атака, трудоёмкость которой примерно в 5 раз ниже, чем у атаки Андерсона. Особо подчеркнём, что в этом случае оценка вероятности $p_{X'}$ существенно меньше 1.

Работа выполнена при финансовой поддержке Российского научного фонда, проект №16-11-10046.

Список литературы

[1] Агибалов Г. П. Логические уравнения в криптоанализе генераторов ключевого потока // Вестник Томского государственного университета. Приложение. 2003. № 6. С. 31–41.

[2] Bard G. Algebraic cryptanalysis. 1st edition. Springer Publishing Company, Incorporated, 2009.

[3] Goldreich O. Computational Complexity: A Conceptual Perspective. Cambridge University Press, 2008.

[4] Otpuschennikov I., Semenov A., Gribanova I., Zaikin O., Kochemazov S. Encoding cryptographic functions to SAT using TRANSALG system // Frontiers in Artificial Intelligence and Applications. 2016. Vol. 285. P. 1594–1595.

[5] Чень Ч., Ли Р. Математическая логика и автоматическое доказательство теорем. М. : Наука, 1983. 360 с.

[6] Anderson R. A5 (Was: Hacking digital phones) / Newsgroup Communication. 1994. URL: http://yarchive.net/phone/gsmcipher.html.

[7] Alfred J. Menezes, Scott A. Vanstone, Paul C. Van Oorschot Handbook of Applied Cryptography. 1st ed. Boca Raton, FL, USA: CRC Press, Inc., 1996.

[8] Semenov A., Zaikin O., Otpuschennikov I., Kochemazov S., Ignatiev A. On cryptographic attacks using backdoors for SAT // The Thirty-Second AAAI Conference on Artificial Intelligence. 2018. P. 6641–6648.

[9] Boros E., Hammer P. L. Pseudo-Boolean optimization // Discrete Applied Mathematics. 2002. Vol. 123, N 1-3. P. 155–225.

[10] Glover F., Laguna M. Tabu Search. Kluwer Academic Publishers, 1997.

[11] Semenov A., Zaikin O. Algorithm for finding partitionings of hard variants of boolean satisfiability problem with application to inversion of some cryptographic functions // SpringerPlus. 2016. 5:554. P. 1–16.

[12] Норвиг П., Рассел С. Искусственный интеллект. Prentice Hall, 1994.

[13] Pavlenko A., Semenov A., Ulyantsev V. Evolutionary computation techniques for constructing SAT-based attacks in algebraic cryptanalysis. Lecture Notes in Computer Science. 2019. 11454. P. 237–253.

Applying Metaheuristic Pseudo-Boolean Optimization Algorithms to Search for Linearizing Sets in Cryptanalysis of Cryptographic Generators

Antonov Kirill Valentinovich[1], **Semenov Aleksandr Anatolevich**[2]

[1] Irkutsk State University, e-mail: aknitr@mail.ru

[2] Institute for System Dynamics and Control Theory SB RAS, e-mail: biclop@rambler.ru

In this paper we consider a new approach to the construction of guess-and-determine attacks on keystream generators based on the concept of linearizing sets. The complexity of the attack for a particular linearizing set is estimated as a value of a specially defined pseudo-Boolean function. To solve the optimization problem for the considered pseudo-Boolean function, various metaheuristic search algorithms are implemented: tabu search, genetic algorithm, (1 + 1) evolutionary algorithm, GBFS. For stream ciphers A5/1 and ASG the complexity estimates of the attacks of considered type are given.

Keywords: algebraic cryptanalysis, guess-and-determine attack, pseudo-boolean optimization, metaheuristic algorithms.

УДК 519.71

О классах эквивалентности мультифункций, порожденных частичными ультраклонами ранга 2

Бадмаев Сергей Александрович, Шаранхаев Иван Константинович, Шишмакова Кристина Александровна

Бурятский государственный университет, e-mail: badmaevsa@mail.ru, goran5@mail.ru, kristi-nomer1998@mail.ru

Найдено число классов эквивалентности мультифункций ранга 2, в частности булевых функций, порожденных максимальными частичными ультраклонами.

Ключевые слова: мультифункция, булева функция, частичный ультраклон, класс эквивалентности.

В теории дискретных функций активно исследуются мультифункции — функции, заданные на конечном множестве A и принимающие в качестве значений подмножества множества A. При определении суперпозиции для мультифункций на A, где $|A| = k$, мы по сути имеем дело с подмножеством множества всех функций 2^k-значной логики. Заметим, что обычная суперпозиция, которая рассматривается для функций многозначной логики, в данном случае не подойдет. К настоящему времени известны два вида суперпозиции для мультифункций [1; 2].

Пусть $A = \{0, 1\}$ и $F = \{\varnothing, \{0\}, \{1\}, \{0, 1\}\}$. Определим следующие множества функций:

$P^{\overline{*}}_{2,n} = \{f | f : A^n \to F\}, P^{\overline{*}}_2 = \bigcup\limits_n P^{\overline{*}}_{2,n}$,

$P_{2,n} = \{f | f \in P^{\overline{*}}_{2,n}$ и $|f(\tilde{\alpha})| = 1$ для всех $\tilde{\alpha} \in A^n\}, P_2 = \bigcup\limits_n P_{2,n}$.

Функции из P_2 называют булевы функциями, из $P^{\overline{*}}_2$ — мультифункциями на A.

Задача о принадлежности функций максимальным (предполным) классам является достаточно известной в теории дискретных функций, например, для булевых функций она решена в [3]. Используя разбиение множества всех функций на классы эквивалентности по отношению принадлежности максимальным классам, можно оценить мощности всевозможных базисов, описать все типы базисов.

В [4] описаны все максимальные частичные ультраклоны мультифункций на A. В докладе рассматривается вопрос о принадлежности мультифункций максимальным частичным ультраклонам. Количество максимальных частичных ультраклонов, равное 12, дает верхнюю оценку числа классов разбиения, как мощность множества всех подмножеств множества максимальных частичных ультраклонов, т. е. 2^{12}. Исследование свойств мультифункций

позволяет понизить эту оценку. Компьютерный эксперимент установил, что мультифункции от трех переменных дают 91 класс эквивалентности. Таким образом, нам удалось получить следующее утверждение.

Теорема 1. *Число классов мультифункций, порожденных отношением принадлежности максимальным частичным ультраклонам, равно 91.*

Если ограничиться рассмотрением подмножеств мультифункций, каждая из которых является булевой функцией, то получается следующее утверждение.

Теорема 2. *Число классов булевых функций, порожденных отношением принадлежности максимальным частичным ультраклонам, равно 15.*

Работа первого автора выполнена при поддержке РФФИ (проект № 18-31-00020).

Список литературы

[1] Перязев Н. А. Клоны, ко-клоны, гиперклоны и суперклоны // Ученые записки Казанского государственного университета. Серия Физико-математические науки. 2009. Т. 151, кн. 2. С. 120–125.

[2] Пантелеев В. И. Критерий полноты для доопределяемых булевых функций // Вестник Самарского государственного университета. Естественнонаучная серия. 2009. № 2 (68). С. 60–79.

[3] Яблонский С. В. О суперпозициях функций алгебры логики // Математический сборник. 1952. Т. 30 (72), № 2. С. 329–348.

[4] Бадмаев С. А. Критерий полноты множества мультифункций в полном частичном ультраклоне ранга 2 // Сибирские электронные математические известия. 2018. Т. 15. С. 450–474.

On equivalence classes of multifunctions generated by partial ultraclones of rank 2

Badmaev Sergey Alexandrovich, Sharankhaev Ivan Konstantinovich, Shishmakova Kristina Alexandrovna

Buryat State University, e-mail: badmaevsa@mail.ru, goran5@mail.ru, kristi-nomer1998@mail.ru

We found the number of equivalence classes of multifunctions of rank 2, in particular Boolean functions, generated by maximal partial ultraclones.

Keywords: multifunction, Boolean function, partial ultraclone, equivalence class.

УДК 519.714.1

О верхней оценке сложности трехзначных функций в классе поляризованных полиномов

Балюк Александр Сергеевич

ООО «Информатика медицины», г. Иркутск, e-mail: sacha@hotmail.ru

В работе с использованием компьютерных вычислений получены улучшенные асимптотические верхние оценки сложности трехзначных функций в классе поляризованных полиномов.

Ключевые слова: поляризованный полином, конечное поле, верхние оценки сложности.

Для произвольного элемента a некоторого кольца введем в рассмотрение величину $[a = 0]$, которая будет равна вещественной единице, если $a = 0$ в этом кольце, и вещественному нулю в противном случае. Обозначим среднее арифметическое непустого конечного множества S вещественных чисел как $\operatorname{avg} S$, а максимальный элемент в нем — $\max S$.

Пусть $\mathbb{F}_q$ — конечное поле порядка q. Множество невырожденных верхних треугольных $q\times q$ матриц над $\mathbb{F}_q$ обозначим $\mathbb{T}_q[q]$. Если $K \subseteq \mathbb{T}_q[q]$, то $K^{\otimes k} = \{M_1 \otimes \cdots \otimes M_k \mid M_1, \dots M_k \in K\}$, где $\otimes$ — кронекерово произведение матриц. Определим множество матриц $\mathcal{P} = \{P_a \mid a \in \mathbb{F}_q\}$, элементы которых равны $\binom{j-1}{i-1}a^{|j-i|}$, где i — номер строки, а j — номер столбца матрицы P_a. Читатель может легко убедиться, что $\mathcal{P} \subset T_q[q]$.

Каждую n-местную функцию над $\mathbb{F}_q$ будем отождествлять с некоторым вектором $f \in \mathbb{F}_q^N$, где $N = q^n$. Для каждого $f \in \mathbb{F}_q^N$ определим величины $Z(f) = \sum_{i=1}^{N}[f_i = 0]$ и $L^q_{K^\otimes}(f) = q^n - \max\{Z(M^{-1}f) \mid M \in K^{\otimes n}\}$, где $K \subseteq \mathbb{T}_q[q]$. Положим также $L^q_{K^\otimes}(n) = \max\{L^q_{K^\otimes}(f) \mid f \in \mathbb{F}_q^N, N = q^n\}$. Величину $L^q_{\mathcal{P}^\otimes}(f)$ назовем *сложностью функции f в классе поляризованных полиномов*. Выбор такого термина восходит к работам [1; 2].

Для случая $q = 3$, то есть для случая трехзначных функций, точное значение величины $L^q_{\mathcal{P}^\otimes}(n)$ неизвестно. Наилучшие на текущий момент нижняя и верхняя оценки были получены в работах [3] и [2] соответственно. Их можно свести в одну формулу $\left\lfloor \frac{3}{4}3^n \right\rfloor \leqslant L^3_{\mathcal{P}^{\otimes n}}(n) \leqslant \left\lfloor \frac{5}{6}3^n \right\rfloor$.

В настоящей работе с привлечением компьютерных вычислений верхнюю оценку удалось слегка уменьшить. Для начала сформулируем утверждение, которое обобщает теорему 1 из [2].

Теорема 1. *Пусть k — положительное целое, $N = q^k$, $K \subseteq \mathbb{T}_q[q]$ и для любой функции $f \in \mathbb{F}_q^N$ выполняется* $\operatorname{avg}\{Z(M^{-1}f) \mid M \in K^{\otimes k}\} \geqslant \beta + \delta[f_N = 0]$, *для некоторых вещественных $\beta > 0$ и $\delta \geqslant 0$. Тогда $L^q_{K^\otimes}(kn) \leqslant \lfloor (1-\alpha)q^{kn} \rfloor$, где $\alpha = \frac{\beta}{N-\delta}$.*

Для случая $q = 3$ были написаны компьютерные программы, которые вычисляют значения β и δ при $k = 2$ и $k = 3$.

Для $k = 2$ были получены следующие значения: $\beta = \frac{14}{9}$, $\delta = 1$. Тогда $\alpha = \frac{14}{9(9-1)} = \frac{7}{36}$ и $L^3_{\mathcal{P}^\otimes}(2n) \leqslant \left\lfloor \frac{29}{36} 3^{2n} \right\rfloor$. Таким образом, получаем асимптотическую оценку $L^3_{\mathcal{P}^\otimes}(n) \lesssim \frac{29}{36} 3^n$.

Для $k = 3$ программой были найдены следующие значения: $\beta = \frac{151}{27}$, $\delta = 1$. Тогда $\alpha = \frac{151}{27(27-1)} = \frac{151}{702}$ и $L^3_{\mathcal{P}^\otimes}(3n) \leqslant \left\lfloor \frac{551}{702} 3^{3n} \right\rfloor$, что дает асимптотическую оценку вида $L^3_{\mathcal{P}^\otimes}(n) \lesssim \frac{551}{702} 3^n$.

Эти оценки улучшают ранее известные, поскольку $\frac{551}{702} < \frac{29}{36} < \frac{5}{6}$.

Работа выполнена при поддержке РФФИ (проект № 19–01–00200).

Список литературы

[1] Селезнева С. Н. О сложности представления функций многозначных логик поляризованными полиномами // Дискретная математика. 2002. Т. 14, № 2. С. 48–53.

[2] Балюк А. С., Янушковский Г. В. Верхние оценки сложности функций над конечными полями в некоторых классах кронекеровых форм // Известия Иркутского государственного университета. Серия Математика. 2015. Т. 14. С. 3–17.

[3] Маркелов Н. К. Нижняя оценка сложности функций трехзначной логики в классе поляризованных полиномов // Вестник Московского университета. Серия 15, Вычислительная математика и кибернетика. 2012. № 3. С. 40–45.

On an upper bound for the complexity of three-valued functions in the class of polarized polynomials

Baliuk Aleksandr Sergeevich

LLC Informatics of Medicine, Irkutsk, e-mail: sacha@hotmail.ru

Using computer program results, improved asymptotic upper bounds have been obtained for the complexity of three-valued functions in the class of polarized polynomials.

Keywords: polarized polynomial, finite field, upper bounds for complexity.

УДК 512.55

Новый критерий о критичности некоторых конечных некоммутативных колец

Батзул Тумур, Ганхуяг Данзан

Монгольский университет науки и технологий, e-mail: must1204@gmail.com

В этой работе вводится понятие коммутатор-тождества конечных колец, через которое определяется максимальное коммутатор-подкольцо. С помощью данных определений формулируется и доказывается новый критерий о критичности некоторых конечных некоммутативных колец.

Ключевые слова: кольцо, полиномиальное тождество кольца, критическое кольцо, абелева группа

Введение

В настоящей работе сформулирован новый критерий о критичности некоторых некоммутативных конечных колец. Заметим, что первый пример конечного кольца, не представимого матрицами, дан Дж. Бергманом в работе [1]. Оно является кольцом эндоморфизмов.

Роль критического кольца в теории многообразий колец впервые показана в работах [6] и [5]. Далее критические кольца и алгебры изучались в работах [2–4; 7–12]. В этой работе мы формулируем новое семейство классов многочленов и некоторые понятия колец.

Основная часть

Прежде всего отметим следующие классические определения.

Определение 1. *Пусть* $Z(x_1, x_2, \ldots, x_n)$ *— кольцо многочленов от* x_1, $x_2, \ldots,$ x_n *переменных с целыми коэффициентами. Пусть* S *— некоторое кольцо и* $f(x_1, x_2, \ldots, x_n) \in Z(x_1, x_2, \ldots, x_n)$. *Многочлен* $f(x_1, x_2, \ldots, x_n)$ *называется полиномиальным тождеством кольца* S, *если* $f(a_1, a_2, \ldots, a_n) = 0$ *для всех* $a_1, a_2, \ldots, a_n \in S$.

Определение 2. *Пусть* S *— некоторое кольцо и* $g(x_1, x_2, \ldots, x_n) \in Z(x_1, x_2, \ldots, x_n)$. *Если многочлен* $g(x_1, x_2, \ldots, x_n)$ *не имеет полиномиального тождества кольца* S *и является полиномиальном тождеством над всеми подкольцами кольца* S, *то кольцо* S *называется критическим кольцом, а многочлен* $g(x_1, x_2, \ldots, x_n)$ *называется критическим многочленом кольца* S.

Замечание 1. *Пусть* $[x_1, x_2] = x_1x_2 - x_2x_1$. *Пусть* $J_1[x_1, x_2] = [x_1, x_2]$, $J_2(x_1, x_2, x_3, x_4) = [J_1(x_1, x_2), J_1(x_3, x_4)] = [x_1, x_2] \cdot [x_3, x_4] - [x_3, x_4] \cdot [x_1, x_2], \ldots,$

$$J_m(x_1, x_2, \ldots, x_{2^m}) = [J_{m-1}(x_1, x_2, \ldots, x_{2^{m-1}}), J_{m-1}(x_{2^{m-1}+1}, x_{2^{m-1}+2}, \ldots, x_{2^m})] =$$
$$= J_{m-1}(x_1, x_2, \ldots, x_{2^{m-1}}) J_{m-1}(x_{2^{m-1}+1}, x_{2^{m-1}+2}, \ldots, x_{2^m}) -$$
$$- J_{m-1}(x_{2^{m-1}+1}, x_{2^{m-1}+2}, \ldots, x_{2^m}) J_{m-1}(x_1, x_2, \ldots, x_{2^{m-1}}).$$

Многочлен J_m назовём m кратным коммутатор-тождеством. Из этого замечания следует, что

$$J_2(x_1, x_2, x_3, x_4) = (x_1x_2 - x_2x_1)(x_3x_4 - x_4x_3) - (x_3x_4 - x_4x_3)(x_1x_2 - x_2x_1)$$

или

$$J_2(x_1, x_2, x_3, x_4) = x_1x_2x_3x_4 - x_2x_1x_3x_4 - x_1x_2x_4x_3 + x_2x_1x_4x_3 -$$
$$- x_3x_4x_1x_2 + x_4x_3x_1x_2 + x_3x_4x_2x_1 - x_4x_3x_2x_1.$$

Теперь докажем следующую лемму

Лемма 1. *Пусть S — конечное кольцо. Тогда существует некоторое кратное коммутатор-тождество J_m такое, что J_m имеет полиномальное тождество кольца S.*

Доказательство. Если S коммутативное кольцо, то $J_1[x, y] = [x, y] = xy - yx = 0$ для всех $x, y \in S$. Пусть S — некоммутативное конечное кольцо. Пусть порядок кольца S равен $|S| = p_1 \cdot p_2 \cdot \ldots \cdot p_i$, где $p_1, p_2, \ldots, p_i$ — простые числа. Докажем индукцией по i.

I. Если $i = 1$ или p_1 — простое число и порядок кольца S равен p_1, то кольцо S является коммутативным кольцом. Поэтому J_1 имеет полиномиальное тождество кольца S.

II. Пусть k — некоторое целое положительное число. Тогда считаем, что если i любое положительное целое число ($i < k$), а $p_1, p_2, \ldots, p_i$ любые простые числа, то существуют кратные коммутатор-тождества каждых колец порядка $p_1 \cdot p_2 \cdot \ldots \cdot p_i$.

III. Пусть $q_1 \cdot q_2 \cdot \ldots \cdot q_k$ — некоторые простые числа, S — некоторое конечное некоммутативное кольцо, порядок S равен $|S| = q_1 \cdot q_2 \cdot \ldots \cdot q_k$, а 0 — нейтральный элемент кольца S. Пусть $r \in S$ и $r \neq 0$.

$$T = \{n_1r + n_2r^2 + \ldots + n_mr^m : 1 \leqslant m \in Z, n_1, n_2, \ldots, n_m \in Z\}.$$

Тогда T имеет коммутативное подкольцо кольца S. Из теоремы Лагранжа группы следует, что порядок кольца T делит порядок кольца S. Пусть $|T| = q_{t+1} \cdot \ldots \cdot q_t > 1$, $1 < t < k$.

Порядок фактор кольца S/T равен $S/T = q_1 \cdot q_t$. Из условия (II) следует, что существует кратное коммутатор-тождество J_m кольца S/T. Из определения следует,

$$J_m(y_1 + T, y_2 + T, \ldots, y_{2^m} + T) = 0 + T \text{ для каждых } y_1, \ldots, y_{2^m}. \qquad (1)$$

Пусть $a_1, \ldots, a_{2^m}, \ldots, a_{2^{m+1}} \in S$

$$\alpha = J_m(a_1, a_2, \ldots, a_{2^m}), \beta = J_m(a_{2^m+1}, a_{2^m+2}, \ldots, a_{2^{m+1}}).$$

Тогда из определения фактор-кольца следует

$$J_m(a_1 + T, a_2 + T, \ldots, a_{2^m} + T) = J_m(a_1, a_2, \ldots, a_{2^m}) + T = \alpha + T$$

и

$$J_m(a_{2^m+1} + T, a_{2^m+2} + T, \ldots, a_{2^{m+1}} + T) = \\ = J_m(a_{2^m+1}, a_{2^m+2}, \ldots, a_{2^{m+1}}) + T = \beta + T.$$

Поэтому из условия (1) следует $\alpha + T = 0 + T \in S/T$, $\beta + T = 0 + T \in S/T$ или $\alpha, \beta \in T$. T — коммутативное кольцо, поэтому $J_1(\alpha, \beta) = 0$ или

$$J_{m+1}(a_1, a_2, \ldots, a_{2_{m+1}}) = \\ = J(J_m(a_1, a_2, \ldots, a_{2_m}), J_m(a_{2^m+1}, a_{2^m+2}, \ldots, a_{2_{m+1}})) = J(\alpha, \beta) = 0.$$

Отсюда J_{m+1} имеет коммутатор-тождество кольца S. По принципу математической индукции лемма доказана. □

Следствие 1. *Пусть $p_1 \cdot p_2 \cdot \ldots \cdot p_i$ — простые числа, S — конечное некоммутативное кольцо, а порядок S равен $|S| = p_1 \cdot p_2 \cdot \ldots \cdot p_i$. Тогда существует положительное целое число m такое, что J_m имеет коммутатор-тождество кольца S и $1 < m \leqslant k$.*

Определение 3. *Пусть S — некоммутативное конечное кольцо. Если J_m не имеет коммутатор-тождество кольца S, а J_{m+1} имеет коммутатор-тождество кольца S, то J_m назовём внешним коммутатор-тождеством кольца S.*

Определение 4. *Пусть S — некоммутативное конечное кольцо, J_m — внешнее коммутатор-тождество кольца S, а T — подкольцо кольца S. Если T максимальное подкольцо удовлетворяет условию, что J_m имеет внешнее коммутатор-тождество, то кольцо T назовём максимальным коммутатор-подкольцом кольца S.*

Лемма 2 (Новый критерий критичности некоторых конечных некоммутативных колец)**.** *Пусть S — конечное некоммутативное кольцо, а T — максимальное коммутатор-подкольцо кольца S. Если T имеет подкольцо всех максимальных колец кольца S и фактор-кольцо S/T имеет критическое кольцо, то кольцо S является критическим кольцом.*

Доказательство. Из определения следует, что существует J_m такое, что

a) $J_m(x_1, x_2, \ldots, x_{2^m}) = 0$, для каждых $x_1, x_2, \ldots, x_{2^m} \in T$.

b) Существуют $a_1, a_2, \ldots, a_{2^m} \in S$ такие, что $J_m(a_1, a_2, \ldots, a_{2^m}) \neq 0$.

