А. А. Вороненко

О ПОРОЖДЕНИИ ОБРАЗОВ НЕСКОЛЬКИХ ЛИТЕРАЛОВ

Первой работой в серии, посвященной порождению образов дискретных функций при условии ложных предположений, является статья [1]. В ней рассматривалось предположение линейности функции. Последние результаты о порождении линейных функций изложены в работе [2]. Стоит отметить статью [3], в которой изучена ситуация ложного предположения монотонности. В настоящей статье рассматривается возможность одновременого порождения двух образов функций при разных ложных о них предположениях.

Рассмотрим следующую задачу. Пусть задано множество переменных $\{x_1, \ldots, x_n\}$. Требуется построить булеву функцию (возможно частичную) $f(x_1, \ldots, x_n)$, такую, что для любых его подмножеств X_1 и X_2, для любой пары переменных x_i, x_j, таких, что

$$x_i \in X_1, \quad x_i \notin X_2, \quad x_j \in X_2, \quad x_j \notin X_1,$$

а также для любых констант σ_i, σ_j можно предъявить значения функции $f(x_1, \ldots, x_n)$ на некоторых наборах таким образом, что единственной функцией, совпадающей на них с $f(x_1, \ldots, x_n)$ и существенно зависящей ровно от одной переменной из множества X_1, является $x_i^{\sigma_i}$, а из X_2 – $x_j^{\sigma_j}$. Такую функцию назовем универсальной для задачи порождения произвольной пары литералов, или, далее, просто, универсальной. Иными словами, требуется построить такую функцию, что для любой пары литералов можно предъявить такие наборы, что тот, кто считает фунцию зависящей ровно от одной переменной и исключает одну переменную из пары, должен сделать вывод о том, что функция равна литералу из пары, зависящему от второй переменной.

Основу решения данной задачи составляет следующее утверждение.

Лемма 1. *Пусть известно, что функция $g(x_1, \ldots, x_n)$ существенно зависит ровно от одной переменной. Пусть дополнительно известно, что переменная $x_j(x_i)$ фиктивна. Тогда если на некоторых двух наборах выполняются равенства*

$$f(\alpha_1, \ldots, \alpha_{i-1}, \overline{\sigma_i}, \alpha_{i+1}, \ldots, \alpha_{j-1}, \overline{\sigma_j}, \alpha_{j+1}, \ldots, \alpha_n) = 0, \qquad (1)$$

$$f(\alpha_1, \ldots, \alpha_{i-1}, \sigma_i, \alpha_{i+1}, \ldots, \alpha_{j-1}, \sigma_j, \alpha_{j+1}, \ldots, \alpha_n) = 1, \qquad (2)$$

то

$$g(x_1, \ldots, x_n) = x_i^{\sigma_i}(x_j^{\sigma_j}).$$

Доказательство. Из условий (1)–(2) следует, что одна из переменных $\{x_i, x_j\}$ является существенной. Из дополнительного условия фиктивности одной из переменных вытекает утверждение леммы.

Построим примеры универсальных функций. Во всех конструкциях будем считать n достаточно большим, чтобы не возникло противоречий.

Конструкция первая. Напомним, что весом двоичного набора называется количество единиц в нем. Положим $f(0, \ldots, 0) = f(1, \ldots, 1) = 0$, а на всех наборах веса 2 и $n-2$ положим $f = 1$. На наборах веса 3 положим функцию f равной единице тогда и только тогда, когда все единицы ее аргументов идут подряд по кругу. Положим функцию f равной нулю тогда и только тогда, когда ровно две единицы ее аргументов идут подряд по кругу. На остальных наборах функцию f оставим неопределенной.

Теорема 1.*При $n \geq 7$ задаваемая первой конструкцией функция $f(x_1, \ldots, x_n)$ универсальна.*

Доказательство. По лемме 1 предъявление значения $f(0, \ldots, 0) = 0$ и единицы на наборе веса два с единицами в i-й и j-й позиции доказывает равенство функции переменной x_i (x_j) в предположении фиктивности переменной x_j (x_i). По той же лемме предъявление значения $f(1, \ldots, 1) = 0$ и единицы на наборе веса $n-2$ с нулями в i-й и j-й позиции доказывает равенство функции отрицанию переменной x_i (x_j) в предположении фиктивности переменной x_j (x_i).

Если предъявить значения функции f на двух наборах: одном с единицами в позициях с номерами $i-2, i-1, i$, а другом с номерами $i-2, i-1, j$ (где для номеров позиций считается $1-1=n$), то мы докажем равенство функции переменной x_i или же отрицанию переменной x_j в предположении фиктивности переменной x_j (x_i). Последнее рассуждение справедливо для $j \notin \{i-3, i-2, i-1\}$. Если предъявить значения функции f на двух наборах: одном с единицами в позициях с номерами $i, i+1, i+2$, а другом с номерами $j, i+1, i+2$ (где для номеров позиций считается $n+1=1$), то мы докажем равенство функции переменной x_i или же отрицанию переменной x_j в предположении фиктивности переменной x_j (x_i). Последнее рассуждение справедливо для $j \notin \{i+1, i+2, i+1\}$. При

$n \geq 7$ множества позиций $\{i-3, i-2, i-1\}$ и $\{i+1, i+2, i+1\}$ при фиксированном i не пересекаются, что позволяет породить пару литералов $x_i, \overline{x}_j$ в одном из двух рассмотренных выше случаев. В силу произвольности i, j теорема доказана.

