А.А. Вороненко[1] [2], А.С. Окунева[3]

УНИВЕРСАЛЬНЫЕ ФУНКЦИИ ДЛЯ КЛАССОВ ЛИНЕЙНЫХ ФУНКЦИЙ ТРЕХ ПЕРЕМЕННЫХ*

Введение

Ранее в работе [1] было введено понятие универсальной функции и поставлена задача её существования и оценки мощности области определения. Задача построения универсальных функций, поставленная в [1] является оригинальной и значительно отличается от близких постановок. В ней изначально имеется "большая ложь" и далее требуется построить объект так, чтобы при помощи частичной правдивой информации можно было задать любое возможное решение единственным образом. Обзор результатов по универсальным функциям можно найти в [6]. Пусть задан некоторый класс функций K. Будем говорить, что функция f, зависящая от того же множества переменных, что и функции из класса K, *порождает функцию* g (при условии $g \in K$), если можно предъявить множество точек X такое, что $g(x)$ является единственной функцией, принадлежащей классу K, такой, что для любого x из множества X выполняется соотношение $f(x) = g(x)$. Функция f называется *универсальной* для класса K, если она порождает любую функцию из данного класса. Случай суммы двух переменных рассмотрен в работе [2]. Наиболее близким объектом к универсальным функциям для класса линейных являются бент-функции (см. например [4]). При этом бент-функция максимально удалена от всех линейных, а универсальная отличается от каждой в n+1 точке из желательно минимально возможного количества. Добавление возможно неверных ответов является классической постановкой и дает возможность долго исследовать близкие задачи. Так задача расшифровки монотонной функции была полностью решена Анселем [8] в 1966 году, а одна из постановок с неверными ответами рассматривалась в работе [5] совсем недавно. Наиболее популярные близкие постановки отражены в работе [7].

[1] Профессор факультета ВМК МГУ имени М.В. Ломоносова. e-mail: dm6@cs.msu.ru
[2] Ведущий научный сотрудник МФТИ
[3] Аспирант факультета ВМК МГУ имени М.В. Ломоносова e-mail: okuneva-anna@mail.ru
* Работа выполнена при поддержке Российского научного фонда
(номер гранта16-11-10014).

Основные результаты

Обозначим множество сумм троек различных переменных как $D = \{x_i \oplus x_j \oplus x_k\}$. Верна следующая теорема.

Теорема 1. Для множества D функций n переменных существует универсальная функция, определенная на $6]\log_2 n[$наборах.

Доказательства

Вспомогательная задача. Пусть загаданы три различных неизвестных элемента из множества мощности n. Мы можем брать любое подмножество исходного множества и задавать вопрос о четности числа загаданных элементов в этом подмножестве. При помощи серии подобных запросов можно найти загаданную тройку. При этом мы имеем право считать элементы множества элементами поля Галуа $GF(2^m)$, где $m = 6]\log_2 n[$ (см. напр. [3],гл.3). Дальнейшее рассмотрение не зависит от вида неприводимых многочленов, за исключением примера в конце текста.

Лемма1. Пусть $\{\mathbf{x}_1, \mathbf{x}_2, \mathbf{x}_3, \mathbf{a}, \mathbf{b}, \mathbf{c}\}$—элементы поля Галуа $GF(2^m)$ и $\mathbf{x}_1, \mathbf{x}_2, \mathbf{x}_3$ попарно различны. Если тройка $\mathbf{x}_1, \mathbf{x}_2, \mathbf{x}_3$ удовлетворяет системе

$$\begin{cases} \mathbf{x}_1 + \mathbf{x}_2 + \mathbf{x}_3 = \mathbf{a}, \\ \mathbf{x}_1^3 + \mathbf{x}_2^3 + \mathbf{x}_3^3 = \mathbf{b}, \\ \mathbf{x}_1^5 + \mathbf{x}_2^5 + \mathbf{x}_3^5 = \mathbf{c}, \end{cases} \quad (1)$$

то ей удовлетворяют только перестановки этих элементов.

Доказательство.