Кроме того, из определения критического кольца следует, что существует некоторый критический многочлен $f(x_1, x_2, \ldots, x_\nu)$ кольца S/T. Пусть

$$g(x_1, x_2, \ldots, x_{2^{m+\nu}}) = f\big(J_m(x_1, x_2, \ldots, x_{2^m}), \ldots \\ \ldots, J_m(x_{2^{m+\nu-2}+1}, x_{2^{m+\nu-2}+2}, \ldots, x_{2^{m+\nu-1}})\big).$$

Легко проверить, что тогда $g(x_1, x_2, \ldots, x_{2^{m+\nu}})$ имеет критическое тождество кольца S. Лемма доказана. □

Список литературы

[1] Bergman G. M. Some examples in PI ring theory // Israel Jour. Math. 1974. Vol. 18, N 3. P. 257–277.

[2] Мекей А. О критичности колец эндоморфизмов некоторых конечных абелевых групп // Фундаментальная и прикладная математика. 1996. Т. 2, вып. 2. С. 449–482.

[3] Генов Г. К., Сидеров П. Базис тождеств алгебры матриц четвертого порядка над конечным полем I // Серд. Бълг. мат. списание. 1982. Т. 8. С. 313–353.

[4] Генов Г. К., Сидеров П. Базис тождеств алгебры матриц четвертого порядка над конечным полем II // Серд. Бълг. мат. списание. 1982. Т. 8. С. 353–366.

[5] Kruse R. L. Identities satisfied by a finite ring // J. of algebra. 1973. Vol. 26. P. 298–318.

[6] Львов И. В. О многообразиях ассоциативных колец I // Алгебра и логика. 1973. Т. 12, № 3. С. 269–297.

[7] Латышев В. Н. Конечная базируемость тождеств некоторых колец // Успехи математических наук. 1976. Т. 32, № 4. С. 259–260.

[8] Мальцев Ю. Н. О строении некоторых критических колец // Сибирский математический журнал. 1984. Т. 25, № 1. С. 91–100.

[9] Мальцев Ю. Н. Кольцо матриц над критическим кольцом является критическим // УМН. 1984. Т. 39. Вып. 4(238). С. 171–172.

[10] Мальцев Ю. Н. О представлении конечных колец матрицами над коммутативным кольцом // Математический сборник. 1985. Т. 128(170), № 3. С. 383–402.

[11] Мальцев Ю. Н., Нечаев А. А. О критических кольцах многообразиях алгебр // Алгебра и логика. 1979. Т. 18, № 3. С. 341–347.

[12] Нечаев А. А. Описание конечных критических колец главных идеалов // Успехи математических наук. 1982. Т. 37, вып. 5(227). С. 193–194.

New criterion on criticality of particular finite noncommutative rings

Batzul Tumur, Gankhuyag Danzan

Mongolian University of Science and Technology , e-mail: must1204@gmail.com

This paper introduces commutator-identity of finite rings and maximal commutator-subring. We formulate and prove a new criterion on criticality of particular finite noncommutative rings using these definitions.

Keywords: ring, polynomial identity of a ring, critical ring, abelian group.

УДК 510.67, 519.24

О метриках многозначных логических высказываний и приложения метрик в базах знаний

Викентьев Александр Александрович

Новосибирский государственный университет, Институт математики им. С. Л. Соболева, e-mail: vikent@math.nsc.ru

В статье рассматриваются модели и формулы многозначных логик, имеющие различные применения в теории моделей и базах знаний, и, в частности для записи многозначных высказываний экспертов (логической базы знаний). С использованием методов математической логики и теории моделей для многозначных логик получены теоремы о богатых совокупностях формул (типов) без предположения стабильности (полной, метрической) многозначной модели, а с условием на класс ее расширений с той же (непрерывной) теорией рассмотрены и ортогональные случаи. Далее находятся «расстояния» на формулах (высказываниях) и степени (меры) нетривиальности (недостоверности) формулы как мера неверности формулы на классе рассматриваемых многозначных моделей (возможных миров). Изучены свойства введенных расстояний и мер нетривиальности (недостоверности) формул на классах многозначных моделей. Предложены различные способы задания на классах эквивалентных формул метрик, степеней нетривиальности (недостоверности) и установлены для них полезные свойства, которые используются в алгоритмах кластеризации, построении решающих функций, распознавании образов и вопроса об эталонах в искусственном интеллекте. Из этого дается описание всевозможных метрик при фиксированном классе конечнозначных моделей фиксированной многозначной логики и/или ее ослабления (уменьшением списка аксиом).

Ключевые слова: теория моделей, двукардинальные(богатые) формулы(типы), многозначные модели непрерывной логики, расстояния на логических формулах –высказываниях экспертов(базы знаний), релевантные модели, метрики на классах эквивалентности, меры недостоверности(нетривиальности), кластеризация, распознавание образов, искусственный интеллект.

В настоящее время изучаются теоретико-модельные метрики на множествах высказываний (базы знаний) многозначных и простейших семантически определенных релевантных логик с помощью релевантного класса моделей от переменных и их отрицаний. Решен вопрос об описании всех таких метрик, которые получаются с привлечением конечного релевантного класса моделей. Доклад посвящен также обобщению и уточнению результатов и теорем о двукардинальных (богатых) множествах типов, доказанных ранее в стабильном случае или с условиями стабильности, на случай многозначной и многосортной теории [1–3]. Некоторые из них вошли в диссертацию автора «Теории с покрытием и формульные подмножества» (ИМ СО РАН, Новосибирск, 1992, 134 с.) для семейств формул, а также опубликованы в сборнике Two cardinal theorems for sets of types in stable theory, посвященном 90-летию академика А. Д. Тайманова (Казахстан, Алма-Ата, 2007, с. 67–69), которые были представлены в Алма-Ате и Новосибирске на ежегодных Мальцевских чтениях с 2006 г., в том числе к 100-летию акад. А. И. Мальцева и др.

На случай богатых семейств типов над параметрами модели многосортной, многозначной теории с-компактными (насыщенными, однородными) измеримыми и вычислимыми моделями со свойством отделимости новых элементов, реализующих вычислимые типы (над малыми подмножествами модели) совместных с этими множествами, от элементов вложенной модели и наличия реализаций в большей (с богатым семейством) модели вполне определимых, вычислимых (стабильных) типов или неразличимых элементов. Стабильность теорий не предполагается, а многие известные теоремы в обычном случае получаются как следствия. Также дан обзор имеющихся результатов по применению многозначных исчислений для кластеризации множеств высказываний.

Основными инструментами доказательств являются теоремы типа компактности, развитая техника современной теории моделей, вычислимости, в частности, для логических исчислений, локальной стабильности и наличия (даже локально) подходящих компактных измеримых (нужных малых мощностей $varkappa$) моделей теории со свойствами $varkappa$-отделимости над реализациями семейств стабильных (определимых, рекурсивных) типов.

Продолжено изучение спектра и числа двукардинальных и предельных моделей в классе теорий с покрытиями введенных автором. Рассмотрены вопросы определимости систем с метрикой в наследственно конечных надстройках, и о мощностях типово определимых подмножеств и их свойств двукардинальности. Интерес к этим вопросам и таким моделям имеет и прикладной характер в поиске наиболее информативных (нетривиальных) типов (формул) прикладной теории, логических закономерностей для кластеризации и упорядочения таких «знаний» с помощью привлечения конечных, многозначных, метрических или измеримых систем и расстояний между множествами моделей.

Все это служит для введения новых метрик на классах неэквивалентных формул (логических высказываний экспертов или типов (совместных совокупностей высказываний) на измеримых подклассах измеримых, вычислимых (метрических, измеримых) моделей, необходимых для разработки алгоритмов распознавания образов, поиска закономерностей, обнаружения редких событий и кластеризации многозначных формул-знаний в различных логиках, например Лукасевича.

В настоящее время найдены различные теоретико-модельные новые метрики, разработаны методы кластеризации по метрикам для конечных множеств формул в различных логических исчислениях с привлечением различных подклассов релевантных моделей (частично совместно с аспирантом Авиловым М. С., Фефеловой В. В., Таганашкиной Л. А.), изучены различные индексы качества для сравнений и способы введения коллективных метрик. Проведены, вначале с Фефеловой В. В., модельные эксперименты с помощью

разработанной программы, поддерживающей все необходимые алгоритмы и нахождение по найденным расстояниям кластеризаций. Показано, что коллективные расстояния имеют более высокие индексы кластеризаций по сравнению с другими введенными метриками. В дальнейшем планируется использование лучших кластеризаций для локальной структуризации баз знаний. Новым шагом в приложениях наших подходов является использование различных малых конечных классов релевантных моделей, предложенных на Мальцевских чтениях автором доклада, и взятие по ним (в конечном числе) коллективного расстояния, которое обеспечивает эффективную и оптимальную коллективную кластеризацию данных множеств формул. Ответ на поставленный выше вопрос важен для полного учета различных расстояний для небольших конечных (малых) подклассов класса релевантных моделей, и будет использоваться в поисках лучшей из (разумных) возможных кластеризаций.

Теорема 1. *Найдены все способы задания теоретико-модельных метрик на формулах многозначной релевантной логики высказываний в классе конечных многозначных релевантных моделей (и при фиксированном размере N многозначной логики).*

Это позволяет проводить алгоритмы классификации таких высказываний, уменьшает трудоемкость алгоритма согласования решений и построения решающих функций.

Работа выполнена при финансовой поддержке РФФИ (проект № 18-07-600-а).

Список литературы

[1] Vikentiev A. A. Distances and Degrees of Uncertainty in Many-Valued Propositions of Experts and Application of These Concepts in Problems of Pattern Recognition and Clustering // Pattern Recognition and Image Analysis: Advances in Mathematical Theory and Applications. 2014. Vol. 24, N 4. P. 409-421.

[2] Викентьев А. А., Фефелова В. В. Новые модельные расстояния и меры достоверности формул логики Лукасевича в автоматической кластеризации высказываний баз данных // Algebra and Model Theory 10. Collection of papers / eds.: A. G. Pinus, K. N. Ponomaryov, S. V. Sudoplatov, and E. I. Timoshenko. Novosibirsk : NSTU, 2015. P. 197–209.

[3] Vikentiev A. A., Avilov M. C. New Model Distances and Uncertainty Measures for Multivalued Logic // Artificial Intelligence: Methodology,

Systems, and Applications. C. Dichev, G. Agre (eds.). Lecture Notes on Computer Science, LNCS 9883, 2016. P. 89–98.

On the Metrics on Multi-Valuable Logical Expression and Application of the Metrics in Databases

Vikentiev Alexandr Alexandrovich

Novosibirsk State University, Sobolev Institute of Mathematics SB RAS, e-mail: vikent@math.nsc.ru

The article discusses models and formulas of multivalued logics having various applications in model theory and knowledge bases, and, in particular, for recording ambiguous statements of experts (logical knowledge base). Using methods mathematical logic and model theory for multi-valued logics, theorems on rich collections of formulas (types) are obtained without assuming the stability of the (complete, metric) model, but with the condition on the class of its extensions with the same (continuous)theory, orthogonal cases are considered. We consider formulas of manyvalued logic. Further are « distances » on formulas (statements) and degrees (measures) nontriviality (uncertainty) of the formula, as a measure of the formula's infidelity on the class models under consideration (possible worlds). The properties of the introduced distances and measures of nontriviality (uncertainty) of formulas on classes of multivalued models. Methods autora proposed assignment on classes of nonequivalent formulas of metrics, degrees of nontriviality (uncertainty) and set useful properties for them, which are used in algorithms clustering, the construction of deciding functions, pattern recognition and the question of standards in artificial intelligence. From this description of all possible metrics is given for a fixed class of finite-valued models of a fixed many-valued logic and / or its weakening (by reducing the list of axioms).

Keywords: model theory, two-cardinal (rich) formulas (types), multivalued models of continuous logic, distances on logical formulas–expressions of experts (knowledge bases), relevant models, metrics on equivalence classes, measures of uncertainty(non-triviality), clustering, pattern recognition, artificial intelligence.

УДК 519.673

Приближенный алгоритм нахождения сложности обратимых реализаций расширенных кронекеровых форм булевых функций

Винокуров Сергей Федорович, Францева Анастасия Сергеевна

Иркутский государственный университет, e-mail: servin38@gmail.com, a.s.frantseva@gmail.com

В работе продолжается исследование задачи обратимых реализаций полиномиальных нормальных представлений булевых функций и приводится реализация алгоритма нахождения сложности обратимых реализаций расширенных кронекеровых форм булевых функций. Данные исследования представляют также теоретический интерес и могут быть использованы для нахождения неизвестной пока оценки значения функции Шеннона сложности представлений булевых функций в соответствующем классе обратимых реализаций.

Ключевые слова: функция Тоффоли, обратимые схемы, булевы функции, кронекерова форма.

Обратимым представлением булевой функции $f(x_1, ..., x_n)$ называется обратимая функция следующего вида:

$$F(x_0, x_1, ..., x_n) = (f_0(x_1, ..., x_n),\ f_1(x_1, ..., x_n),\ ...,\ f_n(x_1, ..., x_n)),$$

где

$$f_0(x_1, ..., x_n) = x_0 \oplus f(x_1, ..., x_n),$$

$$f_i(x_1, ..., x_n) = x_i \text{ по всем } 1 \leqslant i \leqslant n;$$

т.е. функция $F^r(x_0, x_1, ..., x_n)$ осуществляет следующее отображение:

$$(x_0, x_1, ..., x_n) \ \mapsto \ (x_0 \oplus f(x_1, ..., x_n), x_1, ..., x_n).$$

В работе рассматриваются следующие обратимые функции (функции Тоффоли):

$$\begin{aligned} T_0^{n+1}(x_i):&\ \ (x_0, x_1, ..., x_i, ..., x_n) \to (x_0, x_1, ..., \bar{x}_i, ..., x_n);\\ T_k^{n+1}(x_{i_1}, ..., x_{i_k}, x_0):&\ \ (x_0, x_1, .., x_n) \to (x_0 \oplus x_{i_1} \cdot ... \cdot x_{i_k}, x_1, ..., x_n),\\ &\ \ k \leqslant n,\ \{i_1, ..., i_k\} \subset \{1, ..., n\}. \end{aligned}$$

Любая обратимая функция $F(x_0, x_1, ..., x_n)$ представляется в виде суперпозиции функций Тоффоли [5].

Более подробно остальные определения, а также описание построения обратимых схем, реализующих обратимые функции указанного вида, можно прочесть, например в [3]. Вид обратимой схемы (выбранная последовательность элементов функций Тоффоли) зависит от вида полиномиального представления булевой функции. В [3] рассматриваются обратимые реализации

расширенных поляризованных полиномов Жегалкина (или ZhE-полиномов) булевой функции.

В данной работе рассматриваются расширенные кронекеровы формы булевых функций (класс EH), построение которых подробно описано с использованием операторного подхода и введением класса двупорожденных операторных пучков в [2; 4]. Класс EH включает в себя известный класс H кронекеровых форм.

Схематически обратимая схема, реализующая полином булевой функции, выглядит так, как показано на рисунке 1. Внутри блока F располагаются элементы функций Тоффоли T_0 и T_k. Элементы T_0 реализуют отрицания над переменными, элементы T_k — слагаемые полинома. Одним из условий построения обратимой схемы является условие совпадения значений на выходах y_i в схеме со значениями на входах x_i. Тогда с учетом вида EH-полинома булевой функции, для его обратимой реализации требуется, в отличие от обратимой реализации ZhE-полиномов, реализовывать отрицания каждого слагаемого EH-полинома.

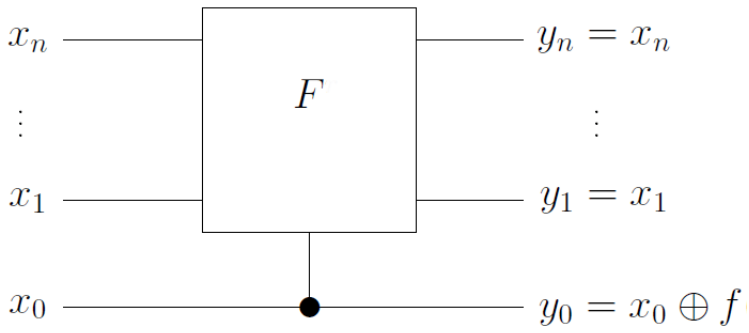


Рис. 1: Обратимая схема, реализующая булеву функцию $f(x_1, ..., x_n)$

Пусть S — обратимая схема, реализующая EH-полином P функции f. Схема S построена в соответствии с вышеприведенными рассуждениями. В ходе выполнения алгоритма в схеме S переставляются те ее части, что реализуют слагаемые EH-полинома. $l(S)$ — количество элементов функций Тоффоли T_0 и T_k, составляющих схему. Тогда под сложностью обратимой реализации EH-полиномов булевой функции будем понимать $\min_P l(S)$ по всем полиномам P класса EH, представляющим булеву функцию.

В соответствии с определением класса EH расширенных кронекеровых форм EH-полином P предполагает две формы: кронекерову и расширенную.

На шаге 1 и 2 алгоритма используется модифицированная версия алгоритма точной минимизации булевых функций в классе кронекеровых форм [1].

Алгоритм нахождения сложности обратимых реализаций EH-полиномов булевых функций

Входные данные: вектор булевой функции f

Выходные данные: минимальное значение $Cost$ сложности обратимых реализаций всех EH-полиномов функции f.

По всем базисам класса кронекеровых форм H:

1. Строится кронекерова форма Fh функции f и вычисляется количество слагаемых t.
2. Строится расширенная кронекерова форма Fe функции f и вычисляется количество слагаемых s.
3. Упорядочиваются в рефлексивном порядке слагаемые формы Fh.
4. В первом слагаемом вставляется отсутствующая (-ие) переменная (-ые) с отрицанием или без в соответствии с ближайшим следующим слагаемым, в котором эта переменная присутствует; в следующем слагаемом (и по всем остальным) вставляются переменные в соответствии с предыдущим слагаемым.
5. Вычисляется количество $n1$ элементов T_0 (отрицаний), необходимое для обратимой реализации каждого слагаемого полинома Fh.
6. Для каждого слагаемого, по порядку, подбирается из оставшихся слагаемых ближайшее следующее слагаемое, отличающееся в наименьшем количестве отрицаний, необходимых для его реализации.
7. Повторяется шаг 5 и вычисляется $n2$.
8. Из значений $n1$ и $n2$ выбирается меньшее n.
9. Выполняются шаги 3 - 8 для формы Fe и вычисляется количество отрицаний m.
10. Если $t + n < s + m$, и $t + n < Cost$, то $Cost = t + n$. Иначе если $s + m < Cost$, то $Cost = s + m$.

Время работы текущей реализации алгоритма для одной функции при $n = 8$ равно примерно 5 секунд.

Результаты алгоритма представлены в таблицах 1–4.

В таблице 4 приведены значения сложности обратимых реализаций EH-полиномов булевых функций, которые являются сложными в классах кронекеровых форм, расширенных кронекеровых форм.

Текущая реализация алгоритма тестировалась на булевых функциях при $n \leqslant 8$. Алгоритм предполагается использовать при n не более 16.

Таблица 1: Значения сложности функций при $n = 3$

Сложность	Количество функций
1	8
2	28
3	56
4	70
5	68
6	25

Таблица 2: Значения сложности функций при $n = 4$

Сложность	Количество функций
1	16
2	120
3	560
4	1820
5	4592
6	10052
7	15080
8	16251
9	12736
10	3876
11	432

Таблица 3: Значения сложности функций при $n = 5$ (представители классов эквивалентности по группе Джевонса)

Сложность	Количество функций
1	6
2	13
3	66
4	189
5	818
6	2378
7	7815
8	18457
9	45083
10	81304
11	150874

Сложность	Количество функций
12	186495
13	243675
14	201856
15	169425
16	78262
17	35027
18	5762
19	623
20	26
21	3

Таблица 4: Значения сложности Banchmarks-функций

Banchmarks-функции	Сложность		
	$n = 6$	$n = 7$	$n = 8$
«сложные» в классах H_b, H [2]	34	57	102
«сложные» в классах EH_b [4]	31	56	99
«сложные» в классе EH [4]	32	63	122

Список литературы

[1] Винокуров С. Ф., Рябец Л. В. Алгоритм точной минимизации булевых функций в классе кронекеровых форм // Алгебра и теория моделей 4. Новосибирск, 2003. С. 148–159.

[2] Избранные вопросы теории булевых функций / А. С. Балюк, С. Ф. Винокуров, А. И. Гайдуков, О. В. Зубков, К. Д. Кириченко, В. И. Пантелеев, Н. А. Перязев, Ю. В. Перязева ; под ред. С. Ф. Винокурова, Н. А. Перязева. М. : Физматлит, 2001. 192 с.

[3] Францева А. С. Алгоритм минимизации функций алгебры логики в классе обратимых схем Тоффоли // Известия Иркутского государственного университета. Серия Математика. 2018. Т. 25. С. 144–158. https://doi.org/10.26516/1997-7670.2018.25.144

[4] Францева А. С. Сложность представлений булевых функций в классах расширенных двупорожденных операторных форм // Сибирские электронные математические известия : электронное периодическое издание. 2019. Т. 16. С. 523–541. https://doi.org/10.33048/semi.2019.16.034

[5] Toffoli T. Reversible Computing // Automata Languages and Programming (Series: Lecture Notes in Computer Science). 1980. Vol. 85. P. 632–644. https://doi.org/ 10.1007/3-540-10003-2_104

An Approximate Algorithm for Finding the Complexity of Reversible Implementations Boolean Functions' Extended Kronecker Forms

Vinokurov Sergey Fedorovich, Frantseva Anastasiya Sergeevna

Irkutsk State University, e-mail: servin38@gmail.com, a.s.frantseva@gmail.com

In this paper, the research of the problem of reversible implementations of Boolean functions' polynomial normal representations (exclusive-or sum-of-products expressions) continues. An implementation of the algorithm for finding the complexity of reversible implementations Boolean functions' extended Kronecker forms is given. These researches are also theoretical interest and can be used to find an unknown estimate of the Shannon function's value of the complexity of Boolean functions' representations in the corresponding class of reversible implementations.

Keywords: Toffoli function, reversible circuits, Boolean functions, Kronecker form.

УДК 512.643, 512.552

Линейные отображения, сохраняющие матричные инварианты

Гутерман Александр Эмилевич

Московский государственный университет имени М. В. Ломоносова, e-mail: guterman@list.ru

Исследуются линейные отображения, сохраняющие матричные инварианты. Получена полная характеризация таких отображений для целого ряда инвариантов, свойств и отношений.

Ключевые слова: матрицы, инварианты матриц, линейные отображения.

Теория отображений, сохраняющих матричные инварианты, восходит к работе Фробениуса [1]. Для решения ряда задач теории представлений Фробениусу потребовалось охарактеризовать линейные отображения комплексных матриц, сохраняющие определитель. В дальнейшем эта теория получила уже самостоятельное развитие: в 1925 г. Шур [5] охарактеризовал линейные отображения, сохраняющие миноры фиксированного порядка, а в 1949 г. Дьедонне [2] охарактеризовал линейные отображения, сохраняющие множество вырожденных матриц. На сегодняшний день теория отображений, сохраняющих матричные инварианты, свойства и отношения — активно и интенсивно развивающаяся область математики, находящаяся в центре внимания математиков во всем мире, см., например [3; 4]. Во многом это определяется как разнообразием применяемых методов, так и целым рядом приложений. В докладе будет представлен обзор данного научного направления и изложены недавние результаты докладчика по этой теме. Планируется обсудить обобщения теорем Фробениуса, Шура и Дьедонне на матрицы над кольцами и полукольцами, отображения, сохраняющие отношения Грина, различные инварианты, возникающие в теории графов, в частности, скрамблинг индекс, индекс цикличности и др.

