ПОЛИЛИНЕЙНОЕ ПРОДОЛЖЕНИЕ БУЛЕВОЙ ФУНКЦИИ И АЛГОРИТМ ЕГО НАХОЖДЕНИЯ

Д. Н. Баротов[1], Р. Н. Баротов[2]

[1]*Финансовый университет при Правительстве Российской Федерации, Москва, Россия*
[2]*Худжандский государственный университет им. акад. Б. Гафурова, Худжанд, Таджикистан*
E-mail: dnbarotov@fa.ru, ruzmet.tj@mail.ru

В данной работе изучено существование и единственность полилинейного продолжения произвольной булевой функции. Доказано, что для любой булевой функции существует соответствующее полилинейное продолжение и оно единственно. Предложен алгоритм нахождения полилинейного продолжения булевой функции в явном виде и доказана его корректность.

A POLYLINEAR CONTINUATION OF A BOOLEAN FUNCTION AND ITS FINDING ALGORITHM

D. N. Barotov, R. N. Barotov

In this paper, we study the existence and uniqueness of a polylinear continuation of an arbitrary Boolean function. It is proved that for any Boolean function, there is a corresponding polylinear continuation and it is unique. An algorithm for finding the polylinear continuation of a Boolean function in explicit form is proposed and its correctness is proved.

1. Введение

В связи с приложениями решение системы логических уравнений играет важную роль в вычислительной математике и во многих других областях [1-3]. В результате развивается множество новых направлений и алгоритмов решения систем логических уравнений. Одно из этих направлений заключается в том, что, во-первых, система логических уравнений, заданная над кольцом булевых полиномов, преобразуется в систему уравнений над полем действительных чисел, а во-вторых, преобразованная система сводится либо к задаче численной минимизации соответствующей целевой функции [4] либо к системе полиномиальных уравнений, решаемой на множестве целых чисел [2] либо к эквивалентной системе полиномиальных уравнений, решаемой символьными методами [5].

Существуют много способов преобразовать систему логических уравнений в задачу минимизации в непрерывной области [1,6-11]. Однако одна из основных проблем этого метода заключается в том, что минимизируемая целевая функция в искомой области может иметь множество локальных минимумов, что значительно усложняет применимость этого метода на практике [1,3,7-10,12]. Полилинейное продолжение булевой функции играет важную роль в том числе и для уменьшения числа локальных минимумов целевой функции [3-

5,12]. Поэтому с учетом этой мотивации в данной статье рассматривается полилинейное продолжение булевой функции.

Определение 1. *Функцию* $f(x_1, x_2, \dots, x_n)$ *будем называть полилинейной функцией, если она линейна по каждому из своих аргументов.*

Пусть $\mathbb{B}^n = \{(x_1, x_2, \dots, x_n)\colon\ x_1, x_2, \dots, x_n \in \{0,1\}\}$ - множество всевозможных двоичных слов (булевых векторов) длины n,

$\mathbb{K}^n = \{(x_1, x_2, \dots, x_n)\colon\ 0 \le x_1, x_2, \dots, x_n \le 1\}$ - n -мерный куб, натянутый на булевых векторах длины n.

2. Алгоритм нахождения явного вида полилинейного продолжения булевой функции

В этом разделе мы конструируем явную формулу полилинейного продолжения булевой функции на основе простого алгоритма.

Пусть задана некоторая полилинейная функция $f(x_1, x_2, \dots, x_n)$. Тогда из полилинейности функции следует, что

$$f(x_1, x_2, \dots, x_n) = a_m(x_1, x_2, \dots, x_{m-1}, x_{m+1}, \dots, x_n) \cdot x_m + b_m(x_1, x_2, \dots, x_{m-1}, x_{m+1}, \dots, x_n),\ \ \forall m \in \{1,2, \dots, n\}.$$

Теперь из последней формулы наблюдаем следующее свойство:

$$f(x_1, x_2, \dots, x_{m-1}, (1-t) \cdot x'_m + t \cdot x''_m, x_{m+1}, \dots, x_n) = a_m(x_1, x_2, \dots, x_{m-1}, x_{m+1}, \dots, x_n) \cdot \left((1-t) \cdot x'_m + t \cdot x''_m\right) + b_m(x_1, x_2, \dots, x_{m-1}, x_{m+1}, \dots, x_n) = (1-t) \cdot a_m(x_1, x_2, \dots, x_{m-1}, x_{m+1}, \dots, x_n) \cdot x'_m + t \cdot a_m(x_1, x_2, \dots, x_{m-1}, x_{m+1}, \dots, x_n) \cdot x''_m + b_m(x_1, x_2, \dots, x_{m-1}, x_{m+1}, \dots, x_n) = \left(a_m(x_1, x_2, \dots, x_{m-1}, x_{m+1}, \dots, x_n) \cdot x'_m + b_m(x_1, x_2, \dots, x_{m-1}, x_{m+1}, \dots, x_n)\right) \cdot (1-t) + t \cdot \left(a_m(x_1, \dots, x_{m-1}, x_{m+1}, \dots, x_n) \cdot x''_m + b_m(x_1, \dots, x_{m-1}, x_{m+1}, \dots, x_n)\right) = (1-t) \cdot f(x_1, x_2, \dots, x_{m-1}, x'_m, x_{m+1}, \dots, x_n) + t \cdot f(x_1, x_2, \dots, x_{m-1}, x''_m, x_{m+1}, \dots, x_n),\ \ \forall x'_m, x''_m, t \in \mathbb{R}.$$