Преобразуем левые части уравнений системы следующим образом.

$$\begin{aligned} (\mathbf{x}_1 + \mathbf{x}_2 + \mathbf{x}_3)^3 &= \mathbf{x}_1^3 + \mathbf{x}_2^3 + \mathbf{x}_3^3 + \mathbf{x}_1^2\mathbf{x}_2 + \mathbf{x}_1\mathbf{x}_2^2 + \mathbf{x}_1\mathbf{x}_3^2 + \mathbf{x}_1^2\mathbf{x}_3 + \mathbf{x}_2^2\mathbf{x}_3 + \mathbf{x}_2\mathbf{x}_3^2 \\ &= \mathbf{b} + \mathbf{x}_1\mathbf{x}_2(\mathbf{x}_1 + \mathbf{x}_2) + \mathbf{x}_2\mathbf{x}_3(\mathbf{x}_2 + \mathbf{x}_3) + \mathbf{x}_1\mathbf{x}_3(\mathbf{x}_1 + \mathbf{x}_3) \\ &= \mathbf{b} + \mathbf{x}_1\mathbf{x}_2(\mathbf{a} + \mathbf{x}_3) + \mathbf{x}_2\mathbf{x}_3(\mathbf{a} + \mathbf{x}_1) + \mathbf{x}_1\mathbf{x}_3(\mathbf{a} + \mathbf{x}_2) \\ &= \mathbf{b} + \mathbf{a}(\mathbf{x}_1\mathbf{x}_2 + \mathbf{x}_2\mathbf{x}_3 + \mathbf{x}_1\mathbf{x}_3) + \mathbf{x}_1\mathbf{x}_2\mathbf{x}_3. \end{aligned}$$

$$\begin{aligned} (\mathbf{x}_1 + \mathbf{x}_2 + \mathbf{x}_3)^5 &= (\mathbf{x}_1 + \mathbf{x}_2 + \mathbf{x}_3)^2(\mathbf{x}_1 + \mathbf{x}_2 + \mathbf{x}_3)^3 \\ &= (\mathbf{x}_1^2 + \mathbf{x}_2^2 + \mathbf{x}_3^2)(\mathbf{x}_1 + \mathbf{x}_2 + \mathbf{x}_3)^3 \\ &= \mathbf{x}_1^5 + \mathbf{x}_2^5 + \mathbf{x}_3^5 + \mathbf{x}_1^4\mathbf{x}_2 + \mathbf{x}_1^4\mathbf{x}_3 + \mathbf{x}_1\mathbf{x}_2^4 + \mathbf{x}_2^4\mathbf{x}_3 + \mathbf{x}_1\mathbf{x}_3^4 + \mathbf{x}_2\mathbf{x}_3^4 \\ &= \mathbf{x}_1^5 + \mathbf{x}_2^5 + \mathbf{x}_3^5 + \mathbf{x}_1\mathbf{x}_2(\mathbf{x}_1^3 + \mathbf{x}_2^3) + \mathbf{x}_1\mathbf{x}_3(\mathbf{x}_1^3 + +\mathbf{x}_3^3) + \mathbf{x}_2\mathbf{x}_3(\mathbf{x}_2^3 \\ &+ \mathbf{x}_3^3) = \mathbf{c} + \mathbf{x}_1\mathbf{x}_2(\mathbf{b} + \mathbf{x}_3^3) + \mathbf{x}_1\mathbf{x}_3(\mathbf{b} + \mathbf{x}_2^3) + \mathbf{x}_2\mathbf{x}_3(\mathbf{b} + \mathbf{x}_1^3) \\ &= \mathbf{c} + \mathbf{b}(\mathbf{x}_1\mathbf{x}_2 + \mathbf{x}_2\mathbf{x}_3 + \mathbf{x}_1\mathbf{x}_3) + \mathbf{x}_1\mathbf{x}_2\mathbf{x}_3(\mathbf{x}_1^2 + \mathbf{x}_2^2 + \mathbf{x}_3^2) \\ &= \mathbf{c} + \mathbf{b}(\mathbf{x}_1\mathbf{x}_2 + \mathbf{x}_2\mathbf{x}_3 + \mathbf{x}_1\mathbf{x}_3) + \mathbf{a}^2\mathbf{x}_1\mathbf{x}_2\mathbf{x}_3. \end{aligned}$$

Получим систему

$$\begin{cases} \mathbf{x_1 + x_2 + x_3 = a}, \\ \mathbf{b + a(x_1x_2 + x_2x_3 + x_1x_3) + x_1x_2x_3 = a^3}, \\ \mathbf{c + b(x_1x_2 + x_2x_3 + x_1x_3) + a^2x_1x_2x_3 = a^5}. \end{cases} \quad (2)$$

Проведем замену переменных

$$\mathbf{(x_1x_2 + x_2x_3 + x_1x_3) = p},$$
$$\mathbf{x_1x_2x_3 = q},$$
$$\mathbf{(x_1 + x_2 + x_3) = s}.$$

Тогда система (2) преобразуется к виду

$$\begin{cases} \mathbf{s = a}, \\ \mathbf{b + ap + q = a^3}, \\ \mathbf{c + bp + a^2q = a^5}. \end{cases} \quad (3)$$

Возможны пять случаев.