Список литературы

[1] Frobenius G. Über die Darstellung der endlichen Gruppen durch lineare Substitutionen. Sitzungsber., Preuss. Akad. Wiss (Berlin), Berlin, 1897. P. 994-1015.

[2] Dieudonné J. Sur une généralisation du groupe orthogonal á quatre variables // Arch. Math. 1949. Vol. 1. P. 282–287.

[3] Molnár L. Selected Preserver Problems on Algebraic Structures of Linear Operators and on Function Spaces, Lecture Notes in Mathematics 1895. B. : Springer-Verlag, 2007. 250 p.

[4] Pierce S. A survey of linear preserver problems // Linear and Multilinear Algebra. 1992. Vol. 33. P. 1–119.

[5] Schur I. Einige Bemerkungen zur Determinantentheorie. Akad. Wiss. Berlin : S.-Ber. Preuÿ, 1925. P. 454–463.

Linear transformations preserving matrix invariants

Guterman Aleksandr Emilevich

Lomonosov Moscow State University, e-mail: guterman@list.ru

Linear maps preserving matrix invariants are investigated. We characterize such maps for certain invariants, properties, and relations.

Keywords: matrices, matrix invariants, linear maps.

УДК 16(077)

Концепция фундирования в формировании, развитии и оценке логических универсальных учебных действий

Дулатова Зайнеп Асаналиевна, Лапшина Елена Сергеевна, Ковыршина Анна Ивановна, Штыков Николай Николаевич

Иркутский государственный университет, e-mail: dulatova@yandex.ru, esl7828@gmail.com, annkow@mail.ru, tukubik8@gmail.com

Статья посвящена описанию формально-логического подхода к формированию, развитию и оценке сформированности логических универсальных учебных действий (УУД) в процессе предметного обучения, основанного на реализации идеи фундирования. Определена концепция фундирования общелогических операций и базовых формально-логических операций и конструкций, в соответствии с которой выделены основные компоненты учебной деятельности школьников в освоении предмета. Возможности применения формально-логического подхода для оценки сформированности логического УУД продемонстрированы на примере действия «умение доказывать».

Ключевые слова: логические универсальные учебные действия, логическое мышление, школьное образование.

Работа посвящена поиску подхода к формированию, развитию и оценке сформированности логических универсальных учебных действий (УУД) в процессе предметного обучения в школе и подготовке будущих учителей к реализации этого подхода в образовательной деятельности. К логическим УУД традиционно относят следующие мыслительные операции и логические действия: анализ и синтез, сравнение, сериацию, классификацию, подведение под понятие, вывод следствий, построение логической цепи рассуждений, доказательство, выдвижение гипотез и их обоснование [2].

Анализ существующих методологических и методических подходов, методических и дидактических средств к формированию у обучающихся логических УУД показал, что они в основном ориентированы на неосознанное использование логических действий в учебном процессе, направленном на выполнение специально сконструированных заданий межпредметного характера, строящихся на содержании, выходящем за рамки школьных дисциплин [1–3]. При анализе учебных пособий для школьников по различным дисциплинам нами изучались формулировки определений, утверждений и условий заданий, описаний объектов (в том числе графических), отдельные умозаключения и цепочки умозаключений, входящие в рассуждения. Кроме того, оценивалось наличие заданий, целенаправленно требующих оценки, построения и преобразования различных суждений и умозаключений. В большей части школьных учебников, в том числе и в учебниках математики, в формулировках наблюдается однообразие и неполнота, практиче-

ски отсутствуют задания перечисленных видов, непосредственно направленные на формирование и развитие логических УУД. Исключение составляют учебники математики Г. В. Дорофеева, Л. Г. Петерсон, в которых есть задания некоторых указанных выше видов [4; 5]. Анализ ошибок, совершаемых выпускниками общеобразовательных организаций на государственных экзаменах (ОГЭ и ЕГЭ) по математике и обществознанию показал, что такой подход к организации предметного обучения, при котором требуется неосознанное выполнение логических УУД, не обеспечивает должного уровня развития логического мышления. Большая часть ошибок основана на неправильном преобразовании истинных суждений и правильных умозаключений. Наиболее часто встречаются ошибочные обращения, превращения, противопоставления субъекту и предикату для простых категорических суждений и соответствующих им непосредственных умозаключений. Также часто совершаются ошибки при построении суждений обратных, противоположных и обратно-противоположных для сложных импликативных суждений и соответствующих им умозаключений. Распространено также неправомерное обобщение суждений и неправильное построение отрицаний для простых и сложных суждений.

Разрабатываемый нами формально-логический подход к формированию и развитию логических УУД в процессе предметного обучения, основан на концепции фундирования логических структур и конструкций в теоретическом и практическом содержании дисциплины. Концепция фундирования в образовании была разработана В. Д. Шадриковым и Е. И. Смирновым как средство реализации инновационных технологий в процессе подготовки учителя математики [6]. Применительно к формированию, развитию и оценке сформированности логических УУД концепцию фундирования определим как процесс создания условий для актуализации базовых общелогических операций и базовых формально-логических операций и конструкций в обучении дисциплинам школьного цикла и их теоретическому обобщению в профессиональной подготовке учителя. Концепция фундирования общелогических операций и базовых формально-логических операций и конструкций предполагает развёртывание в процессе обучения школьников следующих компонентов:

- определение базовых общелогических операций и базовых формально-логических операций и конструкций, необходимых для освоения содержания школьной дисциплины и развития УУД на требуемом стандартом уровне;

- определение уровня и этапов сформированности базовых общелогических операций, базовых формально-логических операций и конструкций, логических УУД, соответствующих содержанию школьной дисциплины и возрастным особенностям обучающихся;

- определение технологии фундирования базовых общелогических операций, базовых формально-логических операций и конструкций в процессе предметного обучения.

Для теоретического обобщения в профессиональной подготовке учителя базовых логических конструкций, их преобразований и логических УУД необходимо соответствующим идее фундирования образом выстраивать курсы методики обучения предмету, логике или математической логике, методологии познания и других курсов методической и методологической направленности. Кроме того, желательно в процессе изучения всех дисциплин актуализировать, по мере возможностей, базовые общелогические операции и базовые формально-логические операции и конструкции и логические УУД, определённые во ФГОС общего образования, содействовать самостоятельному анализу логики в школьных дисциплинах и конструированию дидактических и методических материалов студентами в процессе научно-исследовательской работы.

Дифференциацию по уровням усвоения базовых логических операций и конструкций будем выстраивать с учетом возрастания сложности конструкций, пользуясь аналогией с уровнями усвоения понятия, разработанными советскими психологами [6; 7].

Исследования, посвящённые формированию действий анализа, синтеза, подведению под понятие при обучении математике, в педагогической литературе встречаются довольно часто. Однако мы не обнаружили в них такой конкретизации этих действий, которая бы позволила определить показатели и критерии для оценки сформированности умения выполнять эти действия обучающимися. Также в тех работах, которые декларируют направленность на формирование и развитие умения доказывать, из предложенных методик обучения и оценивания его результатов затруднительно выделить измеримые показатели и критерии оценки сформированности этого умения.

Опишем идею определения показателей и критериев для оценки сформированности логического УУД «умение доказывать». Каждое доказательство представляет собой цепочку умозаключений. Традиционно в формальной логике рассматриваются три вида умозаключений: дедуктивные, индуктивные и традуктивные. Правильные дедуктивные умозаключения характеризуются тем, что из истинных посылок с необходимостью следует истинность заключения. Выделим три показателя: умение оценивать правильность дедуктивных умозаключений, умение строить правильные дедуктивные умозаключения с заданными посылками и умение строить правильные дедуктивные умозаключения с заданным заключением. Критерии для этих показателей определяются типологией умозаключений по количеству и виду посылок (от непосредственного умозаключения из простой посылки до опосредованного умозаключения из двух и более сложных посылок) и типологией умозаклю-

чений по виду заключения. Заметим, что критерии не предназначены для упорядочивания логических действий по уровню сложности. Непосредственное умозаключение из одной простой посылки может оказаться сложнее, чем построение простого категорического силлогизма из двух посылок.

Список литературы

[1] Аджемян Г. А. Формирование универсальных учебных действий у младших подростков при выполнении математических заданий физического содержания : дис. ... канд. пед. наук. Москва, 2016. 277 с.

[2] Асмолов А. Г., Бурменская Г. В., Володарская И. А. Как проектировать универсальные учебные действия в начальной школе: от действия к мысли : пособие для учителя / под ред. А. Г. Асмолова. М. : Просвещение, 2008. 151 с.

[3] Боженкова Л. И. Познавательные универсальные учебные действия в обучении математике // Наука и школа. 2016. № 1. С. 54–60.

[4] Дорофеев Г. В., Петерсон Л. Г. Математика. 5 класс. Ч. 1. Изд. 2-е, перераб. М. : Ювента, 2011. 176 с.

[5] Дорофеев Г. В., Петерсон Л. Г. Математика. 5 класс. Ч. 2. Изд. 2-е, перераб. М. : Ювента, 2011. 240 с.

[6] Подготовка учителя математики: Инновационные подходы : учеб. пособие / под ред. В. Д. Шадрикова. М. : Гардрики, 2002. 383 с.

[7] Усова А. В. Формирование у школьников научных понятий в процессе обучения. М. : Педагогика, 1984. С. 50–105.

The conception of foundation in the formation, development and assessment of logical universal learning activities

Dulatova Zainep Asanalievna, Kovyrshina Anna Ivanovna, Lapshina Elena Sergeevna, Shtykov Nikolay Nikolaevich

Irkutsk State University, e-mail: dulatova@yandex.ru, esl7828@gmail.com, annkow@mail.ru, tukubik8@gmail.com

The article is devoted to the description of the formal logical approach to the formation, development and assessment of the formation of logical universal learning activities (ULE) in the process of in the process of subject teaching based on the implementation of the idea of foundation. The conception of foundation of general logical operations and basic formal logical operations and constructions is defined. In accordance with conception the main components of the learning activities of students in the subject study are identified. The possibilities of applying the formal logical approach to assess the formation of logical ULE are demonstrated by the example of the «ability to prove» action.

Keywords: logical universal learning actions, logical thinking, school education.

УДК 510.67

О композициях циклических плотных порядков со структурами и их алгебрах бинарных формул

Емельянов Дмитрий Юрьевич[1], Кулпешов Бейбут Шайыкович[2], Судоплатов Сергей Владимирович[3]

[1] Новосибирский государственный технический университет, e-mail: dima-pavlyk@mail.ru
[2] Международный университет информационных технологий, e-mail: b.kulpeshov@iitu.kz
[3] Институт математики им. С. Л. Соболева СО РАН, Новосибирский государственный технический университет, Новосибирский государственный университет, e-mail: sudoplat@math.nsc.ru

Рассматриваются композиции структур и композиции теорий для циклических плотных порядков и данных структур, а также сопутствующие алгебры. Доказано, что для любого I-группоида P, состоящего из неотрицательных меток, существует теория T с полным типом p и правильной меточной функцией $\nu(p)$ такая, что алгебра бинарных изолирующих формул над типом p представляется в виде композиции группоида над циклическим плотным порядком и группоида P.

Ключевые слова: композиция структур, композиция теорий, циклический плотный порядок, алгебра бинарных изолирующих формул

Алгебры бинарных формул изучены в серии статей как в общем случае [1–3], так и для теорий упорядоченных структур [4–7]. В работах [8–12] рассматривались различные аспекты теории циклически упорядоченных структур.

В настоящей работе мы рассматриваем композиции структур и композиции теорий для циклических плотных порядков и данных структур, а также сопутствующие алгебры.

Пусть $\mathcal{M}$ и $\mathcal{N}$ — структуры предикатных сигнатур $\Sigma_{\mathcal{M}}$ и $\Sigma_{\mathcal{N}}$ соответственно. Зададим композицию $\mathcal{M}[\mathcal{N}]$ структур $\mathcal{M}$ и $\mathcal{N}$, удовлетворяющую $\Sigma_{\mathcal{M}[\mathcal{N}]} = \Sigma_{\mathcal{M}} \cup \Sigma_{\mathcal{N}}$, $M[N] = M \times N$, а также следующим условиям:

1) если $R \in \Sigma_{\mathcal{M}} \setminus \Sigma_{\mathcal{N}}$, $\mu(R) = n$, то $((a_1, b_1), \ldots, (a_n, b_n)) \in R_{\mathcal{M}[\mathcal{N}]}$ тогда и только тогда, когда $(a_1, \ldots, a_n) \in R_{\mathcal{M}}$;

2) если $R \in \Sigma_{\mathcal{N}} \setminus \Sigma_{\mathcal{M}}$, $\mu(R) = n$, то $((a_1, b_1), \ldots, (a_n, b_n)) \in R_{\mathcal{M}[\mathcal{N}]}$ тогда и только тогда, когда $a_1 = \ldots = a_n$ и $(b_1, \ldots, b_n) \in R_{\mathcal{N}}$;

3) если $R \in \Sigma_{\mathcal{M}} \cap \Sigma_{\mathcal{N}}$, $\mu(R) = n$, то $((a_1, b_1), \ldots, (a_n, b_n)) \in R_{\mathcal{M}[\mathcal{N}]}$ тогда и только тогда, когда $(a_1, \ldots, a_n) \in R_{\mathcal{M}}$, или $a_1 = \ldots = a_n$ и $(b_1, \ldots, b_n) \in R_{\mathcal{N}}$.

Теория $T = \mathrm{Th}(\mathcal{M}[\mathcal{N}])$ называется *композицией* $T_1[T_2]$ теорий $T_1 = \mathrm{Th}(\mathcal{M})$ и $T_2 = \mathrm{Th}(\mathcal{N})$.

По определению композиция $\mathcal{M}[\mathcal{N}]$ получается заменой каждого элемента из $\mathcal{M}$ на копию структуры $\mathcal{N}$.

Композиция $\mathcal{M}[\mathcal{N}]$ называется *E-определимой*, если $\mathcal{M}[\mathcal{N}]$ имеет $\varnothing$-определимое отношение эквивалентности E, у которого E-классы являются носителями копий структуры $\mathcal{N}$, образующих $\mathcal{M}[\mathcal{N}]$. По определению каждая

E-определимая композиция $\mathcal{M}[\mathcal{N}]$ представляется в виде E-комбинации [13] копий структуры $\mathcal{N}$ с дополнительной структурой, порожденной предикатами из $\mathcal{M}$ и связывающими элементы копий структуры $\mathcal{N}$.

Заметим, что композиции сохраняют транзитивность теорий. Кроме того, если композиция $\mathcal{M}[\mathcal{N}]$ является E-определимой, то теория $\mathrm{Th}(\mathcal{M}[\mathcal{N}])$ однозначно определяет теории $\mathrm{Th}(\mathcal{M})$ и $\mathrm{Th}(\mathcal{N})$, и наоборот.

Пусть $\mathcal{C}$ — плотный циклический порядок. Соответствующая алгебра $\mathfrak{P}_{\mathrm{dco}}$ бинарных изолирующих формул имеет четыре метки, скажем 0, 1, 2, 3, где 0 используется для $x \approx y$, 1 для $x < y$ с углами меньше π, 2 для $x > y$ с углами больше π, и 3 для противоположных x и y на $\mathcal{C}$. Имеем $u \cdot 0 = 0 \cdot u = \{u\}$ for $u \in \{0, 1, 2\}$, $1 \cdot 1 = 2 \cdot 2 = \{1, 2, 3\}$, $1 \cdot 2 = 2 \cdot 1 = \{0, 1, 2, 3\}$, $1 \cdot 3 = 3 \cdot 1 = \{2\}$, $2 \cdot 3 = 3 \cdot 2 = \{1\}$, $3 \cdot 3 = \{0\}$.

Пусть λ — положительный кардинал, $\mathcal{M}_\lambda$ — результат замены в $\mathcal{C}$ каждого элемента на дизъюнктные антицепи A, имеющие мощность λ.

Ясно, что теория $T_\lambda = \mathrm{Th}(\mathcal{M}_\lambda)$ транзитивна, т. е. имеет единственный 1-тип.

Теперь поместим изоморфные структуры $\mathcal{N}$, с транзитивной теорией, на каждую антицепь A из $\mathcal{M}_\lambda$. Полученная структура является E-определимой композицией $\mathcal{M}_1[\mathcal{N}]$, имеющей транзитивную теорию. Она может быть рассмотрена как вариант транзитивного размещения структур [14].

Как показано в [1; 2], каждая алгебра $\mathfrak{P}$ бинарных изолирующих формул фиксированного типа является I-группоидом с неотрицательными метками и может быть реализована некоторой структурой $\mathcal{N}$ с транзитивной теорией, используя подходящую синтаксическую генерическую конструкцию.

Рассматривая композиции $\mathcal{M}_1[\mathcal{N}]$, получаем следующую теорему.

Теорема 1. *Для любого I-группоида $\mathfrak{P}$, состоящего из неотрицательных меток, существует теория T с типом $p \in S(T)$ и правильной меточной функцией $\nu(p)$ такая, что $\mathfrak{P}_{\nu(p)} = \mathfrak{P}_{\mathrm{dco}}[\mathfrak{P}]$.*

Работа выполнена при частичной финансовой поддержке Комитета науки Министерства образования и науки Республики Казахстан (грант № AP05132546), программы фундаментальных научных исследований СО РАН № I.1.1, проект № 0314-2019-0002, и Российского фонда фундаментальных исследований (проект 17-01-00531-а).

Список литературы

[1] Судоплатов С. В. Классификация счетных моделей полных теорий. Ч. 1. Новосибирск : НГТУ, 2018. 376 с.

[2] Shulepov I. V., Sudoplatov S. V. Algebras of distributions for isolating formulas of a complete theory // Siberian Electronic Mathematical Reports. 2014. Vol. 11. P. 380–407.

[3] Sudoplatov S. V. Algebras of distributions for semi-isolating formulas of a complete theory // Siberian Electronic Mathematical Reports. 2014. Vol. 11. P. 408–433.

[4] Кулпешов Б. Ш., Судоплатов С. В. Об алгебрах распределений бинарных изолирующих формул для вполне о-минимальных теорий // Известия НАН РК. Серия физико-математическая. 2015. Т. 300. № 2. С. 5–13.

[5] Emelyanov D. Yu., Kulpeshov B. Sh., Sudoplatov S. V. Algebras of distributions for binary formulas in countably categorical weakly o-minimal structures // Agebra and Logic. 2017. Vol. 56, N 1. P. 13–36.

[6] Baikalova K. A., Emelyanov D. Yu., Kulpeshov B. Sh., Palyutin E. A., Sudoplatov S. V. On algebras of distributions of binary isolating formulas for theories of abelian groups and their ordered enrichments // Russian Mathematics. 2018. Vol. 62, N 4. P. 1–12.

[7] Emelyanov D. Yu., Kulpeshov B. Sh., Sudoplatov S. V. On algebras of distributions for binary formulas for quite o-minimal theories // Algebra and Logic. 2018. Vol. 57, N 6.

[8] Kulpeshov B. Sh., Macpherson H. D., Minimality conditions on circularly ordered structures // Mathematical Logic Quarterly. 2005. Vol. 51, N 4. P. 377–399.

[9] Kulpeshov B. Sh. On $\aleph_0$-categorical weakly circularly minimal structures // Mathematical Logic Quarterly. 2006. Vol. 52, N 6. P. 555–574.

[10] Kulpeshov B. Sh. Definable functions in the $\aleph_0$-categorical weakly circularly minimal structures // Siberian Mathematical Journal. 2009. Vol. 5, N 2. P. 282–301.

[11] Kulpeshov B. Sh. On indiscernibility of a set in circularly ordered structures // Siberian Electronic Mathematical Reports. 2015. Vol. 12. P. 255–266.

[12] Kulpeshov B. Sh. On almost binarity in weakly circularly minimal structures // Eurasian Math. J. 2016. Vol. 7, N 2. P. 38–49.

[13] Sudoplatov S. V. Combinations of structures // The Bulletin of Irkutsk State University. Series Mathematics. 2018. Vol. 24. P. 65–84.

[14] Судоплатов С. В. Транзитивные размещения алгебраических систем // Сибирский математический журнал. 1999. Т. 40, № 6. С. 1347–1351.

On compositions of circular dense orders with structures and of their algebras of binary formulas

Emelyanov Dmitry Yuryevich[1], **Kulpeshov Beibut Shaiykovich** [2], **Sudoplatov Sergey Vladimirovich** [3]

[1] Novosibirsk State Technical University, e-mail: dima-pavlyk@mail.ru

[2] Kazakh-British Technical University, International Information Technology University, e-mail: b.kulpeshov@iitu.kz

[3] Sobolev Institute of Mathematics, Novosibirsk State Technical University, Novosibirsk State University, e-mail: sudoplat@math.nsc.ru

We consider compositions of structures and compositions of theories for circular dense orders and given structures, as well as related algebras. It is proved that for any I-groupoid P consisting of non-negative labels, there is a theory T with a complete type p and a regular label function $\nu(p)$ such that the algebra of binary isolating formulas over the type p is represented as a composition of a groupoid over a circular dense order and the groupoid P.

Keywords: composition of structures, composition of theories, circular dense order, algebra of binary isolating formulas.

УДК 519.7

Представление полиномиально устойчивых функций суммами бесповторных в элементарном базисе слагаемых

Зубков Олег Владимирович

Иркутский государственный университет, e-mail: oleg.zubkov@mail.ru

В работе рассматриваются полиномиально устойчивые булевы функции. Доказано, что бесповторные в элементарном базисе функции определенного вида являются полиномиально устойчивыми. Далее приведен алгоритм получения для любой полиномиальной устойчивой функции ее представления в виде суммы таких бесповторных функций.

Ключевые слова: булевы функции, бесповторные функции, полиномиальная устойчивость.

В работе рассматриваются полиномиально устойчивые булевы функции, введенные в рассмотрение в [1]. Напомним, что булева функция называется полиномиально устойчивой, если её вектор совпадает с вектором её же коэффициентов полинома Жегалкина при натуральном упорядочении двоичных наборов. Например, для функции $x_1 \vee x_2$ её вектор (0111) и вектор коэффициентов её полинома Жегалкина $x_2 \oplus x_1 \oplus x_1x_2$, маска которого имеет вид (0111) при порядке слагаемых $1, x_2, x_1, x_1x_2$, совпадают.

В [1] были доказаны некоторые свойства полиномиально устойчивых булевых функций. Основными являются следующие:

1. если f и g — полиномиально устойчивые, то $f \oplus g$ так же полиномиально устойчива.

2. если функция $f(x_1, x_2, \ldots, x_n)$ — полиномиально устойчивая, то $f(x_{i_1}, x_{i_2}, \ldots, x_{i_n})$, где $i_1, i_2, \ldots, i_n$ перестановка индексов $1, \ldots, n$, так же полиномиально устойчива.