Замечание 1.*Область определения функции, строящейся по первой конструкции содержит* $2n^2 - 3n + 2$ *наборов.*

Конструкция вторая. Рассмотрим разбиение n-мерного вектора $\mathbf{x}$ на четыре части $\mathbf{a}, \mathbf{b}, \mathbf{c}, \mathbf{d}$. Сначала рассмотрим все шесть наборов, получаемых тождественным доопределением двух частей нулями, а двух других – единицами. После этого определим функцию f на шести сферах единичного радиуса (см. [4], с. 61) с центрами в этих наборах одинаковым образом для сдвигов одного центра по компонентам одного элемента разбиения согласно таблице:

Таблица 1.

Значения **abcd**	Значения на сфере	Формула
0011	1010	$(a \vee \overline{c})(\overline{b} \vee d)$
1100	1010	$(c \vee \overline{a})(\overline{d} \vee b)$
0101	1001	$(a \vee \overline{d})(\overline{c} \vee b)$
1010	1001	$(d \vee \overline{a})(\overline{b} \vee c)$
0110	1100	$(a \vee \overline{b})(\overline{d} \vee c)$
1001	1100	$(b \vee \overline{a})(\overline{c} \vee d)$

Замечание 2.*Формула в третьей колонке таблицы 1 показывает, функции одной переменной из каких частей разбиения можно породить по лемме 1, предъявив соответствующие наборы на сфере. Например, при помощи пары значений на первой сфере, полученных сдвигом в позициях из* $\mathbf{a}$ *и* $\mathbf{b}$*, можно породить произвольную пару – переменная из* $\mathbf{a}$ *и отрицание переменной из* $\mathbf{b}$*. Заметим, что все* 24 *возможные пары, соответствующие функциям одной переменной разных частей разбиения, порождаются.*

Теорема 2.*При* $n = 4^m$ *для* $m \geq 2$ *существует универсальная функция* n *переменных, заданная на* $6mn = 6n \log_4 n$ *наборах.*

Доказательство. Занумеруем позиции булева вектора длины n от нулевой до $n-1$-й. Построим в соответствии со второй конструкцией m шестерок сфер по правилу: в одну часть разбиения относятся позиции с одинаковой цифре в четверичном разряде номера. В силу замечания 2 построенная функция будет универсальной при отсутствии противоречий в определении значений в точках. Для последнего достаточно, чтобы расстояние между всеми центрами сфер

было не меньше трех. Центры сфер одной шестерки отличаются не менее чем в половине позиций. Если же центры относятся к разным шестеркам, то отличаются ровно в половине позиций.

Теорема 3. *Начиная с некоторого n, существуют универсальные функции n переменных с размером области определения $O(n \log n)$, и при $n \to \infty$.*

Доказательство. Рассмотрим общий случай $16 \leq 4^m < n < 4^{m+1}$. При той же нумерации построим те же шестерки сфер, не производя лишь построения, основанные на различии в старшем разряде. Так же, как и в теореме 2, порождаются все пары литералов, кроме тех, номера которых отличаются кратно 4^m. Положим $f(\mathbf{0}) = f(\mathbf{1}) = 0$. Положим равными единице значения функции f на всех наборах с ровно двумя единицами и на всех наборах ровно с двумя нулями, таких, что разность номеров этих компонент кратна 4^m. При помощи этих значений по лемме 1 порождаются все пары переменных и отрицаний переменных с разностью номеров, кратной 4^m. Далее положим равным единице значение функции f на наборах с ровно одной единицей (ровно одним нулем) в позиции с номером первого разряда 0 или 2 и нулю – с номером 1 или 3. При помощи значений на наборах веса 1 и $n-1$ порождаются все оставшиеся пары переменная – отрицание переменной за исключением пар с разностью $2 \cdot 4^m$. Для получения этих пар доопределим функцию f равной единице на наборе с первыми $2 \cdot 4^m - 2$ позициями, равными единице, а остальными равными нулю, и на противоположном наборе. После этого положим значения f равными нулю на всех наборах, получаемых из данных заменой единицы (нуля) на единицу в позиции на $2 \cdot 4^m$ большей. Если $n = 4^{m+1} - 1$, то при помощи еще четырех наборов породим недостающие пары для переменных и отрицаний с номерами $2 \cdot 4^m - 2$ и $4^{m+1} - 2$. Теперь порождаются и все возможные пары литералов с разностью номеров, кратной 4^m. Полученная функция универсальна, а добавленное к конструкции предыдущей теоремы множество точек ограничено по мощности линейной от n функцией.