1. $\mathbf{a = 0, b \neq 0}$

$$\begin{cases} \mathbf{s = 0}, \\ \mathbf{b + q = 0}, \\ \mathbf{c + bp = 0}. \end{cases} \Rightarrow \begin{cases} \mathbf{s = 0}, \\ \mathbf{q = b}, \\ \mathbf{p = cb^{-1}}. \end{cases}$$

2. $\mathbf{a \neq 0, b = 0}$

$$\begin{cases} \mathbf{s = a}, \\ \mathbf{ap + q = a^3}, \\ \mathbf{c + a^2q = a^5}. \end{cases} \Rightarrow \begin{cases} \mathbf{s = a}, \\ \mathbf{ap + a^3 + ca^{-2} = a^3}, \\ \mathbf{q = a^3 + ca^{-2}}. \end{cases} \Rightarrow \begin{cases} \mathbf{s = a}, \\ \mathbf{p = ca^{-3}}, \\ \mathbf{q = a^3 + ca^{-2}}. \end{cases}$$

3. $\mathbf{a = 0, b = 0}$

$$\begin{cases} \mathbf{s = 0}, \\ \mathbf{q = 0}, \\ \mathbf{c = 0}. \end{cases}$$

Временно вернемся к первоначальным обозначениям и перепишем в них первое и второе уравнения последней системы. Получим

$$\begin{cases} \mathbf{x_1 + x_2 + x_3 = 0}, \\ \mathbf{x_1x_2x_3 = 0}. \end{cases}$$

Откуда следует, что один из элементов равен $\mathbf{0}$, а два других равны между собой. Последнее противоречит условию леммы.

4. $\mathbf{a \neq 0, b \neq 0, a^3 \neq b}$

$$\begin{cases} \mathbf{s = a}, \\ \mathbf{b + ap + q = a^3}, \\ \mathbf{c + bp + a^2q = a^5}. \end{cases} \Rightarrow \begin{cases} \mathbf{s = a}, \\ \mathbf{q = a^3 + b + ap}, \\ \mathbf{c + bp + a^2(a^3 + b + ap) = a^5}. \end{cases} \Rightarrow$$

$$\Rightarrow \begin{cases} \mathbf{s = a}, \\ \mathbf{q = a^3 + b + a}\boldsymbol{p}, \\ \mathbf{p = (a^2b + c)(a^3 + b)^{-1}}. \end{cases}$$

5. $\mathbf{a \neq 0, b \neq 0, a^3 = b}$

Второе уравнение системы (3) $\mathbf{b + ap + q = a^3}$ с учетом равенств $\mathbf{a^3 = b}$ преобразуется в $\mathbf{ap = q}$, что в первоначальных обозначениях имеет вид $\mathbf{(x_1 + x_2 + x_3)(x_1x_2 + x_2x_3 + x_1x_3) = x_1x_2x_3}$, откуда следует

$$\mathbf{x}_1^2\mathbf{x}_2 + \mathbf{x}_1\mathbf{x}_2^2 + \mathbf{x}_1^2\mathbf{x}_3 + \mathbf{x}_1\mathbf{x}_3^2 + \mathbf{x}_2^2\mathbf{x}_3 + \mathbf{x}_3\mathbf{x}_2^2 = \mathbf{0}.$$

Проведем следующую замену $\mathbf{x}_2 = \mathbf{x}_1 + \mathbf{x}, \mathbf{x}_3 = \mathbf{x}_1 + \mathbf{y}$, где $\mathbf{x}, \mathbf{y}$ – элементы поля Галуа $GF(2^m)$ и подставим в равенство $\mathbf{a}^3 = \mathbf{b}$. Получим

$$\mathbf{x}^2\mathbf{y} + \mathbf{y}^2\mathbf{x} = \mathbf{0},$$
$$\mathbf{xy}(\mathbf{x} + \mathbf{y}) = \mathbf{0}.$$

Последнее означает, что либо $\mathbf{x}_1 = \mathbf{x}_2$, либо $\mathbf{x}_1 = \mathbf{x}_3$, либо $\mathbf{x}_2 = \mathbf{x}_3$ противоречит условиям леммы. Следовательно, соотношение $\mathbf{a}^3 = \mathbf{b}$ никогда не выполняется.