3. если f и g — полиномиально устойчивые, то $f \otimes g$ так же полиномиально устойчива.

Из последнего свойства следует, что бесповторная конъюнкция двух полиномиально устойчивых функций $f(x_1, \ldots, x_k) \cdot g(x_{k+1}, \ldots, x_n)$ является полиномиально устойчивой.

Пример 1. Пусть $f = (0111\ 1001)$, $g = (0110)$.
Тогда $f(x_1, x_2, x_3) \cdot g(x_4, x_5) = (0000\ 0110\ 0110\ 0110\ 0110\ 0000\ 0000\ 0110)$ является полиномиально устойчивой.

Утверждение 1. *Пусть множество $X = \{x_1, \ldots, x_n\}$ разбито на подмножества $X_1, X_2, \ldots, X_m$ так, что $X_i \cap X_j = \varnothing$ при $i \neq j$ и $X_1 \cup \ldots \cup X_m = X$. Тогда бесповторная конъюнкция дизъюнкций переменных каждого класса разбиения вида*

$$\left(\bigvee_{x_i \in X_1} x_i\right) \cdot \left(\bigvee_{x_i \in X_2} x_i\right) \cdot \ldots \cdot \left(\bigvee_{x_i \in X_m} x_i\right) \tag{1}$$

является полиномиально устойчивой.

Пример 2. Пусть $n = 6$ и $X = \{x_1, x_4\} \cup \{x_2, x_5, x_6\} \cup \{x_3\}$. Тогда функция $(x_1 \vee x_4) \cdot (x_2 \vee x_5 \vee x_6) \cdot x_3$ является полиномиально устойчивой, в чем можно убедиться непосредственной проверкой.

Доказательство. Пусть дано разбиение $X_1, X_2, \ldots X_m$, причём $|X_i| = n_i$. Построим разбиение $X'_1, X'_2, \ldots X'_m$, так, что первые n_1 переменных $x_1, \ldots, x_{n_1}$ содержатся в X'_1, следующие n_2 переменных $x_{n_1+1}, \ldots, x_{n_1+n_2}$содержатся в X'_2 и т. д. Согласно вышеупомянутому свойству 3 полиномиально устойчивых функций и, принимая во внимание, что многоместная дизъюнкция любой размерности является полиномиально устойчивой, получим, что для любого j от 1 до m функция

$$\left(\bigvee_{x_i \in X'_1} x_i\right) \cdot \ldots \cdot \left(\bigvee_{x_i \in X'_j} x_i\right)$$

является полиномиально устойчивой. Возьмем $j = m$ и переставим в этой формуле переменные требуемым для получения исходного разбиения образом. Согласно свойству 2, при перестановке полиномиальная устойчивость сохранится. □

Далее перейдём к обоснованию утверждения о том, что любую полиномиально устойчивую булеву функцию можно представить в виде суммы бесповторных конъюнкций вида (1), возможно несколькими способами.

В [1] было введено обозначение для $f = \overline{x}_i f^0_{x_i} \oplus x_i f^1_{x_i}$ в виде $f = \begin{pmatrix} f^0_{x_i} \\ f^1_{x_i} \end{pmatrix}$. Кроме того, было показано, что любая полиномиально устойчивая булева функция f имеет вид $\begin{pmatrix} c(f^1_{x_i}) \\ f^1_{x_i} \end{pmatrix}$, где $c(h) = h \oplus P(h)$, и $P(h)$ — булева функция, вектор которой совпадает с вектором коэффициентов полинома Жегалкина для h при натуральном упорядочении наборов. Функция $c(h)$ является полиномиально устойчивой, а h принадлежит её классу.

Разложим f по двум переменным:

$$f = \begin{pmatrix} f^0_{x_i} \\ f^1_{x_i} \end{pmatrix} = \begin{pmatrix} f^{0\,0}_{x_i x_j} \\ f^{0\,1}_{x_i x_j} \\ f^{1\,0}_{x_i x_j} \\ f^{1\,1}_{x_i x_j} \end{pmatrix} = \begin{pmatrix} c(f^{0\,1}_{x_i x_j}) \\ f^{0\,1}_{x_i x_j} \\ f^{1\,0}_{x_i x_j} \\ f^{1\,1}_{x_i x_j} \end{pmatrix} = \begin{pmatrix} c(g_1) \\ g_1 \\ g_2 \\ g_3 \end{pmatrix}, \text{ где } g_1 = f^{0\,1}_{x_i x_j}.$$

Рассмотрим функцию $g = \begin{pmatrix} c(g_1) \\ g_1 \\ g_1 \\ g_1 \end{pmatrix}$. Так как $c \begin{pmatrix} g_1 \\ g_1 \end{pmatrix} = \begin{pmatrix} c(g_1) \\ g_1 \end{pmatrix}$, то функция g является полиномиально устойчивой. Полиномиально устойчивая функция $\begin{pmatrix} c(g_1) \\ g_1 \end{pmatrix} = f^0_{x_i}$ зависит от переменных $x_1, \ldots, x_{i-1}, x_{i+1}, \ldots, x_n$. Подставим в эту функцию вместо переменной x_j выражение $x_i \vee x_j$ и получим формулу $\Phi = f^0_{x_i}(x_1, \ldots, x_{i-1}, x_{i+1}, \ldots, x_{j-1}, x_i \vee x_j, x_{j+1}, \ldots, x_n)$. Покажем, что эта формула реализует функцию g. Действительно, $\Phi^{0\,0}_{x_i x_j} = f^{0\,0}_{x_i x_j} = c(g_1)$, $\Phi^{0\,1}_{x_i x_j} = \Phi^{1\,0}_{x_i x_j} = \Phi^{1\,1}_{x_i x_j} = f^{0\,1}_{x_i x_j} = g_1$.

Далее рассмотрим функцию $h = f \oplus g$. Так как h является суммой двух полиномиально устойчивых функций, то и сама она полиномиально устойчива. Очевидно, что $h^0_{x_i} = 0$, $h^1_{x_i} = \begin{pmatrix} g_2 \oplus g_1 \\ g_3 \oplus g_1 \end{pmatrix}$, и так как $c\left(h^1_{x_1}\right) = 0$, то и сама $h^1_{x_i}$ тоже полиномиально устойчивая. При этом $h = x_i \cdot h^1_{x_i}$.

В итоге получаем, что любую полиномиально устойчивую булеву функцию $f = g \oplus h$ можно представить в виде формулы над двумя полиномиально устойчивыми функциями меньшей размерности $f^0_{x_i}$ и $h^1_{x_i}$:

$$f = f^{0\;x_i \vee x_j}_{x_i\;\;x_j} \oplus x_i \cdot h^1_{x_i}. \tag{2}$$

Утверждение 2. *Любую полиномиально устойчивую функцию, за исключением тождественного нуля, можно представить в виде суммы бесповторных конъюнкций вида (1), возможно несколькими способами.*

Доказательство. При получении для полиномиально устойчивой булевой функции f разложения (2) используются две полиномиально устойчивые функции $f^0_{x_i}$ и $h^1_{x_i}$, размерность которых меньше исходной как минимум на единицу. Если они являются унарными, то первое слагаемое в (2) превращается в дизъюнкцию, а второе в конъюнкцию двух переменных. Оба эти слагаемых имеют вид (1).

Если $f^0_{x_i}$ и $h^1_{x_i}$ не унарные, то каждую из них представим в виде суммы слагаемых вида (1) и подставим это представление в (2) для основной функции f. В левой части полученной формулы вместо одной из переменных появится дизъюнкция двух переменных, в правой части формулы каждое слагаемое

умножится на x_i. И в том и в другом случае каждое слагаемое полученной формулы сохранит вид (1). □

Пример 3. Пусть $f = (0110\ 1101\ 1100\ 1110)$.
$f = (0110\ 1101\ 1101\ 1101) \oplus (0000\ 0000\ 0001\ 0011) = g \oplus h$.
$f^0_{x_1} = (0110\ 1101) = (0110\ 1010) \oplus (0000\ 0111) = g_1 \oplus h_1$.
$f^{0\,0}_{x_1x_2} = (0110) = (0111) \oplus (0001) = (x_3 \vee x_4) \oplus x_3x_4$.
$g_1 = (x_2 \vee x_3 \vee x_4) \oplus (x_2 \vee x_3)x_4$.
$h_1 = x_2(x_3 \vee x_4)$.
$g = (x_1 \vee x_2 \vee x_3 \vee x_4) \oplus (x_1 \vee x_2 \vee x_3)x_4 \oplus (x_2 \vee x_2)(x_3 \vee x_4)$.
$h^1_{x_1} = (0001\ 0011) = (0001\ 0101) \oplus (0000\ 0110) = g_2 \oplus h_2$.
$g_2 = (x_2 \vee x_3)x_4$.
$h_2 = x_2(x_3 \vee x_4) \oplus x_2x_3x_4$.
$h = x_1(x_2 \vee x_3)x_4 \oplus x_1x_2(x_3 \vee x_4) \oplus x_1x_2x_3x_4$.
$f = (x_1 \vee x_2 \vee x_3 \vee x_4) \oplus (x_1 \vee x_2 \vee x_3)x_4 \oplus (x_2 \vee x_2)(x_3 \vee x_4) \oplus x_1(x_2 \vee x_3)x_4 \oplus$
$\oplus x_1x_2(x_3 \vee x_4) \oplus x_1x_2x_3x_4$.

Следствие 1. *Любую булеву функцию можно представить в виде суммы бесповторных конъюнкций вида (1), в каждой из которых, возможно, отсутствует один сомножитель.*

Доказательство. Для любой булевой функции f можно построить полиномиально устойчивую функцию $\begin{pmatrix} c(f) \\ f \end{pmatrix}$, после чего реализовать её в виде суммы слагаемых вида (1). Подставляя в этом представлении 1 на место дополнительной переменной, получим, что из каждого слагаемого, возможно, удалится один сомножитель. □

Список литературы

[1] Зубков О. В. О классе полиномиально устойчивых булевых функций и их свойствах // Синтаксис и семантика логических систем : материалы 5-й Российской школы-семинара (Улан-Удэ, 8-12 августа 2017 г.). Улан-Удэ : Изд-во БГУ, 2017. С. 87–91

Representation of polynomially stable functions by sums of Boolean read-once functions over the elementary basis

Zubkov Oleg Vladimirovich

Irkutsk State University, e-mail: oleg.zubkov@mail.ru

The paper considers polynomially stable Boolean functions. Proved that Boolean read-once functions over the elementary basis of a certain kind are polynomially stable. The following is an algorithm for obtaining for any polynomial stable function its representation as a sum of such Boolean read-once functions.

Keywords: boolean functions, read-once functions, polynomial stability.

УДК 519.7

О сложности мультиопераций ранга k в классе стандартных форм

Казимиров Алексей Сергеевич

Иркутский государственный университет, e-mail: a.kazimirov@gmail.com

Мультиоперации ранга k определяются как функции на множестве всех подмножеств некоторого k-элементного множества A, при этом значения мультиоперации на наборах из A задаются, а на остальных наборах определяются как объединение всех значений мультиопераций на соотвествующих наборах из A. Таким же образом определяется суперпозиция для мультиопераций. Мультиоперации являются обобщением различных моделей неопределенности, частичных и гипероопераций. Для мультиопераций можно определить стандартные формы через мультиоперацию пересечения. Для них можно естественным образом ввести понятие сложности по количеству компонент пересечения. Ранее была найдена сложность стандартных форм мультиопераций ранга 2 сведением к длине наикратчайшей ДНФ. В данной работе обобщается предыдущий результат на мультиоперации ранга k.

Ключевые слова: мультиоперации, сложность, стандартные формы.

Мультиоперации ранга k определяются как функции на множестве 2^A ($|A| = k$), при этом значения мультиоперации на наборах из A задаются, а на остальных наборах определяются как объединение всех значений мультиопераций на соответствующих наборах из A. Таким же образом определяется суперпозиция для мультиопераций.

Мультиоперации являются обобщением различных моделей неопределенности, частичных и гипероопераций.

Для мультиопераций можно определить стандартные формы через мультиоперацию пересечения. Для них можно естественным образом ввести понятие сложности по количеству компонент пересечения.

Ранее [1] была найдена сложность стандартных форм мультиопераций ранга 2 сведением к длине наикратчайшей ДНФ. В данной работе обобщается предыдущий результат на мультиоперации ранга k.

Отображение из A^n в A называется n-местной операцией на A. Через 2^A обозначим множество всех подмножеств A. Отображение из A^n в 2^A называется n-местной мультиоперацией на A. Множество всех n-местных мультиопераций на A при $|A| = k$ будем обозначать H_k^n.

Суперпозиция мультиопераций определяется следующим образом

$$(f * (f_1, \ldots, f_n))(a_1, \ldots, a_m) = \bigcup_{b_i \in f_i(a_1,\ldots,a_m)} f(b_1, \ldots, b_n).$$

Следуя [2], n-местную мультиоперацию f на множестве $A = \{a_1, a_2, \ldots, a_k\}$ будем представлять как отображение

$$f : \{2^0, 2^1, \ldots, 2^{k-1}\}^n \to \{0, 1, \ldots, 2^k - 1\},$$

используя следующую кодировку для элементов 2^A:

$$\varnothing \to 0;\ \ a_i \to 2^i;\ \ \{a_{i_1}, \ldots, a_{i_s}\} \to 2^{i_1} + \ldots + 2^{i_s}.$$

При этом n-местную мультиоперацию f можно задать вектором всех ее значений $(\alpha_1, \ldots, \alpha_{k^n})$, где $f(2^{a_1}, \ldots, 2^{a_n}) = \alpha_i$, если $(i_1, \ldots, i_n)$ есть представление числа i в системе счисления с основанием k.

Определим бинарную мультиоперацию ранга k «пересечение» $\cap$ следующим образом: $\cap(a, b) = \{a\} \cap \{b\}$. Далее будем использовать инфиксную форму записи для пересечения. Эта мультиоперация является коммутативной и ассоциативной, а также принадлежит любому суперклону [3], что делает естественным использование $\cap$ для построения формульных представлений мультиопераций.

Обочначим через $d^n_{i,\alpha}$ следующие мультиоперации

$$d^n_{i,\alpha} = (2^k - 1, \ldots, 2^k - 1, \overset{i}{\alpha}, 2^k - 1, \ldots, 2^k - 1), \quad (1 \leqslant i \leqslant k^n),$$

где $\alpha \in \{0, \ldots, 2^k - 1\}$. В частности, $d^0_{1,\alpha} = (\alpha)$.

В [4] была введена стандартная форма мультиоперации

$$f(x_1, \ldots, x_n) = \bigcap_j d_j(x_{i_1}, \ldots, x_{i_m}),$$

где $d_j \in \{d^m_{i,\alpha} \,|\, 0 \leqslant m \leqslant n, \alpha \in \{0, \ldots, 2^k - 1\}\}$. Представление мультиопераций стандартной формой не единственно.

Для стандартной формы Φ, имеющей вид

$$\Phi = d_1 \cap \ldots \cap d_s,$$

где $d_j \in \{d^m_{i,\alpha} \,|\, 0 \leqslant m \leqslant n, \alpha \in \{0, \ldots, 2^k - 1\}\}$, можно ввести понятие сложности через количество компонент пересечения $L_{SF}(\Phi) = s$.

Для мультиоперации f ранга k сложность определяется как сложность минимальной стандартной формы, представляющей f:

$$L_{SF_k}(f) = \min_{f=\Phi} L_{SF}(\Phi).$$

Сложность класса всех n-местных мультиопераций ранга k (функция Шеннона сложности мультиопераций) определяется как сложность n-местной мультиоперации с наибольшей сложностью:

$$L_{SF_k}(n) = \max_{f \in H^n_k} L_{SF_k}(f).$$

Для любой n-местной мультиоперации f ранга k выполняется $L_{SF_k}(f) \leqslant k^n$.

Рассмотрим последовательность мультиопераций $f_n(x_1, \ldots, x_n)$, которая определяется следующим образом:

$$f_n(a_1, \ldots, a_n) = 2^k - 1 - 2^a, \qquad a = (a_1 + \ldots + a_n) \pmod{k}.$$

Мультиоперации из данной последовательности имеют следующую сложность:

Теорема 1. $L_{SF_k}(f_n) = k^n$.

С учетом верхней оценки сложности можно сделать следующий вывод:

Следствие 1. $L_{SF_k}(n) = k^n$.

Список литературы

[1] Казимиров А. С. О сложности стандартных форм мультифункций // Известия Иркутского государственного университета. Серия Математика. 2017. Т. 22. С. 63–70.

[2] Перязев Н. А. Клоны, ко-клоны, гиперклоны и суперклоны // Ученые записки Казанского государственного университета. Серия Физико-математические науки. 2009. Т. 151, кн. 2. С. 120–125.

[3] Перязев Н. А. Стандартные формы мультиопераций в суперклонах // Известия Иркутского государственного университета. Серия Математика. 2010. Т. 3, № 4. С. 88–95.

[4] Перязев Н. А. Суперклоны мультиопераций // Труды VIII Международной конференции «Дискретные системы в теории управляющих систем». М. : МАИС Пресс, 2009. С. 233–238.

On the Complexity of Standard Forms for Multioperations of rank k

Kazimirov Alexey Sergeevich

Irkutsk State University, e-mail: a.kazimirov@gmail.com

Multioperations of rank k are defined as functions mapping k-element set A to the set of all its subsets. Values of a multioperation for inputs equal to one-element sets are given and values for other sets are calculated as a union of values on one-element sets. Superposition of multioperations is defined in the same way. Multioperation is a generalization of different models of uncertainty, incomplete and partial operations and hyperoperations. Standard forms representing multioperations are defined using intersection multioperation. It is natural to define complexity of a standard form as the number of its components. This paper generalizes previous exact bounds on complexity of n-ary multioperations of rank 2 to multioperations of rank k.

Keywords: multioperation, complexity, standard form.

УДК 519.832.3

Анализ адаптивных алгоритмов для повторяющихся матричных игр

Кириченко Константин Дмитриевич

Иркутский государственный университет, e-mail: constkir@gmail.com

В работе рассматривается ситуация повторяющихся матричных игр двух игроков. Предполагается, что первым игроком является компьютерная программа, второй же игрок может принадлежать одному из двух типов: «взломщик» — игрок который знает алгоритм, реализованный в программе, и оптимально ему противодействует; «простец» — игрок, который не знает оптимальной стратегии или не способен ее реализовать. При этом, первый игрок не знает количество повторений игры, а также своего противника. Ставится задача: ограничив возможный проигрыш взломщику, добиться существенного выигрыша у простеца. Показано, что определение реакции программы на действия противника является нетривиальной задачей. Приводится пример интуитивно хорошего алгоритма оптимальная стратегия противодействия которому тем не менее приводит к существенному проигрышу.

Ключевые слова: матричные игры, повторяющиеся игры, адаптивные стратегии.

В работе рассматривается ситуация повторяющихся матричных игр двух игроков. Предполагается, что первым игроком является компьютерная программа, которая реализует ту или иную стратегию «угадывания» хода противника, а второй игрок не определен и, в частности, может быть человеком. Под угадыванием хода понимается, что в реализации программы явно или неявно присутствует вероятностная модель принятия решений противником. При этом, игра является не совсем симметричной, а именно: первый игрок не знает количество повторений игры, второй же игрок имеет право прервать игру и зафиксировать выигрыш в любой момент, когда этого пожелает.

Из множества вторых игроков выделяется два подмножества, и далее предполагается, что второй игрок может принадлежать одному из двух типов. Первым типом противников являются «простецы» — игроки, которые не знают оптимальной стратегии или просто не способны ее реализовать. Последний вариант имеет место, например, когда противником является человек, который не может использовать различные приспособления для генерации случайных чисел и, кроме того, ограничен во времени. В этом случае программа может, используя различные техники, обнаружить закономерности в игре противника и учесть их в своей стратегии для достижения выигрыша [1; 2]. Формально это означает, что простецы действуют в соответствии с моделью, реализованной в программе. При этом параметры модели (вероятности переходов) заранее неизвестны и вычисляются программой адаптивно. Целью реализации программы является достижение выигрыша у любого противника первого типа. Вместе с тем, очевидно, что такая программа будет отклоняться от равновесной стратегии, поэтому потенциально возможна

ситуация, когда она будет проигрывать в терминах математического ожидания. В частности, программа может оказаться взломана, и противник второго типа («взломщик»), используя специально подобранную стратегию противодействия, сможет добиться существенного выигрыша. На действия взломщика не накладывается никаких ограничений, в частности, он не ограничен вычислительной сложностью решения задачи подбора оптимального способа противодействия. Предположение о существовании взломщиков задает еще одно требование к программе: размер проигрыша взломщику должен быть ограничен некоторой не очень значительной величиной. Здесь мы допускаем потенциальный проигрыш, величина которого не превосходит по порядку логарифма от количества повторений игры.

Мы будем рассматривать алгоритмы, построенные по следующей схеме. На первом этапе алгоритм выполняет распознавание игровой ситуации на основе накопленной статистики ходов противника. Результатом работы алгоритма на этом этапе является принятие решения о том, что в настоящий момент имеет место некоторая игровая ситуация принадлежащая конечному множеству определенных до начала работы игровых ситуаций.

На втором этапе работы анализируются предшествующие ходы противника, сделанные в этой игровой ситуации. Выполняется подсчет количества применений противником каждой игровой стратегии $\tilde{y} = (y_1, y_2, \ldots, y_m)$, где y_i — количество применений игровой стратегии i в рассматриваемой игровой ситуации. Далее некоторым детерминированным образом вычисляется вектор распределения вероятностей $\tilde{p} = F(\tilde{y})$.

На третьем этапе работы алгоритма случайным образом в соответствии с распределением $\tilde{p}$ выбирается ход программы. При этом предполагается, что потенциальный взломщик знает алгоритм работы программы на первом и втором этапах работы, но не может предсказать выбор хода на третьем этапе.

Другими словами, на первом этапе работы алгоритм моделирует логику противника, и реализация этого этапа у разных алгоритмов может различаться настолько, насколько различаются различные модели игровой логики противников. Адекватность модели реальной игровой логике может, в частности, являться целью исследований в области психологии, если в качестве противника выступает человек. Естественным способом представления модели является вероятностный автомат. Вероятности перехода в таком автомате изначально могут быть заданы как вероятности в точке равновесия матричной игры, а далее вычисляться адаптивно.

Однако более важным является второй этап работы алгоритма — этап принятия решения об использовании предсказания хода противника. Например, для игры «Камень, ножницы, бумага» (КНБ) пусть было сделано предсказание, что противник в текущей ситуации выбирает ход «камень» чаще, чем «ножницы». Следует ли из этого, что программа должна сделать ход «бу-

мага» учитывая, что противник мог целенаправленно подвести программу к этому решению предшествующими ходами?