В частности

$$f(x_1, x_2, \dots, x_{m-1}, x_m, x_{m+1}, \dots, x_n) = f(x_1, x_2, \dots, x_{m-1}, (1-x_m) \cdot 0 + 1 \cdot x_m, x_{m+1}, \dots, x_n) = (1-x_m) \cdot f(x_1, x_2, \dots, x_{m-1}, 0, x_{m+1}, \dots, x_n) + x_m \cdot f(x_1, x_2, \dots, x_{m-1}, 1, x_{m+1}, \dots, x_n),\ \ \forall m \in \{1,2, \dots, n\} \quad (1)$$

По лемме Баротовых Д. Н. и Р. Н. для любой булевой функции $p(x_1, x_2, \dots, x_n)$ существует единственная в $\mathbb{K}^n$ неотрицательная полилинейная функция $p_D(x_1, x_2, \dots, x_n)$ такая, что

$$p_D(x_1, x_2, \dots, x_n) = p(x_1, x_2, \dots, x_n),\ \ \forall (x_1, x_2, \dots, x_n) \in \mathbb{B}^n \quad (2)$$

На основе (1) и (2) предлагаем алгоритм нахождения явного вида полилинейного продолжения булевой функции.

Algorithm: *нахождения полилинейного продолжения булевой функции в явной форме*

for s **from** 1 **to** n

do

$p_D(x_1, x_2, x_3, \dots, x_n) := p_D(x_1, x_2, \dots, x_{s-1}, 1, x_{s+1}, \dots, x_n) \cdot x_s +$
$p_D(x_1, x_2, \dots, x_{s-1}, 0, x_{s+1}, \dots, x_n) \cdot (1 - x_s)$

end for

return $p_D(x_1, x_2, x_3, \dots, x_n)$

Напишем результат этого алгоритма и докажем его корректность.

Теорема 1. *Предложенный алгоритм корректен и его результат может быть написан в следующем явном виде*:

$$p_D(x_1, x_2, \dots, x_n) = \sum_{(b_1, b_2, \dots, b_n) \in \mathbb{B}^n} p(b_1, b_2, \dots, b_n) \cdot \prod_{k=1}^{n} \big((2b_k - 1)x_k + (1 - b_k)\big).$$

Доказательство.

(i) корректность алгоритма, из формулы (1) и леммы Баротовых Д. Н. и Р. Н. следует, что предложенный алгоритм на каждом шаге функцию $p_D(x_1, x_2, \dots, x_n)$ тождественно преобразует, то есть не меняет её значение, а лишь меняет её формы, следовательно в результате получим другой вид $p_D(x_1, x_2, \dots, x_n)$.

(ii) результат алгоритма, предложенный алгоритм на выходе возвращает следующую сумму

$$\sum_{(b_1, b_2, \dots, b_n) \in \mathbb{B}^n} p_D(b_1, b_2, \dots, b_n) \cdot \prod_{k=1}^{n} \big((2b_k - 1)x_k + (1 - b_k)\big)$$

Доказательство этого факта проводим по методу математической индукции относительно количества переменных.

1) Если $n = 1$, то

$$p_D(x_1) = (1 - x_1) \cdot p_D(0) + x_1 \cdot p_D(1)$$
$$\equiv \sum_{b_1 \in \mathbb{B}^1} p_D(b_1) \cdot \prod_{k=1}^{1} \big((2b_k - 1)x_k + (1 - b_k)\big)$$

2) Если $n = m$, то предположим, что

$$p_D(x_1, x_2, \dots, x_m) = \sum_{(b_1, b_2, \dots, b_m) \in \mathbb{B}^m} p_D(b_1, b_2, \dots, b_m) \cdot \prod_{k=1}^{m} \big((2b_k - 1)x_k + (1 - b_k)\big)$$