ч.т.д

Если представить элементы поля Галуа $GF(2^m)$ в виде m-мерных характеристических векторов многочленов, то система (1) примет вид:

$$\begin{cases} (\mathbf{x}_1 + \mathbf{x}_2 + \mathbf{x}_3)_0 = a_0, \\ \dots \\ (\mathbf{x}_1 + \mathbf{x}_2 + \mathbf{x}_3)_{m-1} = a_{m-1}, \\ (\mathbf{x}_1^3 + \mathbf{x}_2^3 + \mathbf{x}_3^3)_0 = b_0, \\ \dots \\ (\mathbf{x}_1^3 + \mathbf{x}_2^3 + \mathbf{x}_3^3)_{m-1} = b_{m-1}, \\ (\mathbf{x}_1^5 + \mathbf{x}_2^5 + \mathbf{x}_3^5)_0 = c_0, \\ \dots \\ (\mathbf{x}_1^5 + \mathbf{x}_2^5 + \mathbf{x}_3^5)_{m-1} = c_{m-1}, \end{cases} \quad (4)$$

и будет содержать $3m$ уравнений.

Доказательство. Теорема 1.

Системе (4) соответствует набор из $3m$ пар взаимоисключающих равенств.

$$\begin{gathered} (\mathbf{x}_1 + \mathbf{x}_2 + \mathbf{x}_3)_0 = 0, \\ (\mathbf{x}_1 + \mathbf{x}_2 + \mathbf{x}_3)_0 = 1, \\ \dots \\ (\mathbf{x}_1 + \mathbf{x}_2 + \mathbf{x}_3)_{m-1} = 0, \\ (\mathbf{x}_1 + \mathbf{x}_2\mathbf{x}_3)_{m-1} = 1 \\ (\mathbf{x}_1 + \mathbf{x}_2 + \mathbf{x}_3)_{m-1} = 1, \\ (\mathbf{x}_1^3 + \mathbf{x}_2^3 + \mathbf{x}_3^3)_0 = 0, \\ (\mathbf{x}_1^3 + \mathbf{x}_2^3 + \mathbf{x}_3^3)_0 = 1, \\ (\mathbf{x}_1^3 + \mathbf{x}_2^3 + \mathbf{x}_3^3)_0 = 1, \\ \dots \\ (\mathbf{x}_1^3 + \mathbf{x}_2^3 + \mathbf{x}_3^3)_{m-1} = 0, \\ (\mathbf{x}_1^3 + \mathbf{x}_2^3 + \mathbf{x}_3^3)_{m-1} = 1, \\ (\mathbf{x}_1^5 + \mathbf{x}_2^5 + \mathbf{x}_3^5)_0 = 0, \\ (\mathbf{x}_1^5 + \mathbf{x}_2^5 + \mathbf{x}_3^5)_0 = 1, \\ \dots \\ (\mathbf{x}_1^5 + \mathbf{x}_2^5 + \mathbf{x}_3^5)_{m-1} = 0, \\ (\mathbf{x}_1^5 + \mathbf{x}_2^5 + \mathbf{x}_3^5)_{m-1} = 1. \end{gathered} \quad (5)$$

Построим функцию f— частичную универсальную для класса D, определенную на $6]\log_2 n[$ наборах. Определим вектор $\mathbf{t}(m,k,i)$, где m – размерность, $k \in \{1,3,5\}$– степень, $i \in \{0,\dots,m-1\}$– номер бита. $\mathbf{t}(m,k,i)$– 2^m-мерный вектор, который содержит единицы в тех и только тех позициях, k-я степень номеров которых (нумерация ведется с нуля), как элементов в поле Галуа $GF(2^m)$, имеет в i-й позиции 1.

При $2^m > n$ добавим к переменным функции f фиктивные так, чтобы общее их количество равнялось 2^m. Поставим в соответствие каждому

равенству из (4) вида $(\mathbf{x}_1 + \mathbf{x}_2 + \mathbf{x}_3)_i = 0$ равенство $f(\mathbf{t}(m,1,i)) = 0$;
равенству вида $(\mathbf{x}_1 + \mathbf{x}_2 + \mathbf{x}_3)_i = 1$ – равенство $f(\bar{\mathbf{t}}(m,1,i)) = 1$;
равенству вида $(\mathbf{x}_1^3 + \mathbf{x}_2^3 + \mathbf{x}_3^3)_i = 0$ – равенство $f(\mathbf{t}(m,3,i)) = 0$;
равенству вида $(\mathbf{x}_1^3 + \mathbf{x}_2^3 + \mathbf{x}_3^3)_i = 1$ – равенство $f(\bar{\mathbf{t}}(m,3,i)) = 1$;
равенству вида $(\mathbf{x}_1^5 + \mathbf{x}_2^5 + \mathbf{x}_3^5)_i = 0$ – равенство $f(\mathbf{t}(m,5,i)) = 0$;
равенству вида $(\mathbf{x}_1^5 + \mathbf{x}_2^5 + \mathbf{x}_3^5)_i = 1$ – равенство $f(\bar{\mathbf{t}}(m,5,i)) = 1$.