Рассмотрим пример алгоритма первого игрока для игры КНБ. Алгоритм работает в предположении, что его противником является вероятностный контекстный автомат с глубиной контекста r. Это означает, что состояниями автомата являются подстроки символов из множества $\{0, 1, 2\}$ длины r. Считается, что автомат находится в состоянии s если запись предшествующих r ходов противника образует строку s. Пусть для произвольного состояния s противник ранее сделал y_{s1}, y_{s2}, y_{s3} ходов «камнем» «ножницами» и «бумагой» соответственно, и функция $F(y_{s1}, y_{s2}, y_{s3})$ определена следующим образом:

$$F(y_{s1}, y_{s2}, y_{s3}) = \begin{cases} \left(\frac{1}{3}, \frac{1}{3}, \frac{1}{3}\right), & y_{s1} + y_{s2} + y_{s3} = 0 \\ \left(\frac{y_{s2}}{y_{s1}+y_{s2}+y_{s3}}, \frac{y_{s3}}{y_{s1}+y_{s2}+y_{s3}}, \frac{y_{s1}}{y_{s1}+y_{s2}+y_{s3}}\right), & y_{s1} + y_{s2} + y_{s3} > 0 \end{cases} \quad (1)$$

Такой выбор функции F выглядит логичным и означает, что программа будет выбирать ход «камень» с частотой, с которой противник ранее делал ход «ножницы» и т. д.

Можно предположить, что потенциальный взломщик, зная функцию F, будет жадно ей противодействовать, что приведет к сходимости значения функции F к точке равновесия и обеспечит счет близкий к ничейному. Однако, далее будет показано, что жадная стратегия взломщика в данном случае не является оптимальной.

Построим стратегию противодействия указанному алгоритму следующим образом. Выберем некоторое вещественное число ϕ и целое число $t = 3k - 1$. Построим последовательность $\tilde{\alpha} = \alpha_1\alpha_2 \ldots \alpha_{[\phi^t]}$, где $[x]$ — округление числа x до ближайшего целого.

$$\tilde{\alpha} = 0^{[\phi]}1^{[\phi^2]}2^{[\phi^3]}0^{[\phi^4]-[\phi^1]}1^{[\phi^5]-[\phi^4]}2^{[\phi^6]-[\phi^3]}\ldots 0^{[\phi^{t-1}]-[\phi^{t-4}]}1^{[\phi^t]-[\phi^{t-3}]}2^{[\phi^t]-[\phi^{t-2}]}0^{[\phi^t]-[\phi^{t-1}]}$$

Последовательность состоит из $t + 2$ блоков, причем блоки с номерами вида $3k + 1$ состоят из нулей (ход камнем), блоки с номерами вида $3k + 2$ состоят из единиц (ходы ножницами), остальные блоки — из двоек (ходы бумагой). Длина каждого блока подобрана так, чтобы суммарное количество символов каждого вида в конце блока составляло. $[\phi^i]$, $[\phi^{i-1}]$, $[\phi^{i-2}]$. Длины двух последних блоков подобраны так, чтобы суммарное количество символов каждого вида в последовательности составило $[\phi^t]$, а общая длина последовательности соответственно $3[\phi^t]$.

С использованием последовательности $\tilde{\alpha}$ можно построить последовательность ходов следующим образом. Изначально игрок делает r ходов «камнем» (символ 0), чтобы попасть в состояние $0 \ldots 0$, далее при i-м попадании в некоторое состояние s делается ход α_i.

Рассматривая множество состояний и переходы между ними как граф де Брейна[3] можно заметить, что построенная последовательность ходов начинается и заканчивается в одном состоянии и, кроме того, проходит через каждое состояние ровно $3[\phi^t]$ раз.

Найдем математическое ожидание выигрыша второго игрока против алгоритма на основе контекстной модели глубины r с функцией F (1) при использовании полученной последовательности ходов. Общее математическое ожидание выигрыша будет складываться из математических ожиданий для каждого состояния модели. При этом математическое ожидание выигрыша для каждого состояния будет одинаковым, поэтому, будем искать его для некоторого фиксированного состояния, например, $s = 0 \dots 0$.

$$E(0\dots0) = \sum_{1\leqslant i<[\phi]} \frac{-i}{i} + \sum_{0\leqslant i<[\phi^2]} \frac{[\phi]-i}{[\phi]+i} + \\ + \sum_{0\leqslant i<[\phi^3]} \frac{[\phi^2]-i}{[\phi^2]+[\phi^1]+i} + \sum_{j=1}^{t-3} \sum_{[\phi^j]\leqslant i<[\phi^{j+3}]} \frac{[\phi^{j+2}]-i}{[\phi^{j+2}]+[\phi^{j+1}]+i} + \\ + \sum_{[\phi^{t-2}]\leqslant i<[\phi^t]} \frac{[\phi^t]-i}{[\phi^t]+[\phi^{t-1}]+i} + \sum_{[\phi^{t-1}]\leqslant i<[\phi^t]} \frac{[\phi^t]-i}{2[\phi^t]+i}.$$

Данную сумму можно оценить, избавившись от округлений и заменив суммы интегралами.

$$E(0\dots0) \approx \int_1^{\phi} \frac{-i}{i} di + \int_0^{\phi^2} \frac{\phi-i}{\phi+i} di + \int_0^{\phi^3} \frac{\phi^2-i}{\phi^2+\phi^1+i} di + \\ + \sum_{j=1}^{t-3} \int_{\phi^j}^{\phi^{j+3}} \frac{\phi^{j+2}-i}{\phi^{j+2}+\phi^{j+1}+i} di + \int_{\phi^{t-2}}^{\phi^t} \frac{\phi^t-i}{\phi^t+\phi^{t-1}+i} di + \int_{\phi^{t-1}}^{\phi^t} \frac{\phi^t-i}{2\phi^t+i} di = \\ = 1 - \phi - \phi^2 + 2\phi\ln(\phi+1) + -\phi^3 + (2\phi^2+\phi)(ln(\phi^2+\phi+1) - ln(\phi+1)) + \\ + \sum_{j=1}^{t-3} (-\phi^{j+3} + \phi^j + (2\phi^{j+2}+\phi^{j+1})\ln\phi) + \\ - \phi^t + \phi^{t-2} + (2\phi^t+\phi^{t-1})(\ln(2\phi^2+\phi) - \ln(\phi^2+\phi+1)) + \\ - \phi^t + \phi^{t-1} + 3\phi^t(\ln 3\phi - \ln(2\phi+1)).$$

Предел отношения математического ожидания выигрыша к количеству ходов будет равен

$$\lim_{t\to\infty} \frac{E(0\dots0)}{3\phi^t} = -1 + \frac{\ln\phi}{\phi(\phi-1)} + \frac{2\ln\phi}{3\phi} + \frac{2\phi+1}{3\phi}\ln\left(\frac{2\phi^2+\phi}{\phi^2+\phi+1}\right) + \ln\left(\frac{3\phi}{2\phi+1}\right).$$

Это значение достигает максимума при $\phi \approx 2.17818769$, а значение предела при данном ϕ приблизительно равно 0.0577026. Это означает, что выигрыш

потенциального взломщика у приведенного алгоритма линейно зависит от количества повторений игры и составляет примерно 0.057 на одну партию.

Этот пример показывает нетривиальность задачи определения вероятности хода первого игрока для случая, когда он пришел к выводу о неслучайности ходов противника и получил обоснованные предположения о его следующем ходе. Далее будет приведен способ построения функции F, гарантирующий, что потенциальный проигрыш взломщику по порядку не будет превосходить логарифма от числа повторов игры.

Пусть программой было распознано состояние s, которое ранее встречалось в игре n раз, причем была собрана статистика ходов второго игрока $\tilde{y} = (y_1, y_2, y_k)$, где y_i количество применений стратегии i в состоянии s, $n = \sum_{i=1}^{k} y_i$. Будем вычислять вектор вероятностей $\tilde{p} = (p_1, p_2, p_m)$ как набор некоторых линейных функций от $\tilde{z}$.

$$p_j = \frac{f_{j1}y_1 + f_{j2}y_2 + ...f_{jk}y_k}{n}$$

или в матричном виде

$$\tilde{p} = n^{-1}F\tilde{y}.$$

Следующая теорема указывает способ проверки правильности выбора функции вычисления распределения вероятностей.

Теорема 1. *Пусть игра задана матрицей A и функция вычисления распределения вероятностей задана матрицей F такой, что матрица A^TF является симметричной, и квадратичная форма, заданная матрицей A^TF, положительно полуопределена. Тогда, существует константа c такая, что для любой последовательности длины n ходов второго игрока математическое ожидание выигрыша второго игрока удовлетворяет неравенству*

$$E \leqslant c \ln n.$$

Из данной теоремы следует, что правильным выбором функции нахождения распределения вероятностей для рассматриваемого алгоритма будет

$$F(y_{s1}, y_{s2}, y_{s3}) = \\ = \begin{cases} \left(\frac{1}{3}, \frac{1}{3}, \frac{1}{3}\right), & y_{s1} + y_{s2} + y_{s3} = 0 \\ \left(\frac{y_{s1}+2y_{s2}}{3(y_{s1}+y_{s2}+y_{s3})}, \frac{y_{s2}+2y_{s3}}{3(y_{s1}+y_{s2}+y_{s3})}, \frac{y_{s3}+2y_{s1}}{3(y_{s1}+y_{s2}+y_{s3})}\right), & y_{s1} + y_{s2} + y_{s3} > 0 \end{cases}.$$

С учетом этого рассматриваемый алгоритм сможет выиграть у противника, играющего в соответствии с контекстной вероятностной моделью, величину, пропорциональную количеству повторений игры. При этом величина проигрыша в случае взлома программы не превосходит логарифма от числа повторений.

Список литературы

[1] Блудов В. В. Анализ псевдослучайных последовательностей и компьютерные игры. // Прикладная логика – 95 : материалы 4-й Международной конференции по прикладной логике (15-17 июня 1995 г.). Иркутск, 1995. С. 8–9.

[2] McLoone J. How to Win at Rock-Paper-Scissors. WOLFRAM BLOG. URL: https://blog.wolfram.com/2014/01/20/how-to-win-at-rock-paper-scissors/

[3] de Bruijn N. G. A Combinatorial Problem. // Koninklijke Nederlandse Akademie V. Wetenschappen. 1946. Vol. 49. P. 758–764.

Analysis of adaptive algorithms for repeated matrix games

Kirichenko Konstantin Dmitrievich

Irkutsk State University, e-mail: constkir@gmail.com

In this paper we consider repeated matrix games. We assume that the first player is a computer program, and the second one can belong to one of two types: "hacker"is a player who knows the algorithm implemented in the program and optimally counteracts it; "simpleton"is a player who does not know the optimal strategy or is not able to implement it. In this case, the first player does not know the number of repetitions of the game, and his opponent as well. The problem is posed by limiting the possible value of loss to the hacker, to achieve significant gains from the simpleton. It is shown that determining the reaction of the program to opponent‘s actions is a non-trivial problem. An example of an intuitively good algorithm is given, the optimal strategy for counteracting which nonetheless leads to a significant value of loss.

Keywords: matrix games, repeated games, adaptive strategies.

УДК 519.714

Немонотонная сложность логических схем и близкие задачи

Кочергин Вадим Васильевич[1], **Михайлович Анна Витальевна**[2]

[1] Московский государственный университет им. М. В. Ломоносова, Национальный исследовательский университет «Высшая школа экономики», e-mail: vvkoch@yandex.ru

[2] Национальный исследовательский университет «Высшая школа экономики», e-mail: avmikhailovich@gmail.com

Исследуется сложность логических схем, реализующих булевы функций и функции многозначной логики, в бесконечных базисах, состоящих из всех монотонных и конечного числа немонотонных функций. В качестве мер сложности рассматривается как классическая мера, характеризующая общее число элементов в схеме, так и немонотонная сложность, отражающая только число использований немонотонных элементов. В работе дан обзор результатов авторов, обобщающих теорему Маркова об инверсионной сложности булевых функций, а также представлены новые результаты в задачах, связанных с немонотонной сложностью, и в близких задачах.

Ключевые слова: булевы функции, функции многозначной логики, логические схемы, схемная сложность, немонотонная сложность, инверсионная сложность, теорема Маркова.

Рассматривается задача о сложности реализации булевых функций и функций многозначной логики схемами из функциональных элементов (логическими схемами) в бесконечных базисах, состоящих из всех монотонных и конечного числа немонотонных функций, причем в качестве меры сложности схем помимо классической меры, характеризующей общее число элементов в схеме, исследуется также немонотонная сложность, отражающая только число использований немонотонных элементов (монотонные функции «бесплатны»). Для случая реализации систем булевых функций в базисе, содержащем помимо монотонных функций только отрицание, А. А. Марковым установлено точное значение немонотонной сложности (называемой в этом случае инверсионной сложностью). В настоящей работе дан обзор результатов авторов, обобщающих теорему Маркова, а также представлены новые результаты в задачах, связанных с немонотонной сложностью, и в близких задачах.

Дадим несколько определений.

Пусть P_k — множество всех функций k-значной логики ($k \geqslant 2$), M — класс всех функций из P_k, монотонных относительно порядка $0 < 1 < \ldots < k-1$.

Обозначим множество $\{0, 1, \ldots, k-1\}$ через E_k. Последовательность

$$\tilde{\alpha}_1 = (\alpha_{11}, \ldots, \alpha_{1n}),\ \tilde{\alpha}_2 = (\alpha_{21}, \ldots, \alpha_{2n}),\ \ldots,\ \tilde{\alpha}_r = (\alpha_{r1}, \ldots, \alpha_{rn})$$

наборов из множества E_k^n назовем *возрастающей цепью относительно порядка* $0 < 1 < \ldots < k-1$ или просто *цепью*, если все наборы $\tilde{\alpha}_1, \tilde{\alpha}_2, \ldots, \tilde{\alpha}_r$ различны и выполняются неравенства

$$\alpha_{ij} \leqslant \alpha_{i+1,j}, \quad i = 1, \ldots, r-1, \quad j = 1, \ldots, n.$$

Пусть $f(x_1, \ldots, x_n)$ — функция k-значной логики. Упорядоченную пару наборов $\tilde{\alpha} = (\alpha_1, \ldots, \alpha_n)$ и $\tilde{\beta} = (\beta_1, \ldots, \beta_n)$, $\tilde{\alpha}, \tilde{\beta} \in E_k^n$, будем называть *обрывом для функции* f, если выполнены условия:

1) $\alpha_j \leqslant \beta_j$, $j = 1, \ldots, n$;

2) $f(\tilde{\alpha}) > f(\tilde{\beta})$.

Обрывом для системы функций будем называть любую пару наборов, являющуюся обрывом хотя бы для одной функции системы.

Пусть $F = \{f_1, \ldots, f_m\}$, $m \geqslant 1$, — система функций k-значной логики от переменных $x_1, \ldots x_n$, а C — цепь, имеющая вид $\tilde{\alpha}_1, \tilde{\alpha}_2, \ldots, \tilde{\alpha}_r$. Под *падением* $d_C(F)$ *системы* F *на цепи* C будем понимать число обрывов для системы F на парах вида $(\tilde{\alpha}_i, \tilde{\alpha}_{i+1})$.

Спад $d(F)$ системы F определим равенством $d(F) = \max d_C(F)$, где максимум берется по всем цепям C.

Для произвольной системы функций $F \subset P_k$, $k \geqslant 2$, и полного в P_k базиса B обозначим через $L_B(F)$ и $I_B(F)$ обычную сложность и немонотонную сложность системы F в базисе B, т. е. минимальное число всех элементов и, соответственно, немонотонных элементов в схемах, реализующих систему F в базисе B.

А. А. Марковым в 1957–1963 гг. установлено [1; 2] точное значение инверсионной сложности (т. е. немонотонной сложности в булевом базисе $B_0 = \mathrm{A} \cup \{\overline{x}\}$, где $[A] = M$) для произвольной конечной системы F булевых функций:

$$I_{B_0}(F) = \lceil \log_2(d(F) + 1) \rceil .$$

В 1961 г. Э. И. Нечипоруком найдено [3] точное значение инверсионной сложности для любой булевой функции в классе схем без ветвления выходов элементов (формул).

В 2015 г. установлена асимптотика роста немонотонной сложности произвольной последовательности F_n систем булевых функций при $d(F_n) \to \infty$.

Теорема 1 ([4]). *Для любого полного базиса* B *найдется такая константа* $c(B)$, *что для любой системы* F *функций из* P_2 *выполняются неравенства*

$$\lceil \log_2(d(F) + 1) \rceil - c(B) \leqslant I_B(F) \leqslant \lceil \log_2(d(F) + 1) \rceil .$$

Эта теорема дает верхнюю и нижнюю оценки немонотонной сложности систем булевых функций, отличающиеся не более чем на константу. Однако этот результат далек от окончательного, так как эта константа зависит от базиса, причем для любой константы можно подобрать базис рассматриваемого вида и булеву функцию так, что разность верхней оценки из теоремы 1 и реальной немонотонной сложности этой функции превосходит эту константу.

В случае реализации одной булевой функции установлено точное значение немонотонной сложности.

Теорема 2 ([5]). *Пусть B — полный в P_2 базис, $\omega_1, \ldots, \omega_p$ — все монотонные функции базиса B, $D(B) = \max\{d(\omega_1), \ldots, d(\omega_p)\}$. Тогда для любой булевой функции f выполняется равенство*

$$I_B(f) = \left\lceil \log_2 \left(\frac{d(f)}{D(B)} + 1 \right) \right\rceil .$$

Для того чтобы сформулировать полученные результаты о немонотонной сложности в общем случае (при реализации функций k-значной логики, $k \geqslant 2$), требуется ввести еще некоторые понятия.

Для произвольной функции k-значной логики $f(x_1, x_2, \ldots, x_n)$ и произвольной цепи $C = (\tilde{\alpha}_1, \tilde{\alpha}_2, \ldots, \tilde{\alpha}_r)$ наборов из E_k^n определим величину $u_C(f)$ как наибольшую длину t подпоследовательности $\tilde{\beta}_1, \tilde{\beta}_2, \ldots, \tilde{\beta}_t$ последовательности C, удовлетворяющей условию $f(\tilde{\beta}_1) > f(\tilde{\beta}_2) > \ldots > f(\tilde{\beta}_t)$.

Теперь определим *инверсионную силу $u(f)$ функции f* равенством $u(f) = \max u_C(f)$, где максимум берется по всем цепям C наборов из E_k^n. Очевидно, что для любой функции f выполняются соотношения $1 \leqslant u(f) \leqslant d(f) + 1$, при этом если функция f не является монотонной, то справедливо неравенство $u(f) \geqslant 2$.

Наконец, для базиса B функций k-значной логики равенством $u(B) = \max u(f)$, где максимум берется по всем функциям f из базиса B, введем величину $u(B)$ — *инверсионную силу базиса B*.

Асимптотика роста немонотонной сложности произвольной последовательности F_n систем функций k-значной логики при условии $d(F_n) \to \infty$ установлена в 2017 г.

Теорема 3 ([6]). *Для любого полного базиса B найдется такая константа $c(B)$, что для любой системы F функций из P_k выполняются неравенства*

$$\left\lceil \log_{u(B)}(d(F) + 1) \right\rceil - c(B) \leqslant I_B(F) \leqslant \left\lceil \log_{u(B)}(d(F) + 1) \right\rceil .$$

Отметим, что как и в теореме 1 в теореме 3 заменить константу $c(B)$, зависящую от базиса, на абсолютную константу нельзя: для любого $k \geqslant 2$ и для любого заданного значения N найдется базис B_N в P_k и функция $g_N \in P_k$, для которых справедливо неравенство $\left\lceil \log_{u(B_N)}(d(g_N) + 1) \right\rceil - I_{B_N}(g_N) > N$.

Далее будем рассматривать два естественных базиса функций k-значной логики, а именно, базисы $B_P = M \cup \{N_P(x)\}$ и $B_L = M \cup \{N_L(x)\}$, где $N_P(x)$ — отрицание Поста, т. е. функция $x + 1 \pmod k$, а $N_L(x)$ — отрицание Лукасевича, т. е. функции $k - 1 - x$.

Относительно немонотонной сложности в этих базисах в 2016 г. получен в некотором смысле окончательный результат.

Теорема 4 ([7]). *Для любой конечной системы F функций k-значной логики справедливы равенства*

$$I_{B_P}(F) = \left\lceil \log_2(d(F) + 1) \right\rceil , \qquad I_{B_L}(F) = \left\lceil \log_k(d(F) + 1) \right\rceil .$$

Отметим, что теорема 4 дает возможность выписать точные значений соответствующих функций Шеннона немонотонной сложности функций и вектор-функций в базисах B_P и B_L (это проделано в [7]).

Теперь рассмотрим тесно связанную с задачей о немонотоннной сложности задачу о сложности реализации функций k-значной логики в базисах B_P и B_L. Принципиальной отличительной особенностью задач изучения величин $L_{B_P}(f)$, $L_{B_L}(f)$, $L_{B_P}(n)$ и $L_{B_L}(n)$ является бесконечность базисов B_P и B_L.

Справедливость естественной гипотезы о том, что величина $L_{B_L}(f)$ растет примерно как $2\lceil\log_k(d(f)+1)\rceil$, доказана в 2018 г.

Теорема 5 ([8]). *Для любой функции k-значной логики f справедливы неравенства*

$$2\lceil\log_k(d(f)+1)\rceil - 1 \leqslant L_{B_L}(f) \leqslant 2\lceil\log_k(d(f)+1)\rceil + 1.$$

Положим

$$T(k,n) = (k-1)n - \left\lfloor\frac{(k-1)n}{k}\right\rfloor + 1 = (k-2)n + \left\lceil\frac{n}{k}\right\rceil + 1.$$

Легко проверить, что величина $T(k,n)$ ровно на единицу превосходит максимально возможный спад у функций k-значной логики от n переменных.

Обозначим через R_k множество натуральных чисел n, удовлетворяющих условию: число $T(k,n)-1$ является степенью числа k.

Теорема 6 ([8]). *При $n \geqslant k+2$ для функции Шеннона сложности реализации функций k-значной логики ($k \geqslant 2$) в базисе B_L верно равенство*

$$L_{B_L}(n) = \begin{cases} 2\lceil\log_k T(k,n)\rceil, & \text{если } n \in R_k; \\ 2\lceil\log_k T(k,n)\rceil + 1, & \text{если } n \in \mathbb{N}\setminus R_k. \end{cases}$$

Переходя к базису B_P, для произвольного натурального n положим

$$\tau(n) = \begin{cases} 1, & \text{если } 3^r < n \leqslant 4\times 3^{r-1} \text{ для некоторого целого } r; \\ 2, & \text{если } 4\times 3^{r-1} < n \leqslant 2\times 3^r \text{ для некоторого целого } r; \\ 3, & \text{если } 2\times 3^r < n \leqslant 3\times 3^r \text{ для некоторого целого } r. \end{cases}$$

В 2017 г. для базиса B_P с точностью до единицы установлено значение сложности реализации произвольной функции k-значной логики ($k \geqslant 3$), а также найдено точное значение соответствующей функции Шеннона.

Теорема 7 ([9]). *При $k \geqslant 3$ для любой функции k-значной логики f, удовлетворяющей условию $d(f) \geqslant 2$, справедливы неравенства*

$$L_{B_P}(f) \geqslant 3\left(\lceil\log_3(d(f)+1)\rceil - 1\right) + \tau(d(f)+1),$$
$$L_{B_P}(f) \leqslant 3\left(\lceil\log_3(d(f)+1)\rceil - 1\right) + \tau(d(f)+1) + 1.$$

Теорема 8 ([9]). *При $k \geqslant 3$ для любого натурального $n \geqslant 4$ для функции Шеннона сложности реализации функций k-значной логики в базисе B_P справедливо равенство*

$$L_{B_P}(n) = 3\left(\lceil \log_3 T(k,n) \rceil - 1\right) + \tau(T(k,n)) + 1.$$

При реализации в базисах B_P и B_L систем функций k-значной логики справедливы похожие оценки.