3) Из формулы (1) следует, что

$$p_D(x_1, x_2, \dots, x_m, x_{m+1}) = p_D(x_1, x_2, \dots, x_m, 0) \cdot (1 - x_{m+1}) +$$
$p_D(x_1, x_2, \dots, x_m, 1) \cdot x_{m+1}$, а из пунктов $1) - 2)$ следуют, что

$$p_D(x_1, \dots, x_m, 0) = \sum_{(b_1, b_2, \dots, b_m) \in \mathbb{B}^m} p_D(b_1, \dots, b_m, 0) \cdot \prod_{k=1}^{m} \big((2b_k - 1)x_k + (1 - b_k)\big),$$

$$p_D(x_1, \dots, x_m, 1) = \sum_{(b_1, b_2, \dots, b_m) \in \mathbb{B}^m} p_D(b_1, \dots, b_m, 1) \cdot \prod_{k=1}^{m} \big((2b_k - 1)x_k + (1 - b_k)\big).$$

Подставляем значения $p_D(x_1, x_2, \dots, x_m, 0)$ и $p_D(x_1, x_2, \dots, x_m, 1)$ и находим $p_D(x_1, x_2, \dots, x_m, x_{m+1})$. По верхнему равенству $p_D(x_1, x_2, \dots, x_m, x_{m+1}) =$

$$p_D(x_1, x_2, \dots, x_m, 0) \cdot (1 - x_{m+1}) + p_D(x_1, x_2, \dots, x_m, 1) \cdot x_{m+1} =$$

$$\left(\sum_{(b_1, b_2, \dots, b_m) \in \mathbb{B}^m} p_D(b_1, b_2, \dots, b_m, 0) \cdot \prod_{k=1}^{m} \big((2b_k - 1)x_k + (1 - b_k)\big) \right) \cdot (1 - x_{m+1})$$

$$+$$

$$+ \left(\sum_{(b_1, b_2, \dots, b_m) \in \mathbb{B}^m} p_D(b_1, b_2, \dots, b_m, 1) \cdot \prod_{k=1}^{m} \big((2b_k - 1)x_k + (1 - b_k)\big) \right) \cdot x_{m+1} =$$

$$\sum_{(b_1, b_2, \dots, b_m) \in \mathbb{B}^m,\ b_{m+1}=0} p_D(b_1, b_2, \dots, b_m, b_{m+1}) \cdot \prod_{k=1}^{m} \big((2b_k - 1)x_k + (1 - b_k)\big)$$

$$\cdot \big((2b_{m+1} - 1)x_{m+1} + (1 - b_{m+1})\big) +$$

$$\sum_{(b_1, b_2, \dots, b_m) \in \mathbb{B}^m,\ b_{m+1}=1} p_D(b_1, b_2, \dots, b_m, b_{m+1}) \cdot \prod_{k=1}^{m} \big((2b_k - 1)x_k + (1 - b_k)\big)$$

$$\cdot \big((2b_{m+1} - 1)x_{m+1} + (1 - b_{m+1})\big) =$$

$$\sum_{(b_1, b_2, \dots, b_m, b_{m+1}) \in \mathbb{B}^{m+1}} p_D(b_1, b_2, \dots, b_m, b_{m+1}) \cdot \prod_{k=1}^{m+1} \big((2b_k - 1)x_k + (1 - b_k)\big).$$

Таким образом, во-первых, из метода математической индукции следует, что

$$p_D(x_1, \dots, x_n) = \sum_{(b_1, \dots, b_n) \in \mathbb{B}^n} p_D(b_1, \dots, b_n) \prod_{k=1}^{n} \big((2b_k - 1)x_k + (1 - b_k)\big), \quad \forall n \in \mathbb{N},$$

во-вторых, из $p_D(b_1, b_2, \dots, b_n) = p(b_1, b_2, \dots, b_n), \ \forall (b_1, b_2, \dots, b_n) \in \mathbb{B}^n$ следует, что

$$p_D(x_1, x_2, \dots, x_n) = \sum_{(b_1, b_2, \dots, b_n) \in \mathbb{B}^n} p(b_1, b_2, \dots, b_n) \prod_{k=1}^{n} \big((2b_k - 1)x_k + (1 - b_k)\big) \ \blacksquare$$

$p_D(x_1, x_2, \dots, x_n)$ - полилинейное продолжение произвольной булевой функции $p(x_1, x_2, \dots, x_n)$, причем в явном виде.

Для полноты изложения ещё докажем, что $p_D(x_1, x_2, \dots, x_n)$ - единственно.

От противного, пусть существует другая полилинейная функция $f(x_1, x_2, \dots, x_n)$ такая, что $f(b_1, b_2, \dots, b_n) = p(b_1, b_2, \dots, b_n), \ \forall (b_1, b_2, \dots, b_n) \in \mathbb{B}^n$. Тогда рассмотрим разность $d(x_1, x_2, \dots, x_n) = p_D(x_1, x_2, \dots, x_n) - f(x_1, x_2, \dots, x_n)$. Заметим, что во-первых, если $(x_1, x_2, \dots, x_n) \in \mathbb{B}^n$, то $d(x_1, x_2, \dots, x_n) = p_D(x_1, x_2, \dots, x_n) - f(x_1, x_2, \dots, x_n) = p(x_1, x_2, \dots, x_n) - p(x_1, x_2, \dots, x_n) = 0$. Во-вторых, функция $d(x_1, x_2, \dots, x_n)$ - полилинейна, так как разность полилинейных функций.