В заключение рассмотрим ситуацию порождения образов нескольких переменных. Будем говорить, что булева функция $f(x_1, \ldots, x_n)$ порождает набор литералов $\{x_{i_1}^{\sigma_1}, \ldots, x_{i_k}^{\sigma_k}\}$, если можно предъявить такие наборы значений функции f, что из предположений существенной зависимости функции ровно от одной переменной и фиктивности переменных $\{x_{i_1}, \ldots, x_{i_{j-1}}, x_{i_{j+1}}, \ldots, x_{i_k}\}$ вытекает ее равенство литералу $x_{i_j}^{\sigma_j}$. Будем называть k-универсальной функцию

$f(x_1, \ldots, x_n)$, если она порождает любой набор из k литералов.

Лемма 2. *Пусть известно, что функция $g(x_1, \ldots, x_n)$ существенно зависит ровно от одной переменной. Пусть дополнительно известно, что переменные $\{x_{i_1}, \ldots, x_{i_{j-1}}, x_{i_{j+1}}, \ldots, x_{i_k}\}$ фиктивны. Тогда если на некоторых двух наборах выполняются равенства*

$$f(\alpha_1, \ldots, \alpha_{i_1-1}, \overline{\sigma_{i_1}}, \alpha_{i_1+1}, \ldots, \alpha_{i_k-1}, \overline{\sigma_{i_k}}, \alpha_{i_k+1}, \ldots, \alpha_n) = 0, \qquad (3)$$

$$f(\alpha_1, \ldots, \alpha_{i_1-1}, \sigma_{i_1}, \alpha_{i_1+1}, \ldots, \alpha_{i_k-1}, \sigma_{i_k}, \alpha_{i_k+1}, \ldots, \alpha_n) = 1, \qquad (4)$$

то

$$g(x_1, \ldots, x_n) = x_{i_j}^{\sigma_j}.$$

Доказательство. Из равенств (3)–(4) следует существенная зависимость функции $g(x_1, \ldots, x_n)$ от одной из переменных $x_{i_1}, \ldots, x_{i_k}$. Из существенной зависимости функции $g(x_1, \ldots, x_n)$ ровно от одной переменной, фиктивности переменных $x_{i_1}, \ldots, x_{i_{j-1}}, x_{i_{j+1}}, \ldots, x_{i_k}$ вытекает, что либо $g(x_1, \ldots, x_n) = x_{i_j}$, либо $g(x_1, \ldots, x_n) = \overline{x_{i_j}}$. Возможность монотонности (антимонотонности) функции $g(x_1, \ldots, x_n)$ по переменной x_{i_j} также следует из равенств (3)–(4).

Теорема 4. *Пусть*

$$k < n - \log_2 n + \log_2(\log_3 4 - 1). \qquad (5)$$

Тогда существует k-универсальная функция. Пусть при $n \to \infty$

$$n - \log_2 n - k \to \infty. \qquad (6)$$

Тогда почти все булевы функции n переменных являются k-универсальными.

Доказательство. Рассмотрим равномерное дискретное распределение на множестве всех булевых функций n переменных. Вероятность порождения (непорождения) соответствующего набора из k литералов на паре наборов из условия леммы 2 равна $\frac{1}{4}$ $(\frac{3}{4})$. В силу того, что оставшиеся $n - k$ компонент можно выбирать произвольно независимым образом, вероятность непорождения фиксированного набора из k литералов не превосходит

$$\left(\frac{3}{4}\right)^{2^{n-k}}.$$

Поэтому вероятность непорождения хотя бы одного набора из k литералов не превосходит

$$\left(\frac{3}{4}\right)^{2^{n-k}} \cdot 2^k \cdot \binom{n}{k} < \left(\frac{3}{4}\right)^{2^{n-k}} \cdot 3^n.$$

Троичный логарифм последней величины равен

$$(1 - \log_3 4) \cdot 2^{n-k} + n. \tag{7}$$

При выполнении неравенства (5) величина (7) отрицательна, из чего следует, что вероятность того, что случайная функция не универсальна, меньше единицы, и, следовательно, k-универсальная функция существует. Если же выполнено соотношение (6), то величина (7) стремится к минус бесконечности при $n \to \infty$, а вероятность того, что случайная функция не является k-универсальной, стремится к нулю.

Замечание 3. *Утверждение теоремы 1 вытекает из утверждения теоремы 4 при подстановке $k = 2$ в формулу (5). Однако теорема 4 не дает гарантированной верхней оценки на размер области определения универсальной функции.*

Литература

1. Вороненко А. А. Об универсальных частичных функциях для класса линейных функций // Дискретная математика. 2012. **24**. №3. С. 62–65.
2. Вороненко А. А. О порождении ложных образов линейных k-значных функций // Прикладная математика и информатика. №48. М: Макс Пресс. 2015. С. 85–92.
3. Вороненко А. А., Федорова В. С. О порождении булевых функций в предположении монотонности // Вестн. Моск. ун-та. Сер. 15. Вычисл. матем. и киберн. 2013. №1. С. 46–47.
4. Алексеев В. Б. Лекции по дискретной математике. Учебное пособие. М: Изд-во факультета ВМиК МГУ им. М.В.Ломоносова. 2004. 76 с.