Теорема 9. *Для любой системы функций $F = \{f_1, f_2, \ldots, f_m\} \subset P_k$, $k \geqslant 2$, выполняются неравенства*

$$2\lceil \log_k(d(F)+1) \rceil - 1 \leqslant L_{B_P}(F) \leqslant 2\lceil \log_k(d(F)+1) \rceil + m.$$

Теорема 10. *Для любой системы функций $F = \{f_1, f_2, \ldots, f_m\} \subset P_k$, $k \geqslant 3$, выполняются неравенства*

$$3\left(\lceil \log_3(d(F)+1) \rceil - 1\right) + \tau(d(F)+1) - 1 \leqslant L_{B_P}(F) \leqslant$$
$$\leqslant 3\left(\lceil \log_3(d(F)+1) \rceil - 1\right) + \tau(d(F)+1) + m.$$

Работа первого автора выполнена при частичной финансовой поддержке РФФИ, проект № 18-01-00337.

Список литературы

[1] Марков А. А. Об инверсионной сложности систем функций // ДАН СССР. 1957. Т. 116, № 6. С. 917–919.

[2] Марков А. А. Об инверсионной сложности систем булевых функций // ДАН СССР. 1963. Т. 150, № 3. С. 477–479.

[3] Нечипорук Э. И. О сложности схем в некоторых базисах, содержащих нетривиальные элементы с нулевыми весами // Проблемы кибернетики. Вып. 8. М. : Физматгиз, 1962. С. 123–160.

[4] Кочергин В. В., Михайлович А. В. О сложности схем в базисах, содержащих монотонные элементы с нулевыми весами // Прикладная дискретная математика. 2015. № 4 (30). С. 24–31.

[5] Кочергин В. В., Михайлович А. В. Точное значение немонотонной сложности булевых функций // Математические заметки. 2019. Т. 105. Вып. 1. С. 32–41.

[6] Kochergin V. V., Mikhailovich A. V. Asymptotics of growth for non-monotone complexity of multi-valued logic function systems // Siberian Electronic Mathematical Reports. 2017. Vol. 14. P. 1100–1107.

[7] Кочергин В. В., Михайлович А. В. О минимальном числе отрицаний при реализации систем функций многозначной логики // Дискретная математика. 2016. Т. 28, вып. 4. С. 80–90.

[8] Кочергин В. В., Михайлович А. В. О схемной сложности функций k-значной логики в одном бесконечном базисе // Прикладная математика и информатика. 2018. № 58. С. 21–34.

[9] Кочергин В. В., Михайлович А. В. О сложности функций многозначной логики в одном бесконечном базисе // Дискретный анализ и исследование операций. 2018. Т. 25, № 1. С. 42–74.

Nonmonotone complexity of logic circuits and similar problems

Kochergin Vadim Vasil'evich [1], **Mikhaylovich Anna Vital'evna** [2]

[1] Lomonosov Moscow State University; National Research University — Higher School of Economics , e-mail: vvkoch@yandex.ru

[2] National Research University — Higher School of Economics , e-mail: avmikhailovich@gmail.com

We study the complexity of the realization of Boolean functions and multi-valued logic functions by circuits in infinite complete bases containing all monotone functions and finitely many nonmonotone functions. We consider both classical measure of complexity which corresponds to the total number of elements in the circuit and nonmonotone complexity that indicates the number of non-monotone elements of the circuit. The paper reviews our results that extend Markov's theorem of inversion complexity of Boolean function as well as contains new results concerning non-monotone complexity and similar problems.

Keywords: Boolean functions, multi-valued logic functions, logic circuits, circuit complexity, nonmonotone complexity, inversion complexity, Markov's theorem.

УДК 519.716

Классификация k-значных функций на основе аддитивных формул

Мещанинов Дмитрий Германович

НИУ «Московский энергетический институт», e-mail: MeshchaninovDG@mpei.ru

Рассматриваются функциональная система P_k функций k-значной логики и решетка $\mathcal{L}_k$ по включению замкнутых относительно суперпозиции классов в P_k. Классы описываются каноническими аддитивными формулами (в виде сумм по модулю k) своих элементов. Одно слагаемое в сумме является линейной функцией, остальные слагаемые зависят от делителя d числа k и определяют классы различных семейств. Для всех k и d находятся полные системы и базисы таких классов, определяется их положение в решетке $\mathcal{L}_k$.

Ключевые слова: функциональная система, суперпозиция, решетка замкнутых классов, полиномы по модулю k, полные системы.

Пусть $k \geqslant 2$, $E_k = \{0, 1, \ldots, k-1\}$, и пусть

$$P_k = \{f : \ E_k^n \to E_k, \ n = 0, 1, 2 \ldots\}$$

— класс всех функций k-значной логики. Мы рассматриваем замкнутые относительно суперпозиции классы в P_k, содержащие все линейные по модулю k функции, и решетку таких классов как важную часть континуальной при $k \geqslant 3$ решетки $\mathcal{L}_k$. Анализируемые классы описываются каноническими представлениями своих элементов в виде аддитивных формул (сумм) [1; 2], слагаемые которых определены однозначно. В каждой такой сумме одно слагаемое является линейной функцией. Мы укажем семейства таких классов, их полные системы, канонические формулы и место классов в решетке $\mathcal{L}_k$.

Введем следующие **определения и обозначения**.

Пусть $d|k$. Функция $f(\tilde{x}) = f(x_1, \ldots, x_n)$ из P_k, удовлетворяющая условию

$$\tilde{a} \equiv \tilde{b} \pmod{d} \ \Rightarrow \ f(\tilde{a}) = f(\tilde{b}) \pmod{d},$$

называется *d-периодической*.

Будем применять обозначения:
$G_d(\tilde{x})$ — для d-периодической функции;
$d \cdot F(\tilde{x})$ — для функции, все значения которой кратны d;
$l(\tilde{x})$ — для линейной функции;
$A(M)$ — для системы функций, полной в замкнутом классе M;
$p, p_1, \ldots, p_s, q$ — для простых чисел.

Введем функции:

$$g_d(\tilde{x}) = \begin{cases} 1, & \text{если } \tilde{x} \equiv \tilde{0} \pmod{d}, \\ 0, & \text{иначе,} \end{cases} \qquad j(\tilde{x}) = \begin{cases} 1, & \text{если } \tilde{x} = \tilde{0}, \\ 0, & \text{иначе,} \end{cases}$$

$$\chi_{d,\,i}(\tilde{x}) = x_i g_d(\tilde{x}), \ i = 1, \ldots, n; \qquad \delta_d(x) = d\lfloor x/d \rfloor.$$

Рассмотрим следующие **семейства классов** (всюду $d|k$).

1. Классы *сохранения сравнения по модулю d*

$$C(d) = \{f(\tilde{x}) = l(\tilde{x}) + G_d(\tilde{x}) + d \cdot F(\tilde{x})\}$$

порождаются системами

$$\{1, x + y,\ g_d(x, y),\ d \cdot j(x, y)\}.$$

Если $d \neq 1$ и $d \neq k$, то класс $C(d)$ является предполным в P_k [3].

2. Классы

$$C_1(d) = \{f(\tilde{x}) = l(\tilde{x}) + d \cdot F(\tilde{x})\}$$

порождаются системами

$$\{1, x + y,\ d \cdot j(x, y)\}.$$

Класс $C_1(d)$ является предполным в классе $C(d)$ в точности при $k = pd$ [4].

3. Классы *сохранения d-разностей*

$$R(d) = \{f(\tilde{x}) = l(\tilde{x}) + G_d(\tilde{x}) + d \cdot F(\tilde{x})\},$$

где

$$d \cdot F(\tilde{x}) = \sum_{\tilde{a} \in E_d^n} \sum_{i=1}^{n} c_1(\tilde{a},\ i)\chi_{d,\,i}(\tilde{x} - \tilde{a}) + \sum_{i=1}^{n} c_2(i)\delta_d(x_i), \qquad (1)$$

$c_1(\tilde{a}, i), c_2(i) \in E_k$, порождаются системами

$$\{1, x + y,\ \chi_{d,\,1}(x),\ dj(x, y)\}.$$

Класс $R(d)$ является предполным в классе $C(d)$ в точности при $k = pd$ [5].

4. Классы *абсолютного сохранения d-разностей*

$$L(d) = \{f(\tilde{x}) = l(\tilde{x}) + G_d(\tilde{x}) + \sum_{i=1}^{n} \delta_d(x_i)\}$$

порождаются системами

$$\{1, x + y,\ g_d(x, y)\}.$$

Класс $L(d)$ является предполным в классе $R(d)$ в точности при $k = pd$ [6].

5. Классы

$$S(d) = \{f(\tilde{x}) = l(\tilde{x}) + d \cdot G_d(\tilde{x}) + d \cdot F(\tilde{x})\},$$

где $d \cdot F(\tilde{x})$ имеет вид (1), порождаются системами

$$\{1, x + y,\ \chi_{d,\,1}(x)\} \cup \bigcup_{n=1}^{\infty} \{d \cdot g_d(x_1, \ldots, x_n)\}.$$

При $k = p^2$ и $k = pq$ класс $S(p)$ конечно-порожден и является предполным в $R(p)$ [4].

6. Классы

$$K(d) = \{f(\tilde{x}) = l(\tilde{x}) + d \cdot G_d(\tilde{x})\}$$

порождаются системами

$$\{1, x + y\} \cup \bigcup_{n=1}^{\infty} \{d \cdot g_d(x_1, \ldots, x_n)\}.$$

В [7] доказана

Теорема 1. *Пусть $k = pq$, тогда*:

1) *класс $K(p)$ конечно-порожден, его базисом является система*

$$\{1, x + y, p \cdot g_p(x)\};$$

2) *класс $K(p)$ является предполным в классе $L(p)$*;

3) *класс L является предполным в $K(p)$ и $K(q)$*;

4) *в решетке $\mathcal{L}_k$ имеются следующие неуплотняемые цепи замкнутых классов*:

$$L \subset K(d) \subset L(d) \subset R(d) \subset C(d) \subset P_k, \quad d = p, q;$$

5) *классы $K(p)$ содержат функции, не представимые полиномами по модулю pq.*

Для сравнения приведем результат из [8], имеющий место при $k = p^2$.

Теорема 2. *При $k = p^2$ класс всех полиномов по модулю p^2 есть $R(p)$. Решетка всех классов полиномов, содержащих L, бесконечна. Класс $K(p)$ бесконечно-порожден, не имеет базиса и является пределом возрастающей цепи своих подклассов.*

Для классов полиномов, содержащих L, в [6] доказана

Теорема 3. *При $k = p_1 \cdots p_s$ все классы полиномов, содержащие L, образуют решетку, изоморфную s-мерному кубу.*

В [9–11] содержатся результаты о подобной классификации частичных функций в функциональной системе P_k^*.

С точки зрения логики функциональные системы P_k и P_k^* интересны, в частности, тем, что они используются как интерпретации формальных теорий.

Список литературы

[1] Мещанинов Д. Г. Семейства замкнутых классов в P_k, определяемые аддитивными и полиномиальными представлениями функций // Материалы XII Международного семинара «Дискретная математика и ее приложения» имени академика О. Б. Лупанова (Москва, 20–25 июня 2016 г.). М. : Изд-во механико-математического факультета МГУ, 2016. С. 96–106.

[2] Мещанинов Д. Г. Функции, обобщающие полиномы по модулю k // Труды X Международной конференции «Дискретные модели в теории управляющих систем» (Москва и Подмосковье, 23–25 мая 2018 г.). М. : МАКС-Пресс, 2018. С. 198–200.

[3] Яблонский С. В. Функциональные построения в k-значной логике // Труды МИАН СССР. 1958. Т. 51. С. 5–142.

[4] Мещанинов Д. Г. Некоторые замкнутые классы в P_k и их гомоморфизмы в P_d при $d|k$ // Труды XVIII Международной конференции «Проблемы теоретической кибернетики» (Пенза, 19–23 июня 2017 г.). М. : МАКС-Пресс, 2017. С. 161–163.

[5] Мещанинов Д. Г. О первых d-разностях функций k-значной логики // Математические вопросы кибернетики. М. : Наука, 1998. Вып. 7. С. 265–280.

[6] Мещанинов Д. Г. О замкнутых классах k-значных функций, сохраняющих первые d-разности // Математические вопросы кибернетики. М. : Наука, 1999. Вып. 8. С. 219–230.

[7] Мещанинов Д. Г. Об одном семействе замкнутых классов в k-значной логике // Вестник Московского университета. Сер. 15. Вычислительная математика и кибернетика. 2019. № 1. С. 26–32.

[8] Мещанинов Д. Г. Замкнутые классы полиномов по модулю p^2 // Дискретная математика. 2017. Т. 29, вып. 3. С. 54–69.

[9] Мещанинов Д. Г. Классификация аддитивных представлений частичных и всюду определенных функций k-значной логики // Труды VIII Международной конференции «Дискретные модели в теории управляющих систем» (Подмосковье, 6–9 апреля 2009 г.). М. : МАКС-Пресс, 2009. С. 214–218.

[10] Мещанинов Д. Г. Замкнутые классы в P_k^*, определяемые значениями функций на параллелограммах // Материалы XI Международного се-

минара «Дискретная математика и ее приложения», посвященного 80-летию со дня рождения академика О. Б. Лупанова (Москва, 18–23 июня 2012 г.). М. : Изд-во механико-математического факультета МГУ, 2012, С. 202–204.

[11] Мещанинов Д. Г. Периодические функции и замкнутые классы в P_k^* // Материалы 4-й Российской школы-семинара «Синтаксис и семантика логических систем» (Улан-Удэ, 14–19 августа 2012 г.). Иркутск : Изд-во ФГБОУ ВПО «Восточно-Сибирская государственная академия образования», 2012. С. 74–77.

Logical k-valued functions classification based on additive formulae

Meshchaninov Dmitrii Germanovich

Moscow Power Engineering Institute, e-mail: MeshchaninovDG@mpei.ru

Function algebra P_k of k-valued logic functions and the inclusion lattice $\mathcal{L}_k$ of closed under superposition classes in P_k are analysed. The classes are described with the use of canonical additive formulae (modulo k sums) of their elements. One summand of each sum is a linear function, the other terms depend on a divisor d of k, they determine various families of such classes. For all k and d, generating sets and bases of the classes are found, location of each class in $\mathcal{L}_k$ is determined.

Keywords: function algebra, lattice of closed classes, modulo k polynomials, generating sets.

УДК 519.716

Критерий ES_U-полноты множества мультифункций ранга 2

Пантелеев Владимир Иннокентьевич, Рябец Леонид Владимирович

Иркутский государственный университет, e-mail: vl.panteleyev@gmail.com, l.riabets@gmail.com

В работе рассматривается действие оператора разветвления по предикату равенства на множестве мультифункций ранга 2. Определяются 11 предполных множеств мультифункций и формулируется критерий полноты.

Ключевые слова: замыкание, предикат равенства, мультифункция, замкнутое множество, суперпозиция, критерий полноты.

Мультифункции представляют собой функции, задаваемые на конечном множестве и возвращающие в качестве своих значений все подмножества рассматриваемого множества. Оператор суперпозиции приводит к континууму замкнутых множеств. Поэтому возникает необходимость рассмотрения операторов замыкания, которые наряду с суперпозицией содержат другие операции. К таким относится рассматриваемый оператор разветвления по предикату равенства (оператор E-замыкания) [2–5].

В работе рассматривается ES_U-замыкание мультифункций, полученное применением операции суперпозиции, основанной на объединении, и оператора разветвления по предикату равенства.

Пусть $E_2 = \{0, 1\}$. Множество всех мультифункций ранга 2 обозначается как M_2 и определяется следующим образом:

$$M_{2,n} = \left\{ f \mid f : E_2^n \to 2^{E_2} \right\}, \; M_2 = \bigcup_n M_{2,n},$$

В дальнейшем не будем различать множество из одного элемента и элемент этого множества. Для множества E_2 будем использовать обозначение «$-$» (прочерк), для пустого множества — «$*$».

Пусть $f(x_1, \ldots, x_n)$, $f_1(x_1, \ldots, x_m), \ldots, f_n(x_1, \ldots, x_m)$ — мультифункции. Суперпозиция $f(f_1(x_1, \ldots, x_m), \ldots, f_n(x_1, \ldots, x_m))$ задает $g(x_1, \ldots, x_m)$ следующим образом: если набор $(\alpha_1, \ldots, \alpha_m) \in E_2^m$, то по определению

$$g(\alpha_1, \ldots, \alpha_m) = \bigcup_{\beta_i \in f_i(\alpha_1, \ldots, \alpha_m)} f(\beta_1, \ldots, \beta_n). \tag{1}$$

Будем говорить, что мультифункция $g(x_1, \ldots, x_n)$ получается из функций $f_1(x_1, \ldots, x_n)$, $f_2(x_1, \ldots, x_n)$ с помощью операции разветвления по предикату равенства, если для некоторых $i, j \in \{1, \ldots, n\}$ выполняется соотношение

$$g(x_1, \ldots, x_n) = \begin{cases} f_1(x_1, \ldots, x_n), & \text{если } x_i = x_j, \\ f_2(x_1, \ldots, x_n), & \text{в противном случае.} \end{cases} \tag{2}$$

Определим ES_U-замыкание множества $Q \subseteq M_2$ как множество всех мультифункций из M_2, которые можно получить из множества Q с помощью операций введения фиктивных переменных, отождествления переменных, суперпозиции (1) и разветвления по предикату равенства (2). ES_U-замыкание множества Q обозначаем как $[Q]$.

Введем в рассмотрение 11 множеств мультифункций:
$K_1 = \{f \mid f(0,\dots,0) \in \{0,-\}\}$; $K_2 = \{f \mid f(1,\dots,1) \in \{1,-\}\}$;
$K_3 = \{f \mid f(0,\dots,0) \in \{0,*\}\}$; $K_4 = \{f \mid f(1,\dots,1) \in \{1,*\}\}$;
$K_5 = O_2^*$; $K_6 = H_2$; $K_7 = \{f \mid f(\tilde{\alpha}) \in \{*,1,-\}\}$;
$K_8 = \{f \mid f(\tilde{\alpha}) \in \{*,0,-\}\}$; $K_9 = PolR_9$; $R_9 = \begin{pmatrix} 0 & 1 & * & - \\ 1 & 0 & * & - \end{pmatrix}$;
$K_{10} = PolR_{10}$; $R_{10} = \begin{pmatrix} 0 & 1 & * & * & * & * & 0 & 1 & - \\ 1 & 0 & 0 & 1 & - & * & * & * & * \end{pmatrix}$;
$K_{11} = \{f \mid * \in f(0,\dots,0) \cup f(1,\dots,1)$ либо $f(0,\dots,0) = 0$ и $f(1,\dots,1) = 1\}$.

Где через $Pol\ R$ обозначается множество функций, сохраняющих предикат R. Понятие сохранения предиката функцией является стандартным [1].

Для рассматриваемых множеств справедлива лемма.

Лемма 1. *Множества $K_1 - K_{11}$ являются ES_U-замкнутыми.*

Будем в дальнейшем использовать обозначение f_{K_i} для функции, не принадлежащей множеству K_i ($i \in \{1,\dots,11\}$).

Рассмотрим набор вспомогательных утверждений, позволяющих получить критерий полноты.

Лемма 2. *Справедливо* $[0, 1, f_{K_5}, f_{K_6}] = M_2$.

Лемма 3. *Пусть* $g_1(x) = (--), g_2(x) = (10)$. *Тогда справедливо* $[g_1, g_2, f_{K_5}, f_{K_6}, f_{K_9}] = M_2$.

Лемма 4. *Пусть* $g_1(x) = (--), g_2(x) = (11)$. *Тогда справедливо* $[g_1, g_2, f_{K_2}, f_{K_5}, f_{K_6}, f_{K_7}] = M_2$.

Лемма 5. *Пусть* $g_1(x) = (--), g_2(x) = (1-)$. *Тогда справедливо* $[g_1, g_2, f_{K_2}, f_{K_5}, f_{K_6}, f_{K_7}] = M_2$.

Лемма 6. *Пусть* $g_1(x) = (--), g_2(x) = (00)$. *Тогда справедливо* $[g_1, g_2, f_{K_2}, f_{K_5}, f_{K_6}, f_{K_9}] = M_2$.

Лемма 7. *Пусть* $g_1(x) = (--), g_2(x) = (**)$. *Тогда справедливо* $[g_1, g_2, f_{K_2}, f_{K_5}, f_{K_6}, f_{K_7}] = M_2$.

Лемма 8. *Пусть* $g_1(x) = (--), g_2(x) = (*-)$. *Тогда справедливо* $[g_1, g_2, f_{K_2}, f_{K_5}, f_{K_6}, f_{K_7}] = M_2$.

Теорема. *Множество мультифункций Q является ES_U-полным тогда и только тогда, когда оно не содержится целиком ни в одном из классов $K_1 - K_{11}$.*

Список литературы

[1] Казимиров А. С., Пантелеев В. И., Токарева Л. В. Классификация и перечисление базисов клона всех гиперфункций ранга 2 // Известия Иркутского государственного университета. Серия Математика. 2014. Т 7. С. 61–78.

[2] Марченков С. С. Операторы замыкания с разветвлением по предикату // Вестник МГУ. Серия 1, Математика и механика. 2003. № 6. С. 37–39.

[3] Марченков С. С. Оператор замыкания с разветвлением по предикату равенства на множестве частичных булевых функций // Дискретная математика. 2008. Т. 20, вып. 6. С. 80–88.

[4] Марченков С. С. Оператор E-замыкания на множестве частичных функций многозначной логики // Математические вопросы кибернетики. М. : Физматлит, 2013. Т. 19. С. 227–238.

[5] Пантелеев В. И., Рябец Л. В. Оператор замыкания с разветвлением по предикату равенства на множестве гиперфункций ранга 2 // Известия Иркутского государственного университета. Серия Математика. Т. 10. С. 93–105.

ES_U-completeness criterion of multifunctions on two-element set

Panteleev Vladimir Innokentevich, Riabets Leonid Vladimirovich

Irkutsk State University, e-mail: vl.panteleyev@gmail.com, l.riabets@gmail.com

In this paper, we consider the action of the operator with branching on equality on the set of multifunction functions of rank 2. Eleven precomplete sets of multifunctions are determined and a completeness criterion is formulated.

Keywords: closure, equality predicate, multifunction, closed set, composition, completeness criterion.

УДК 519.716

Алгебры унарных мультиопераций конечного ранга

Перязев Николай Алексеевич

Санкт-Петербургский государственный электротехнический университет «ЛЭТИ» им. В. И. Ульянова (Ленина), e-mail: nikolai.baikal@gmail.com

В работе рассматриваются бинарные ношения как унарные мультиоперации. Определяются алгебры унарных мультиопераций в сигнатуре бинарные метаоперации подстановки и пересечения, унарная метаоперация обратимости и константные метаоперации тождественная, пустая и полная. Изучаются тождества выполнимые в таких алгебрах.