Из последнего равенства, полилинейности функции $d(x_1, x_2, \dots, x_n)$, принципа максимума следуют следующие неравенства [4,12-15]:

$$0 = \min_{(a_1,a_2,\dots,a_n)\in\mathbb{B}^n} d(a_1,\dots,a_n) \le d(x_1,x_2,\dots,x_n) \le \max_{(a_1,a_2,\dots,a_n)\in\mathbb{B}^n} d(a_1,\dots,a_n) = 0,$$

$\forall(x_1,x_2,\dots,x_n)\in\mathbb{K}^n \implies d(x_1,x_2,x_3,\dots,x_n)\equiv 0 \implies f(x_1,x_2,\dots,x_n)\equiv p_D(x_1,x_2,\dots,x_n)$ - это противоречие, что и требовалось доказать. ■

Таким образом, в явном виде найдено $p_D(x_1,x_2,\dots,x_n)$ - единственное в $\mathbb{K}^n$ неотрицательное полилинейное продолжение произвольной булевой функции $p(x_1,x_2,\dots,x_n)$.

СПИСОК ЛИТЕРАТУРЫ

1. *Файзуллин Р. Т., Дулькейт В. И., Огородников Ю. Ю.* Гибридный метод поиска приближенного решения задачи 3-выполнимость, ассоциированной с задачей факторизации // Труды Института математики и механики УрО РАН. 2013. Т. 19. №. 2. С. 285-294.

2. *Abdel-Gawad A. H., Atiya A. F., Darwish N. M.* Solution of systems of Boolean equations via the integer domain // Information Sciences. 2010. Т. 180. №. 2. С. 288-300.

3. *Barotov D. N., Barotov R. N.* Polylinear Transformation Method for Solving Systems of Logical Equations // Mathematics. 2022. Т. 10. №. 6. С. 918.

4. *Barotov D. et al.* Transformation Method for Solving System of Boolean Algebraic Equations // Mathematics. 2021. Т. 9. №. 24. С. 3299.

5. *Barotov D. N. et al.* The Development of Suitable Inequalities and Their Application to Systems of Logical Equations // Mathematics. 2022. Т. 10. №. 11. С. 1851.

6. *Faizullin R. T., Khnykin I. G., Dylkeyt V. I.* The SAT solving method as applied to cryptographic analysis of asymmetric ciphers // arXiv preprint arXiv:0907.1755. 2009.

7. *Gu J.* How to solve very large-scale satisfiability problems // Technical Report UUCS-Tr-88-032. 1990. Т. 1. №. 9. С. 88.

8. *Gu J.* On optimizing a search problem // Artificial Intelligence Methods and Applications. 1992. С. 63-105.

9. *Gu J.* Global optimization for satisfiability (SAT) problem // IEEE Transactions on Knowledge and Data Engineering. 1994. Т. 6. №. 3. С. 361-381.

10. *Gu J., Gu Q., Du D.* On optimizing the satisfiability (SAT) problem // Journal of Computer Science and Technology. 1999. Т. 14. №. 1. С. 1-17.

11. *Баротов Д. Н., Музафаров Д. З., Баротов Р. Н.* Об одном методе решения систем булевых алгебраических уравнений // Современная математика и концепции инновационного математического образования. 2021. Т. 8. №. 1. С. 17-23.

12. *Barotov D. N.* Target Function without Local Minimum for Systems of Logical Equations with a Unique Solution // Mathematics. 2022. Т. 10. №. 12. С. 2097.

13. *Мухсинов А., Бобоев Э. Д., Баротов Д. Н.* Формула представления решений начально-краевой задачи для одного многомерного параболического уравнения с сингулярными коэффициентами // Ученые записки Худжандского государственного университета им. академика Б. Гафурова. Серия: Естественные и экономические науки. 2016. №. 4. С. 18-25.

14. *Баротов Д. Н., Музафаров Д. З., Баротов Р. Н.* Алгебраический метод проверки четности битов // Интеллектуально-информационные технологии и интеллектуальный бизнес (ИНФОС-2021) : Материалы XII Междунар.науч.-технич. конф., 2021. С. 193-195.

15. *Баротов Д. Н., Баротов Р. Н.* Представление одного частного решения дифференциального уравнения с сингулярными коэффициентами // Ученые записки Худжандского государственного университета им. академика Б. Гафурова. Серия: Естественные и экономические науки. 2018. №. 2. С. 3-8.