А.А. Вороненко

УНИВЕРСАЛЬНЫЕ ФУНКЦИИ ДЛЯ КЛАССОВ БИЛИНЕЙНЫХ И ПОЛИЛИНЕЙНЫХ БУЛЕВЫХ ФУНКЦИЙ*

Рассматривается следующая задача.

Напомним, что булева функция $g(x_1, \dots, x_n)$ называется линейной, если она представима в виде $\alpha \oplus \alpha_1 x_1 \oplus \dots \oplus \alpha_n x_n$. Назовем булеву функцию k −полилинейной(билинейной при $k = 2$) если она представима в виде конъюнкции не более чем k линейных функций, не имеющих общих существенных переменных.Будем говорить, что частичная булева функция $f(x_1, \dots, x_n)$ порождает для заданногоk −полилинейнуюфункцию $g(x_1, \dots, x_n)$, если существует такая подобласть X области определения функции $f(x_1, \dots, x_n)$, что функция $\mathrm{g}(x_1, \dots, x_n)$ является единственной k −полилинейной, совпадающей с $f(x_1, \dots, x_n)$на этой подобласти. Функция $f(x_1, \dots, x_n)$(возможно частичная) называется универсальной для класса k −полилинейных функций n переменных, если порождает все такие функции. Случай $k = 2$ (универсальные функции для класса линейных булевых функций) впервые рассмотрен в работе [1]. В этой работе построена конструктивная линейная верхняя оценкана минимальную мощность области определения универсальной функции для класса линейных булевых функций.

В работе [2] для случая линейных функций тривиальная нижняя оценка размера области определения универсальной функции для класса линейных булевых функций $2n + 2$ поднята до $2\frac{1}{6} \cdot n$.

Очень близка к настоящей работе статья [3], в которой доказана оценка $\Theta(n^s)$для размера области определения универсальной функции для класса всех булевых полиномов степени не выше s.Следующее несложное утверждение оценивает число k −полилинейных функций и их пар.

Лемма 1. Количество k −полилинейных функций n переменных не превосходит $(k + 1)^n 2^k$. Количество упорядоченных пар k −полилинейных функций n переменных не превосходит $(k + 1)^{2n} 2^{2k}$.

Доказательство.

Любую k −полилинейную функцию n переменных можно задать вектором расположения n переменных по k скобкам (($k + 1$) - максимум

* Работа поддержана Российским научным фондом (номер гранта 16-11-10014).

вариантов для каждой переменной) и вектором свободных коэффициентов линейных функций в скобках.Второе утверждение леммы является тривиальным следствием первого. Лемма доказана.

Следующее утверждение доказывается почти дословно так же как лемма 3 из работы [3].

Лемма 2. Две различных k −полилинейных функции n переменных не совпадают минимум в 2^{n-k} точках.

Теорема. Для любого k, начиная с некоторого n, существует частичная универсальная функция для класса k −полилинейных функций n переменных с областью определения ограниченной величиной $O(n)$.

Доказательство.

Мы используем то же сведение и ту же технику, что и в работе [3]. Различие утверждений теорем настоящей статьи и работы [3] объясняется малостью величин из утверждения леммы 1 по сравнению с их аналогами из лемм 1 и 2 работы [3]. Задача построения универсальной функции эквивалентна задаче построения покрытия $(0-1)$-матрицы,строкам которой соответствуют всевозможные значения функции на всех наборах ($2 \cdot 2^n$ строк), столбцам −упорядоченные пары различных k −полилинейных функций n переменных (не более $((k+1)^{2n}2^{2k})$ пар). При таком сведении [3] по лемме 2 мы получим матрицу, у которой изначально в каждом столбце не менее2^{n-k} единиц. В отличие от классической задачи о покрытии в силу вышеуказанного дополнительного запрета вместе со строкой мы вынуждены удалять еще одну, соответствующую противоположному значению функции в данной точке. Поэтому после того, как мы взяли t строк, количество единиц в оставшихся столбцах будет не меньше, чем $2^{n-k}-t$.Пусть M_t − количество оставшихся столбцов после t шагов.Тогда число единиц в матрице после t шагов не меньше $(2^{n-k}-t)M_t$.Количество строк этой матрицы равно $2(2^n-t)$, поэтому в ней есть хотя бы одна строка с не менее чем

$$\frac{(2^{n-k}-t)M_t}{2(2^n-t)}$$

единицами. Таким образом,

$$M_{t+1} \leq M_t\left(1-\frac{2^{n-k}-t}{2(2^n-t)}\right) \tag{1}$$

Множитель $\left(1-\frac{2^{n-k}-t}{2(2^n-t)}\right)$ растет с ростомt. Таким образом, положив в неравенстве (1) значение $t=c(k)\cdot n$, где $c(k)$ −некоторая константа, не зависящая отn, получаем

$$M_{c(k)\cdot n} \leq (k+1)^{2n}2^{2k}\left(1-\frac{2^{n-k}-c(k)\cdot n+1}{2(2^n-c(k)\cdot n+1)}\right). \tag{2}$$

Если при этом выполнено неравенство

$$c(k) \cdot n = 2^{n-k-1}, \tag{1}$$

то из неравенства (2) следует, что

$$M_{c(k)\cdot n} \leq 4^k \left((k+1)^2 \cdot \left(1 - \frac{2^{n-k} - 2^{n-k-1} + 1}{2(2^n - 2^{n-k-1} + 1)}\right)^{c(k)} \right)^n.$$

Из последнего неравенства в силу того, что

$$\frac{2^{n-k} - 2^{n-k-1} + 1}{2^n - 2^{n-k-1} + 1} \geq \frac{1}{2^{k+1} - 1},$$

Получим

$$M_{c(k)\cdot n} \leq 4^k \left((k+1)^2 \cdot \left(1 - \tfrac{1}{2^{k+1}-1}\right)^{c(k)} \right)^n. \tag{2}$$

Выберем достаточно большую константу $c(k)$ так, чтобы выполнялось неравенство

$$(k+1)^2 \cdot \left(1 - \tfrac{1}{2^{k+1}-1}\right)^{c(k)} < 1. \tag{3}$$

Обозначим левую часть неравенства (5) через q. При

$$4^k q^n < 1 \tag{4}$$

из неравенства (4) следует, что величина $M_{c(k)\cdot n}$ равна нулю. Последнее достигается при произвольном n, большем чем $k \log_{\frac{1}{q}} 4$.При выполнении условий (3),(5),(6) имеем

$$M_{c(k)\cdot n} = 0.$$

Теорема доказана.

Литература

1. *Вороненко А.А.* Об универсальных частичных функциях для класса линейных // Дискретная математика. 2012. №3. С. 62−65. (Англ. пер.:Voronenko A.A. Discrete Mathematics and Applications, издательство V S P (Netherlands). 2012. Том 22, № 4, с. 421−425).
2. *Вороненко А.А., Вялый М.Н.* Нижняя оценка мощности области определения универсальных функций для класса линейных булевых функций// Дискретная математика. 2016. №4. С.50−57. (Англ. пер.:Voronenko A.A., Vyalyi M.N. Discrete Mathematics and Applications, издательство V S P (Netherlands). 2017. Том 27, № 5, с. 319−324)
3. *Вороненко А.А.* Универсальные функции для классов булевых полиномов // Вестник Моск. ун-та. Сер. 15. Вычисл. матем. и киберн. 2017. №3. С. 36−38. (Англ. пер.:VoronenkoA.A. Universal functions for classes of Boolean polynomials // Moscow University Computational Mathematics and Cybernetics. 2017. Том 41, № 3, с. 142−144).