Ключевые слова: мультиоперация, суперпозиция, алгебра мультиопераций, тождество.

Введение

Изучение свойств операций на бинарных отношениях ведется достаточно давно. В связи с этим отметим следующие публикации [1–4]. Рассмотрению бинарных отношений как унарных мультиопераций и исследованию алгебр унарных мультиопераций посвящены работы [5–8].

Определение алгебр унарных мультиопераций

В этом разделе определяются алгебры унарных мультиопераций. При этом в качестве сигнатурных операций (метаопераций) взяты: бинарные метаоперации подстановки и пересечения, унарная метаоперация обратимости и константные метаоперации тождественная, пустая и полная.

Пусть A — произвольное множество, $B(A)$ — множество всех подмножеств A. Отображение f множества A в $B(A)$ называется унарной мультиоперацией на A. Если при этом все образы одноэлементные или пустые, то f называем квазиоперацией, если не пустые, то f называем гипероперацией, а если только одноэлементные, то операцией.

Будем использовать следующие обозначения:

- $\mathcal{M}_A^{(1)}$ — множество унарных мультиопераций на A;
- $\mathcal{H}_A^{(1)}$ — множество унарных гипероперaций на A;
- $\mathcal{P}_A^{(1)}$ — множество унарных квазиопераций на A;
- $\mathcal{O}_A^{(1)}$ — множество унарных операций на A.

Очевидно выполняются соотношения:

$$\mathcal{H}_A^{(1)} \subset \mathcal{M}_A^{(1)}, \mathcal{P}_A^{(1)} \subset \mathcal{M}_A^{(1)}, \mathcal{H}_A^{(1)} \cap \mathcal{P}_A^{(1)} = \mathcal{O}_A^{(1)}.$$

Ранг k мультиоперации определим так: $k = |A|$.

Определим следующие унарные мультиоперации:

- пустая мультиоперация
  $o(a) = \varnothing$;
- полная мультиоперация
  $u(a) = A$;
- тождественная мультиоперация
  $e(a) = \{a\}$.

Определим следующие метаоперации на множестве унарных мультиопераций: если $f, g \in \mathcal{M}_A^{(1)}$, то

- бинарная метаоперация подстановки g в f $(*)$
  $(f * g)(a) = \bigcup_{b \in g(a)} f(b)$;
- бинарная метаоперация пересечения f и g $(\cap)$
  $(f \cap g)(a) = f(a) \cap g(a)$;
- унарная метаоперация обратимости (μ)
  $(\mu f)(a) = \{b \mid a \in f(b)\}$;
- константные метаоперации для мультиопераций тождественной (e), пустой (o) и полной (u).

Определение 1. *Алгеброй $\mathcal{R}$ унарных мультиопераций над множеством A называется любое подмножество $R \subseteq \mathcal{M}_A^{(1)}$, содержащее мультиоперации тождественную, пустую, полную и замкнутое относительно метаопераций подстановки, пересечения и обратимости.*

Многообразие алгебр $\mathcal{Q}^1$

Сигнатура: $\Omega = \langle \cdot, \wedge, ^{-1}, 1, \bot, \top \rangle$. Обозначение: $x \leqslant y \Leftrightarrow x \wedge y = x$.

Определение 2. *Многообразия $\mathcal{Q}^1$ задается следующей системой тождеств:*

1. $x \cdot (y \cdot z) = (x \cdot y) \cdot z$;
2. $x \cdot 1 = 1 \cdot x = x$;

3. $x \wedge (y \wedge z) = (x \wedge y) \wedge z$;
4. $x \wedge y = y \wedge x$;
5. $x \wedge x = x$;
6. $x \wedge \top = x$;
7. $x \cdot \bot = \bot \cdot x = \bot$;
8. $x \wedge \bot = \bot$;
9. $(x^{-1})^{-1} = x$;
10. $(x \cdot y)^{-1} = y^{-1} \cdot x^{-1}$;
11. $(x \wedge y)^{-1} = x^{-1} \wedge y^{-1}$;
12. $1^{-1} = 1$;
13. $\bot^{-1} = \bot$;
14. $\top^{-1} = \top$;
15. $x \wedge 1 = x^{-1} \wedge 1$;
16. $x \leqslant x \cdot (x^{-1} \cdot x)$;
17. $x \cdot (y \wedge z) \leqslant (x \cdot y) \wedge (x \cdot z)$;
18. $x \wedge (y \cdot z) \leqslant ((x \cdot z^{-1}) \wedge y) \cdot ((y^{-1} \cdot x) \wedge z)$.

В силу ассоциативности $\cdot$ и $\wedge$ будем опускать скобки при повторении этих операций. Также будем опускать скобки по приоритету $\cdot$ над $\wedge$.

Теорема 1. *В алгебрах многообразия $\mathcal{Q}^1$ выполняются:*
1. $x \leqslant x$;
2. $x \leqslant y, y \leqslant z \Rightarrow x \leqslant z$;
3. $x \leqslant y, y \leqslant x \Rightarrow x = y$;
4. $x \leqslant y \Rightarrow x^{-1} \leqslant y^{-1}$;
5. $x \leqslant z, y \leqslant v \Rightarrow x \cdot y \leqslant z \cdot v$;
6. $x \leqslant z, y \leqslant v \Rightarrow x \wedge y \leqslant z \wedge v$;
7. $(x \wedge y) \cdot z \leqslant x \cdot z \wedge y \cdot z$;
8. $x \wedge y \leqslant x$;
9. $x \leqslant \top \cdot x$;
10. $x \leqslant x \cdot \top$;
11. $\top = \top \cdot x \Leftrightarrow 1 \leqslant x^{-1} \cdot x$;
12. $\top = x \cdot \top \Leftrightarrow 1 \leqslant x \cdot x^{-1}$;
13. $x^{-1} \cdot x \leqslant 1 \Rightarrow x \cdot (y \wedge z) = x \cdot y \wedge x \cdot z$;
14. $z \cdot z^{-1} \leqslant 1 \Rightarrow (x \wedge y) \cdot z = x \cdot z \wedge y \cdot z$;
15. $z^{-1} \cdot z \leqslant 1 \Rightarrow x \wedge y \cdot z = (x \cdot z^{-1} \wedge y) \cdot (y^{-1} \cdot x \wedge z)$;
16. $y \cdot y^{-1} \leqslant 1 \Rightarrow x \wedge y \cdot z = (x \cdot z^{-1} \wedge y) \cdot (y^{-1} \cdot x \wedge z)$;
17. $x^{-1} \cdot x \leqslant 1 \Rightarrow x = x \cdot x^{-1} \cdot x$;
18. $x \cdot x^{-1} \leqslant 1 \Rightarrow x = x \cdot x^{-1} \cdot x$.

Теорема 2. *Если $\mathcal{R}$ алгебра унарных мультиопераций конечного ранга, то $\mathcal{R} \in \mathcal{Q}^1$ (при интерпретации: $\cdot \to *$; $\wedge \to \cap$; $^{-1} \to \mu$; $1 \to e$; $\bot \to o$; $\top \to u$).*

Список литературы

[1] Riguet J. Relations binaires, fermetures, correspondances de Galois // Bull. Soc. math. Ffance. 1948. N 1–4 (76). P. 114–155.

[2] Вагнер В. В. Теория отношений и алгебра частичных отображений // Теория полугрупп и ее приложения. Саратов : Изд-во Саратовского университета, 1965. Вып. 1. С. 3–178.

[3] Диасамидзе Я. И., Махарадзе Ш. И. Полные полугруппы бинарных отношений. М. : Спутник+, 2010. 657 с.

[4] Lau D. Function Algebras on Finite Sets. Springer-Verlag Berlin YeideWater Resourses Research, 2006. 668 p.

[5] Казимиров А. С., Перязев Н. А. Алгебры унарных мультиопераций // Международная конференция «Мальцевские чтения» : тезисы докладов. Новосибирск, 2013. С. 156.

[6] Peryazev N. A., Peryazeva Yu. V., Sharankhaev I. K. Minimal Algebras of Unary Multioperations // Journal Siberian Federal University. Mathematics & Physics. 2016. Vol. 9, N 2. P. 220–224.

[7] Малина А. В., Перязев Н. А. Шефферовы мультиоперации в полной алгебре унарных мультиопераций ранга 4 // Известия Юго-Западного университета. 2016. № 1. С. 29–32.

[8] Перязев Н. А., Шаранхаев И. К. Алгебры мультиопераций // Algebra and Model Theory 11. Collection of hahers. Novosibirsk : NSTU Publisher, 2017. P. 102–111.

Algebras of unary multioperations of finite rank

Peryazev Nikolay Alekseevich

Saint-Petersburg Electrotechnical University «LETI», e-mail: nikolai.baikal@gmail.com

In work binary relation as unary multioperations are considered. Algebras of unary multioperations in a signature binary metaoperations of substitution and crossing, unary metaoperation of reversibility and constant metaoperations identical, empty and full are defined. Identities in such algebras are studied.

Keywords: multioperation, superposition, algebra of multioperations, identity.

УДК 510.665

О полноте теорий второго порядка с аксиомами бесконечности

Смелянский Дмитрий Михайлович

Московский центр непрерывного математического образования, e-mail: dmsolardens@gmail.com

Доклад посвящен определению понятия аксиом бесконечности для формально-логических систем и постановке вопроса о существовании полных теорий второго порядка с аксиомами бесконечности, в дополнение к чему показано, что основные примеры полных эффективных теорий первого порядка не являются таковыми при расширении их логикой второго порядка.

Ключевые слова: теория второго порядка, полнота, аксиоматизируемость, аксиома бесконечности.

В работе ставится вопрос о существовании полных эффективно аксиоматизируемых теорий второго порядка с аксиомами бесконечности. Определение языка и системы вывода для логики второго порядка дается в соответствии с [1]. В отношении семантики рассматривается два рода моделей: стандартные (по Черчу главные) и так называемые модели Хенкина (по Черчу вторичные). Для последних, как показал Хенкин, имеет место полнота дедуктивной системы, и, как следствие, ее компактность.

1. Под аксиомой бесконечности понимается формула, не выполнимая ни в какой конечной модели. Соответственно, отрицание такой формулы может быть названо аксиомой конечной структуры. В действительности, не существует абсолютного формального признака конечной и бесконечной структуры, как показывают утверждения:

Предложение 1. *Не существует формулы, истинной во всех конечных структурах и только в них.*

Утверждение может быть усилено:

Предложение 2. *Если формула выполнима в конечной структуре произвольной мощности, то она выполнима и в некоторой бесконечной структуре.*

Как обращение первого утверждения получаем:

Предложение 3. *Не существует универсального следствия из всех аксиом бесконечности.*

Как следствие отсюда получаем существование нестандартных бесконечных структур, в том смысле, что они не имеют изоморфной множеству натуральных чисел подструктуры.

2. В языке второго порядка арифметика является конечно аксиоматизируемой теорией, что позволяет формализовать ее внутреннюю интерпретируемость, именно существование такой внутренней модели описывает формула:

$$\exists N \exists R \exists z$$
$$(\forall x N(x) \exists! y N(y) R(x,y) \wedge \forall u N(u) \forall v N(v) \forall w N(w)(R(u,w) \wedge R(v,w) \to u = v) \wedge$$
$$\wedge \neg \exists x N(x) R(x,z) \wedge \forall P((P(z) \wedge \forall u N(u) \forall v N(v)(R(v,w) \to (P(u) \to P(v)))) \to$$
$$\to \forall x N(x) P(x)))$$

Из основных результатов о неполноте формальных теорий отсюда следует, что любая эффективно аксиоматизируемая теория второго порядка, совместная с приведенной формулой, неполна.

3. По этой причине расширения в логике второго порядка ряда известных теорий первого порядка, таких как:

- теория плотного линейного порядка без первого и последнего элемента;
- теория вещественно-замкнутых полей;
- арифметика Пресбургера;

представляющих основные примеры полных систем, полными не оказываются. Действительно, каждая из них либо интерпретирует арифметику, либо совместна с такой интерпретацией.

Можно показать, однако, что такие расширения консервативны. Поэтому все полные теории с аксиоматикой первого порядка являются расширениями полных теорий первого порядка с идентичными аксиомами.

4. Еще один ряд примеров полных теорий в случае первого порядка доставляет свойство категоричности; в случае же второго порядка не имеет смысла, как следует из утверждения:

Предложение 4. *Пусть* $\mathfrak{K}$ *— некоторая структура для языка второго порядка. Если* T *— теория с аксиомой бесконечности, то она имеет модель* $\mathfrak{M}$*, для которой существует подмножество* N *ее носителя* M*, такое что вместе с ограничениями на него всех предикатов из* $\mathfrak{M}$ *оно образует подструктуру* $\mathfrak{N}$*, изоморфную* $\mathfrak{K}$*.*

Отсюда следует, что если какая-либо теория категорична хотя бы в некоторой бесконечной мощности, то всякая ее модель должная содержать все возможные подструктуры, что невозможно, если модель не главная.

Таким образом примеры эффективно аксиоматизируемых полных теорий второго порядка можно найти только среди систем с нестандартной бесконечностью.

Список литературы

[1] Правиц Д. Натуральный вывод. Теоретико-доказательственное исследование. М. : Лори, 1997. 108 с.

[2] Черч А. Введение в математическую логику. М. : Либроком, 2009. 482 с.

[3] Такеути Г. Теория доказательств. М. : Мир, 1978. 412 с.

On the Completeness of Second-Order Theories with Infinity Axioms

Smelianskiy Dmitry Mikhailovich

Moscow Center for Continuous Mathematical Education, e-mail: dmsolardens@gmail.com

The talk is devoted to defining of the notion of infinity axioms for the formal logic systems and go statement of the question: are there any second order theories that are complete? In addition it is shown that the main examples of first order ones become not such by their extension having applied the second order logic.

Keywords: second order theory, completeness, axiomatizability, infinity axiom.

УДК 519.716

Критерий ES_I-полноты множества мультифункций ранга 2

Тагласов Эдуард Станиславович, Пантелеев Владимир Иннокентьевич

Иркутский государственный университет, e-mail: taglasov1@gmail.com, vl.panteleyev@gmail.com

В работе рассматривается ES_I-замыкание мультифункций, заданных на двухэлементном множестве. Приводятся примеры полных множеств, формулируется и доказывается критерий функциональной полноты.

Ключевые слова: мультифункция, полнота, базис, замыкание, суперпозиция.

Наряду с классическими функциональными системами над множеством k-значных функций ($k \geqslant 2$) достаточно давно изучаются системы, в которых рассматриваются обобщения функций k-значной логики: частичные функции, мультифункции и гиперфункции — функции, заданные на конечном множестве A и принимающие в качестве своих значений подмножества множества A, относительно оператора суперпозиции (например, [1; 2; 11]).

Оператор суперпозиции приводит, как правило, к счетной или континуальной классификации, поэтому вызывают интерес операторы замыкания, которые порождают конечные классификации функций. К таким операторам относятся, в частности, операторы параметрического и позитивного замыканий, оператор E-замыкания [3–6; 8–10].

Пусть $E_2 = \{0, 1\}$. Множество всех мультифункций ранга 2 обозначается как M_2 и определяется следующим образом:

$$M_{2,n} = \left\{ f \mid f : E_2^n \to 2^{E_2} \right\}, \; M_2 = \bigcup_n M_{2,n},$$

При дальнейшем изложении мы не будем различать множество из одного элемента и элемент этого множества. Для множества E_2 будем использовать обозначение «$-$» (прочерк), а для пустого множества — $*$.

Пусть $f(x_1, \ldots, x_n)$, $f_1(x_1, \ldots, x_m), \ldots, f_n(x_1, \ldots, x_m)$ — мультифункции. Суперпозиция $f(f_1(x_1, \ldots, x_m), \ldots, f_n(x_1, \ldots, x_m))$ задает мультифункцию $g(x_1, \ldots, x_m)$ следующим образом: если набор $(\alpha_1, \ldots, \alpha_m) \in E_2^m$, то по определению

$$g(\alpha_1, \ldots, \alpha_m) = \begin{cases} \bigcap\limits_{\beta_i \in f_i(\alpha_1, \ldots, \alpha_m)} f(\beta_1, \ldots, \beta_n), & \text{если это пересечение не пусто;} \\ \bigcup\limits_{\beta_i \in f_i(\alpha_1, \ldots, \alpha_m)} f(\beta_1, \ldots, \beta_n), & \text{иначе.} \end{cases}$$

Определенную таким образом суперпозицию будем называть I-суперпозицией. I-суперпозиция позволяет находить значения мультифункций на наборах, составленных из элементов множества $\{0, 1, -, *\}$.

Пример. Пусть мультифункция $f(x,y)$ такая, что $f(0,0)=0$, $f(0,1)=-$, $f(1,0)=*$, $f(1,1)=1$. Тогда $f(0,-)=f(0,0)\cap f(0,1)=0$ и, так как $f(1,0)\cap f(1,1)=*$, то $f(1,-)=f(1,0)\cup f(1,1)=1$.

Будем говорить, что мультифункция $g(x_1,\ldots,x_n)$ получается из функций $f_1(x_1,\ldots,x_n)$, $f_2(x_1,\ldots,x_n)$ с помощью операции разветвления по предикату равенства, если для некоторых $i,j\in\{1,\ldots,n\}$ выполняется соотношение

$$g(x_1,\ldots,x_n)=\begin{cases} f_1(x_1,\ldots,x_n), & \text{если } x_i=x_j,\\ f_2(x_1,\ldots,x_n), & \text{в противном случае.}\end{cases}$$

Определим ES_I-замыкание множества $Q\subseteq M_2$ как множество всех мультифункций из M_2, которые можно получить из множества Q с помощью операций введения фиктивных переменных, отождествления переменных, I-суперпозиции и разветвления по предикату равенства. ES_I-замыкание множества Q обозначаем как $[Q]$.

Множество гиперфункций, которое совпадает со своим замыканием, называется ES_I-замкнутым классом. Множество R называется полным в M_2, если ES_I-замыкание R совпадает с M_2.

Множество функций, сохраняющих предикат R, обозначим как $Pol\ R$. Далее m-местный предикат, содержащий n наборов, будем задавать матрицей размерности $m\times n$, в которой столбцами являются наборы из предиката.

Введем в рассмотрение следующие 9 множеств мультифункций:
$K_1=\{f\mid f(0,\ldots,0)\in\{0,*\}\}$; $K_2=\{f\mid f(1,\ldots,1)\in\{1,*\}\}$;
$K_3=O_2^*$; $K_4=H_2$; $K_5=\{f\mid f(\tilde{\alpha})\in\{*,1,-\}\}$;
$K_6=\{f\mid f(\tilde{\alpha})\in\{*,0,-\}\}$; $K_7=PolR_7$; $R_7=\begin{pmatrix}0&1&*&-\\1&0&*&-\end{pmatrix}$;
$K_8=PolR_8$; $R_8=\begin{pmatrix}0&1&*&*&*&*&0&1&-\\1&0&0&1&-&*&*&*&*\end{pmatrix}$;
$K_9=\{f\mid *\in f(0,\ldots,0)\cup f(1,\ldots,1)$ либо $f(0,\ldots,0)=0$ и $f(1,\ldots,1)=1\}$.

Теорема 1. *Множества K_1-K_9 являются ES_I-замкнутыми.*

Теорема 2. *Для множеств $K_1,\ldots,K_9$ выполняется $K_i\not\subseteq K_j$ при $i\neq j$.*

Будем использовать обозначение f_{K_i} для функции, не принадлежащей множеству K_i ($i\in\{1,\ldots,9\}$).

Лемма 1. *Справедливо* $[0,1,f_{K_3},f_{K_4}]=M_2$.

Лемма 2. *Пусть* $g_1(x)=(--), g_2(x)=(10)$. *Тогда справедливо* $[g_1,g_2,f_{K_3},f_{K_4},f_{K_7}]=M_2$.

Лемма 3. *Пусть* $g_1(x)=(--), g_2(x)=(11)$. *Тогда справедливо* $[g_1,g_2,f_{K_3},f_{K_4},f_{K_5}]=M_2$.

Лемма 4. *Пусть* $g_1(x) = (--), g_2(x) = (00)$. *Тогда справедливо* $[g_1, g_2, f_{K_3}, f_{K_4}, f_{K_6}] = M_2$.

Теорема 3. *Множество мультифункций* R *является* ES_I*-полным тогда и только тогда, когда оно не содержится целиком ни в одном из классов* $K_1 - K_9$.

Доказательство. Отождествлением переменных из функции f_{K_9} можно получить одну из восьми следующих одноместных функций:

$f^1_{K_9} = (--)$, $f^2_{K_9} = (00)$, $f^3_{K_9} = (11)$, $f^4_{K_9} = (10)$, $f^5_{K_9} = (0-)$, $f^6_{K_9} = (-0)$, $f^7_{K_9} = (1-)$, $f^8_{K_9} = (-1)$.

Так как $f^6_{K_9}(f^6_{K_9}(x)) = f^5_{K_9}$ и $f^5_{K_9}(f^5_{K_9}(x)) = (00)$, $f^8_{K_9}(f^8_{K_9}(x)) = f^7_{K_9}$ и $f^7_{K_9}(f^7_{K_9}(x)) = (11)$, то достаточно рассмотреть первые четыре случая.

Случай 1. $f^1_{K_9} = (--)$. Из функции f_{K_5} отождествлением переменных можно получить функцию $h(x, y)$ такую, что на наборах (01) и (10) она принимает одно из следующих четырех значений — (00), (01), (0∗), (0−).

Определим функцию $t(x, y)$:

$$t(x,y) = \begin{cases} -, \text{ если } x = y; \\ h(x,y), \text{ иначе.} \end{cases}$$

Суперпозиция $t(x, -)$ определяет одноместную функцию $p(x) = (0\beta)$, где $\beta \in \{0, -, 1\}$. Первые два случая сводятся к лемме 4. Рассмотрим оставшийся случай: $p(x) = (01)$.

Оператор разветвления по предикату равенства позволяет из функции $p(x)$ и $-$ получить функцию $(-01-)$, а с помощью суперпозиции — (10). Справедливость утверждения следует из леммы 2.

Случай 2. $f^2_{K_9} = (00)$. Подставляя константу 0 в функцию f_{K_1}, получим одно из двух множеств функций: $\{0, 1\}$ или $\{0, -\}$.

Для первого множества воспользуемся леммой 1. Для второго леммой 4.

Случай 3. $f^3_{K_9} = (11)$. Подставляя константу 1 в функцию f_{K_2}, получим одно из двух множеств функций: $\{0, 1\}$ или $\{1, -\}$.

Для первого множества воспользуемся леммой 1. Для второго леммой 3.

Случай 4. $f^4_{K_9} = (10)$. Функция f_{K_8} на некоторой паре противоположных наборов возвращает одну из следующих пар — (00), (11), (0−), (−0), (1−), (−1), (11). А это означает, что, подставляяя в функцию f_{K_8} на соответствующие места переменных функцию (10), можно получить одну из следующих одноместных функций: (00), (11), (0−), (−0), (1−), (−1), (−−), которые легко сводятся к случаю 1.

□

Список литературы

[1] Ло Джукай. Максимальные замкнутые классы в множестве частичных функций многозначной логики // Кибернетический сборник. Новая серия. М. : Мир, 1988. Вып. 25. С. 131–141.

[2] Ло Джукай. Теория полноты для частичных функций многозначной логики // Кибернетический сборник. Новая серия. М. : Мир, 1988. Вып. 25. С. 142–157.

[3] Марченков С. С. О выразимости функций многозначной логики в некоторых логико-функциональных языках // Дискретная математика. 1999. Т. 11, вып. 4. С. 110–126.

[4] Марченков С. С. Операторы замыкания с разветвлением по предикату // Вестник МГУ. Серия 1, Математика и механика. 2003. № 6. С. 37–39.

[5] Марченков С. С. Оператор замыкания с разветвлением по предикату равенства на множестве частичных булевых функций // Дискретная математика. 2008. Т. 20, вып. 6. С. 80–88.

[6] Марченков С. С. Оператор E-замыкания на множестве частичных функций многозначной логики // Математические вопросы кибернетики. М. : Физматлит, 2013. Вып. 19. С. 227–238.

[7] Матвеев С. А. Построение всех E-замкнутых классов частичных булевых функций // Математические вопросы кибернетики. М. : Физматлит, 2013. Вып. 18. С. 239–244.

[8] Пантелеев В. И., Рябец Л. В. Оператор замыкания с разветвлением по предикату равенства на множестве гиперфункций ранга 2 // Изв. Иркут. гос. ун-та. Сер. Математика. 2014. Т. 10. С. 93–105.

[9] Рябец Л. В. Параметрически замкнутые классы гиперфункций ранга 2 // Известия Иркутского государственного университета. Серия Математика. 2016. Т. 17. С. 46–61.

[10] Рябец Л. В. Операторы параметрического и позитивного замыкания на множестве гиперфункций ранга 2 // Интеллектуальные системы. Теория и приложения. 2016. Т. 20, вып. 3. С. 79–84.

[11] Machida H., Pantovic J. On maximal hyperclones on $\{0, 1\}$ — a new approach // Proceedings of 38th IEEE International Symposium on Multiple-Valued Logic (ISMVL 2008). 2008. P. 32–37.

Criterion for the ES_I-completeness of Sets of Multifunctions of Rank 2

Taglasov Eduard Stanislavovich, Panteleev Vladimir Innokentevich

Irkutsk State University , e-mail: taglasov1@gmail.com, vl.panteleyev@gmail.com

In this paper the ES_I-closure of multifunction defined on a two-element set is considered. Examples of complete sets are given, a criterion of functional completeness is formulated and proved.

Keywords: multifunction, completeness set, base, closing, superposition.

УДК 519.7

Алгоритм минимизация мультопераций в классе ключевых стандартных форм

Тодиков Сергей Игоревич

Санкт-Петербургский государственный электротехнический университет «ЛЭТИ» им. В. И. Ульянова (Ленина), e-mail: sergeytodikov@gmail.com

В работе рассматривается вопрос минимизации мультиопераций в классе ключевых стандартных форм. В основе работы лежит разработанный алгоритм минимизации мультиопераций для $n = 2$ и $n = 3$ в классе ключевых стандартных форм. С помощью разработанного алгоритма получены минимальные представления мультиопераций для $n = 2$ и $n = 3$, средняя сложность минимального представления мультиопераций и количественное распределение мультиопераций по сложностям полученных минимальных представлений в классе ключевых стандартных форм. Произведено сравнение полученных результатов минимизации мультиопераций в классе ключевых стандартных форм с минимизацией мультиопераций в классе стандартных форм.

Ключевые слова: мультиоперация, суперклон, ключевая стандартная форма, алгоритм, минимизация.

В работе рассматривается реализация алгоритма нахождения представления минимальной сложности для мультиопераций в классе ключевых стандартных форм.

Пусть 2^A — множество всех подмножеств A. Отображением из A^n в 2^A называется n-местной мультиоперацией над A. Множество всех n-местных мультиопераций на A будем обозначать через H_n^A. При $|A| = k$ будем использовать обозначение H_n^k. Мультиоперации заданные на k-элементном множестве A будем называть мультиоперациями ранга k.

Определим бинарную мультиоперацию $\cap \in H_k^2$ как $\cap(a, b) = \{a\} \cap \{b\}$. В дальнейшем будем использовать суффиксную форму записи $\cap(a, b) = a \cap b$. Эта мультиоперация является коммутативной и ассоциативной. Также эта мультиоперация принадлежит любому суперклону [1], что делает естественным её использование для построений формульных представлений мультиопераций.

Через $d_{i,\alpha}^n \in H_k^n$ обозначим следующие мультиоперации:

$$d_{i,\alpha}^n = (2^k - 1, ..., 2^k - 1, \alpha^i, 2^k - 1, ..., 2^k - 1), (1 \leqslant i \leqslant k^n),$$

где $\alpha \in \{2^k - 1, ..., 2^k - 1\}$. В частности $d_{1,\alpha}^0 = (\alpha)$. Если $\alpha = 2^k - 1$, то используем обозначение d^n, то есть $d^n = (2^k - 1, ..., 2^k - 1)$.

В [2] была введена ключевая стандартная форма мультиопераций

$$f(x_1, ..., x_n) = \bigcap_j d_j(x_{j_1}, ..., x_{j_m}),$$

при котором выполняется $d_j \in \left\langle f, d_{1,1}^1, ..., d_{s,2^{s-1}}^1, ..., d_{k,2^{k-1}}^1 \right\rangle$.

Также в [2] была введена лемма, говорящая о том, что если $f \in H_k^n$ и $f \neq d^n$, то существует разложение по аргументу x_i:

$$f(x_1, ..., x_n) = f_0 \cap f_1 \cap f_2 \cap ... \cap f_2^{s-1} \cap ... \cap f_2^{k-1},$$

где в f_0 аргумент x_i является фиктивным, а f_2^{k-1} такие, что $2^r - 1$ остаточные по аргументу x_i при $r \neq s$ равным d^{n-1}, при этом выполняется $f_0, f_2^{s-1} \in \left\langle f, d_{1,1}^1, ..., d_{s,2^{s-1}}^1, ..., d_{k,2^{k-1}}^1 \right\rangle, s \in \{1, ..., k\}$.

Пример 1. Представим мультиоперацию $f \in H_2^n$ заданной векторно $f(x_1, x_2, x_3) = (20312001)$ в ключевой стандартной форме.

$$f(x_1, x_2, x_3) = d_{2,1}^1(x_3) \cap d_{1,2}^1(x_2) \cap d_{7,0}^3(x_1, x_2, x_3)$$

Также данную мультиоперацию можно представить следующим видом:

$$f(x_1, x_2, x_3) = d_{2,1}^1(x_3) \cap d_{1,2}^1(x_2) \cap d_{2,0}^2(x_2, x_3) \cap d_{3,2}^2(x_1, x_3) \cap d_{4,1}^2(x_1, x_3) \cap d_{3,2}^2(x_1, x_2) \cap d_{4,1}^2(x_1, x_2) \cap d_{6,0}^3(x_1, x_2, x_3) \cap d_{7,0}^3(x_1, x_2, x_3)$$

Как видно, представление мультиопераций в ключевой стандартной форме не единственно.

Под минимальностью будем понимать представление мультиоперации в виде ключевой стандартной формы с наименьшим количеством компонент пересечения. Количество компонент пересечения в представление назовем его сложностью.

Работа алгоритма заключается в наилучших заменах нулевых элементов мультиоперации с помощью леммы, так как именно на этих шагах ключевая стандартная форма дает разные сложности.

На вход алгоритма подается вектор, представляющий мультиоперацию.

На выходе алгоритма получим минимальную ключевую стандартную форму, представляющую мультиоперацию и сложность её формы.

Работу алгоритма можно представить следующими шагами:

Шаг 1. Выполнить основные шаги алгоритма представления мультиоперации в ключевой стандартной формы до момента замены нулевых элементов мультиоперации, где начинает работать лемма.

Шаг 2. Если в мультиоперации нет ни одного нулевого элемента, то перейти к шагу 1, иначе переходим к шагу 3.

Шаг 3. Если в мультиоперации нулевой элемент можно заменить на элемент $2^k - 1$, то производим замену. Если на данном шаге все нулевые элементы заменяются на элементы $2^k - 1$, то возвращаемся на шаг 1.

Шаг 4. Если с помощью замены нулевых элементов можно построить одинаковую последовательность элементов в мультиоперации, то производим замену, создаем последовательность и переходим к шагу 1, иначе переходим к шагу 5.

Шаг 5. Производим замену нулевых элементов с помощью элементов, которые получаются по остаточной мультиоперации от последней переменной в мультиоперации и возвращаемся к шагу 1.

Для тестирования алгоритма была реализована компьютерная программа и проведена минимизация всех мультиопераций в классе ключевых стандартных форм для $n = 2$ и $n = 3$.

Мультиоперации вида $d^0_{1,0}$ и $d^0_{1,3}$ являются специфическими для данного алгоритма и найти их сложность по алгоритму невозможно, но они имеют сложность 1, так как их представление в ключевой стандартной форме очевидно и сложность каждого представления равна 1. Для остальных мультиопераций, с помощью алгоритма, были найдены все минимальные представления и их сложности.

Полученные данные позволили определить среднюю сложность минимального представления мультиопераций в классе ключевых стандартных форм для $n = 2$ и $n = 3$ и количественное распределение мультиопераций по сложностям полученных минимальных представлений.

$L_{aver}(2) = 2,36; L_{aver}(3) = 4,46$; где L_{aver} — средняя сложность минимального представления мультиопераций в классе ключевых стандартных форм.

Распределение полученных минимальных представления при $n = 2$ отображено в таблице 1 и при $n = 3$ в таблице 2. Используем следующие обозначения: L — сложность мультиопераций; K — количество мультиопераций, имеющих соответствующую сложность, P — процент от числа мультиопераций.

Таблица 1

L	K	P
1	28	10,51%
2	122	47,76%
3	92	36,22%
4	14	5,51%

Данные результаты позволяют сравнить минимизацию мультиопераций в классе ключевых стандартных форм с минимизацией в классе стандартных форм [3]. Средние сложности минимального представления мультиопераций в классе стандартных форм для $n = 2$ и $n = 3$ имеют следующие значения: $L_{aver}(2) = 2,36; L_{aver}(3) = 4,14$. В таблицах 3 и 4 показаны распределения минимальных представления при $n = 2$ и при $n = 3$ для класса стандартных форм.

При сравнении видно, что для мультиопераций от $n = 2$ минимизация почти совпала, а средние сложности минимального представления почти равны. Для мультиопераций от $n = 3$ минимизация по сложностям совпала, но зна-

Таблица 2

L	K	P
1	82	0,12%
2	1548	2,36%
3	9560	14,60%
4	22580	34,45%
5	21560	32,89%
6	8648	13,20%
7	1472	2,25%
8	86	0,13%

Таблица 3

L	K	P
1	24	9,45%
2	124	48,82%
3	92	36,22%
4	14	5,51%

Таблица 4

L	K	P
1	78	0,12%
2	1765	2,69%
3	13319	20,32%
4	28966	44,2%
5	17144	26,16%
6	3724	5,69%
7	512	0,78%
8	26	0,04%

чения P различаются, причем в классе стандартных форм он лучше. Также видно, что средняя сложность минимального представления в классе стандартных форм при $n = 3$ немного лучше, чем в классе ключевых стандартных форм. Это говорит о том, что минимальное представление мультиопераций в классе стандартных форм лучше, чем в классе ключевых стандартных форм,

но так как класс ключевых стандартных форм является частью класса стандартных форм, то получение таких результатов вполне естественно.

Список литературы

[1] Перязев Н. А. Стандартные формы мультиопераций в суперклонах // Известия Иркутского государственного университета. Серия Математика. 2010. Т. 3, № 4. С. 88-95.

[2] Peryazev N. A., Sharankhaev I. K. Galois theory for clones and superclones // Discrete Mathematics and Applications. 2016. Vol. 26. № 4. P. 227-238.

[3] Перязев Н. А., Яковчук И. А. Минимизация мультиопераций в классе стандартных форм // Известия Иркутского государственного университета. Серия Математика. 2009. Т. 2, № 2. С. 117-125.

Algorithm for Minimizing Multioperations in the Class of Key Standard Forms

Todikov Sergei Igorevich

Saint-Petersburg Electrotechnical University «LETI», e-mail: sergeytodikov@gmail.com

This article addresses the problem of minimizing multioperations in a class of key standard forms. The work is based on the developed algorithm for minimizing multi-operations for $n = 2$ and $n = 3$. Using the developed algorithm, all minimal representations of multioperations for $n = 2$ and $n = 3$, the average complexity of the minimal representation of multiopearions and the quantitative distribution of multioperations by the minimal complexity of the obtained minimal representation in the class of key standard forms are obtained. The obtained results of minimizing multioperations in the class of key standard forms are compared with the minimization of multioperations in the class of standard forms.

Keywords: multiopration, superclone, key standard form, algorithm, minimization.

УДК 510.64

Константа Сметанича и метод конечной канонической модели

Яшин Александр Данилович

Удмуртский государственный университет, e-mail: yashin.alexandr@yandex.ru

Метод конечной канонической модели, разработанный К. Шютте, применяется к так называемой логике Сметанича, определяющей новую логическую константу в интуиционистской пропозициональной логике. Это позволяет одновременно доказать семантическую полноту в классе соответствующих моделей Крипке и финитную аппроксимируемость логики Сметанича.

Ключевые слова: интуиционистская пропозициональная логика, новая логическая константа по П. С. Новикову, семантическая полнота, финитная аппроксимируемость.

В неклассических логиках для доказательства семантической полноты исчислений с успехом применяется так называемый метод *канонических моделей*. Точками таких моделей обычно являются непротиворечивые множества (или пары множеств) формул данного языка. Получаемые при этом модели часто следует понимать в обобщённом смысле, они обычно велики (несчётны). Далее для уменьшения размера полученных моделей применяются варианты *метода фильтрации*, позволяющие получать конечные модели (*финитная аппроксимируемость*).

В работе [1] К. Шютте продемонстрировал метод *конечной канонической модели* для интуиционистского пропозиционального исчисления Int, позволивший «одним махом» обосновать как семантическую полноту исчисления, так и его финитную аппроксимируемость.

В работе [2] Я. С. Сметанич предложил пример исчисления, определяющего новую логическую константу в Int по П. С. Новикову. Семантика этой константы в классе конечных моделей Крипке известна автору под названием *крыша* (из личных бесед автора с А. А. Мучником).

Логика Сметанича Sm формулируется в пропозициональном языке с дополнительной константой φ (имеет тот же синтаксический статус, что и константы 0 «ложь» и 1 «истина») [3]:

$Sm = Int + 1^\circ : \neg\neg\varphi + 2^\circ : \varphi \to (A \vee \neg A)$.

Это исчисление корректно в классе конечных моделей Крипке относительно интерпретации $a \Vdash \varphi \leftrightharpoons max(a)$.

В данной работе предлагается доказательство теоремы о семантической полноте Sm и параллельно теоремы о финитной аппроксимируемости методом конечной канонической модели.

Фиксируем формулу A_0, невыводимую в Sm. Через $Sub(A_0)$ обозначаем множество всех её подформул.

Введём множество формул

$$\Sigma(A_0) := Sub(A_0) \cup \{\varphi, \neg\varphi, \neg\neg\varphi\} \cup \{\neg A \mid A \in Sub(A_0)\}.$$

Множество $\Sigma(A_0)$ является конечным и замкнуто по подформульности.

В дальнейшем упоминание об A_0 будем опускать.

Упорядоченная пара подмножеств $\Gamma, \Delta \subseteq \Sigma$ называется *противоречивой* (относительно Sm), если $Sm \vdash \bigwedge \Gamma \to \bigvee \Delta$; в противном случае пара называется *непротиворечивой*. Примером непротиворечивой пары является пара $(\varnothing \mid \{A_0\})$.

Пара $(\Gamma \mid \Delta)$ называется *полной*, если $\Gamma \cup \Delta = \Sigma$.

Лемма 1. *Пусть пара* $(\Gamma \mid \Delta)$ *непротиворечива и* C *— произвольная формула* φ*-языка. Тогда по крайней мере одна из пар* $(\Gamma \cup \{C\} \mid \Delta)$, $(\Gamma \mid \Delta \cup \{C\})$ *непротиворечива.*

Следствие 1. *Любая непротиворечивая пара может быть дополнена до полной непротиворечивой пары.*

Полные непротиворечивые пары называем *типами*. Типы обозначаем буквами σ, τ, ..., при этом $\sigma = (\sigma^0 \mid \sigma^1)$. Иногда применяем наглядное изображение $\sigma = (\ldots B, \ldots C \ldots \mid \ldots D, \ldots)$, акцентируя внимание на нужные формулы. Заметим, что множество всех типов непусто и конечно.

Частичный порядок на множестве типов определяется по включению левых компонент:

$$\sigma \leqslant \tau :\Leftrightarrow \sigma^0 \subseteq \tau^0.$$

Нетрудно убедиться, что это действительно частичный порядок.

Лемма 2 (общие свойства типов)**.** *Имеют место следующие свойства типов:*

(i) $A \wedge B \in \sigma^0 \Rightarrow A \in \sigma^0$ *и* $B \in \sigma^0$*;*
(ii) $A \wedge B \in \sigma^1 \Rightarrow A \in \sigma^1$ *или* $B \in \sigma^1$*;*
(iii) $A \vee B \in \sigma^0 \Rightarrow A \in \sigma^0$ *или* $B \in \sigma^0$*;*
(iv) $A \vee B \in \sigma^1 \Rightarrow A \in \sigma^1$ *или* $B \in \sigma^1$*;*
(v) $A \to B \in \sigma^0 \Rightarrow A \in \sigma^1$ *или* $B \in \sigma^0$*;*
(vi) $A \to B \in \sigma^1 \Rightarrow$ *найдётся* $\tau \geqslant \sigma : A \in \tau^0$ *и* $B \in \tau^1$*;*
(vii) $\neg A \in \sigma^0 \Rightarrow A \in \sigma^1$*;*
(viii) $\neg A \in \sigma^1 \Rightarrow$ *найдётся* $\tau \geqslant \sigma : A \in \tau^0$*.*

Теперь приведём свойства типов, связанные с наличием константы φ.

Лемма 3. $\varphi \in \sigma^0 \Rightarrow max_{\mathcal{M}}(\sigma)$.

Доказательство. Предполагаем посылку и, от противного, неверно $max(\sigma)$. Найдётся $\tau > \sigma$, т. е. $\sigma^0 \subsetneq \tau^0$. Для некоторой формулы $B \in \Sigma$ имеем $B \in \sigma^1$ и $B \in \tau^0$. Что такое B?

1. Пусть $B \in Sub(A_0)$. Тогда $\neg B \in \Sigma$.

Имеем $\neg B \notin \tau^0$ (иначе τ противоречив). Поэтому $\neg B \in \tau^1$. $\neg B \in \sigma^1$. Тип σ имеет вид

$$\sigma = (\varphi, \ldots \mid B, \neg B, \ldots)$$

и оказывается противоречивым в силу аксиомы 2°.

2. Имеем $B \not\vdash \varphi$ (так как σ непротиворечив);

$B \not\vdash \neg\varphi$ (так как τ непротиворечив);

$B \not\vdash \neg\neg\varphi$, так как иначе $\sigma = (\varphi, \ldots \mid \neg\neg\varphi, \ldots)$, и σ оказывается противоречивым в силу $X \to \neg\neg X \in Int$.

3. Пусть $B \doteq \neg C$ для некоторой $C \in Sub(A_0)$. Изобразим типы $\sigma < \tau$:

$$\begin{array}{c} \tau = (\varphi, \neg C, \ldots \mid \ldots \quad\;\;) \\ \mid \\ \sigma = (\varphi, \ldots \mid \neg C, \ldots) \end{array}$$

Если $C \in \sigma^0$, то $C \in \tau^0$, т. е. τ противоречив.

Если $C \in \sigma^1$, то σ противоречив по аксиоме 2°. □

Лемма 4. $\forall\sigma\exists\tau \geqslant \sigma : \varphi \in \tau^o$.

Доказательство. В силу аксиомы 1° $\neg\neg\varphi \in \sigma^0$ (напомним, что $\neg\neg\varphi \in \Sigma$). По общим свойствам типов сначала $\neg\varphi \in \sigma^1$, затем $\exists\tau \geqslant \sigma : \varphi \in \tau^0$.

Следствие 2. $max(\sigma) \Rightarrow \varphi \in \sigma^0$.

Зададим на структуре $\mathcal{M}$ выделенный конус для интерпретации константы φ так:

$$\Phi := \{\sigma \in \mathcal{M} \mid max(\sigma)\}.$$

Для переменных $p \in Sub(A_0)$ оценку на $\mathcal{M}$ зададим так:

$$\sigma \Vdash p :\Leftrightarrow p \in \sigma^0.$$

Лемма 5 (семантическая)**.** *Для любой формулы $A \in \Sigma$, для любой $\sigma \in \mathcal{M}$:*

$$A \in \sigma^0 \Rightarrow \sigma \Vdash A;$$

$$A \in \sigma^1 \Rightarrow \sigma \nVdash A.$$

Доказательство. Доказательство. Оба утверждения доказываются одновременной индукцией по построению формулы A.

Для переменной $p \in \Sigma$ первое утверждение следует из определения оценки $\Vdash$ на $\mathcal{M}$, второе: из непротиворечивости типа и из $p \in \sigma^1$ получаем $p \notin \sigma^0$, далее по определению оценки $\Vdash$ получаем $\sigma \not\Vdash p$.

Для константы φ. Если $\varphi \in \sigma^0$, то по лемме 3 $max(\sigma)$. По определению конуса Φ имеем $\sigma \in \Phi$, т. е. $\sigma \Vdash \varphi$.

Если $\varphi \in \sigma^1$, то в силу непротиворечивости типов $\varphi \notin \sigma^0$. По следствию 2 имеем неверно $\max(\sigma)$, т. е. $\sigma \notin \Phi$, поэтому $\sigma \not\Vdash \varphi$.

Для связок $\wedge, \vee, \to, \neg$ шаги индукции проводятся обычным образом со ссылкой на общие свойства типов. □

Теорема 1. *Если $Sm \not\Vdash A_0$, то построенная конечная каноническая φ-шкала является моделью логики Sm, опровергающей формулу A_0.*

Список литературы

[1] Шютте К. Полные системы модальной и интуиционистской логики // Р. Фейс. Модальная логика. М. : Наука, 1974. С. 324–421.

[2] Сметанич Я. С. Об исчислениях высказываний с дополнительной операцией // ДАН СССР. 1961. Т. 139 № 2. С. 309–312.

[3] Яшин А. Д. Логика Сметанича T^{Φ} и два определения новой интуиционистской связки // Математические заметки. 1994. Т. 56, № 1. С. 135–142.

The Smetanich constant and finite canonical model method

Yashin Alexandr Danilovich, (Izhevsk, Russia)

Udmurt State University, e-mail: yashin.alexandr@yandex.ru

The method of finite canonical model described by K. Shchütte is applied to the Smetanich logic which determines a new logical constant in the intuitionistic propositional logic (in the sence of P. Novikov's approach). This method allows to prove semantical completeness and finite model property for Smetanich logic simultaneously.

Keywords: intuitionistic propositional logic, new logical constant in the P. Novikov sence, semantical completeness, finite model property.