Получим задание универсальной функции:

$$\begin{gathered}
f\big(\mathbf{t}(m,1,0)\big) = 0,\\
f\big(\bar{\mathbf{t}}(m,1,0)\big) = 1,\\
\dots\\
f\big(\mathbf{t}(m,1,m-1)\big) = 0,\\
f(\bar{\mathbf{t}}(m,1,m-1)) = 1,\\
f\big(\mathbf{t}(m,3,0)\big) = 0,\\
f(\bar{\mathbf{t}}(m,3,0)) = 1,\\
\dots\\
f\big(\mathbf{t}(m,3,m-1)\big) = 0,\\
f\big(\bar{\mathbf{t}}(m,3,m-1)\big) = 1\\
f\big(\mathbf{t}(m,5,0)\big) = 0,\\
f(\bar{\mathbf{t}}(m,5,0)) = 1,\\
\dots\\
f(\mathbf{t}(m,5,m-1)) = 0,\\
f(\bar{\mathbf{t}}(m,5,m-1)) = 1.
\end{gathered} \tag{6}$$

Противоречие в соотношениях (6) может возникнуть если $\mathbf{t}(m,k,i) \equiv \bar{\mathbf{t}}(m,l,j)$ при $i \neq j$ либо $k \neq l$. Данная ситуация невозможна, так как $\mathbf{0} = \mathbf{0}^3 = \mathbf{0}^5$, следовательно $\bar{\mathbf{t}}(m,k,i)_0 = 1$, а $\mathbf{t}(m,l,j)_0 = 0$.

Выбрав ровно одно условие из каждой пары взаимоисключающих для линейной функции условий системы (6), мы перейдем к системе (4) и найдем номера трех существенных переменных функции по лемме 1. Тем самым доказана универсальность f и теорема 1.

ч.т.д.

Пример

Частичная булева функция f, заданная ниже, является универсальной для множества D функций восьми переменных. Здесь в качестве неприводимого многочлена для операции умножения в поле Галуа $GF(8)$ выбран многочлен $x^3 + x + 1$.

$$f(01010101) = 1, f(10101010) = 0,$$
$$f(11001100) = 1, f(00110011) = 0,$$
$$f(11110000) = 1, f(00001111) = 0,$$

$$f(01101010) = 0, f(10010101) = 1,$$
$$f(00100111) = 0, f(11011000) = 1,$$
$$f(00011110) = 0, f(11100001) = 1,$$

$$f(00111001) = 0, f(00111001) = 1,$$
$$f(01101010) = 0, f(10010101) = 1,$$
$$f(00100111) = 0, f(00100111) = 1.$$

Список литературы

1. Вороненко А.А.,“Об универсальных частичных функциях для класса линейных функций”,*Дискретная математика*,24:3(2012),62–65.
2. Вороненко А.А, Окунева А.С., “Универсальные функции для классов линейных функций двух переменных”, *Дискретная математика*, 32:1 (2020), 3–7.
3. Журавлев Ю.И., Флеров Ю.А., Вялый М.Н., *Дискретный анализ. Основы высшей алгебры,* МЗ Пресс, Москва, 2007, 224с.
4. Токарева Н. Н. Нелинейные булевы функции: бент-функции и их обобщения //Saarbrucken: LAP LAMBERT AcademicPublishing. – 2011. – Т. 180.
5. С. Н. Селезнева, Ю. Лю, “Расшифровка монотонных функций с исправлением одной ошибки”, *Дискретная математика*, **31**:4 (2019), 53–69.
6. Voronenko A. A., Voronova N. K., Il'yutko V. P.“Existence of universal functions for the class of linear k-valued functions with moderate k”// *Computational Mathematics and Modeling. — 2017. — Vol. 28, no. 1. — P. 78–85.* [Вороненко А. А., Воронова Н. К., Ильютко В. П. “О существовании универсальных функций для класса линейных k-значных функций при небольших k” // *Прикладная математика и информатика.* — Т. 51. — МАКС Пресс Москва, 2016. — С. 100–108.]

7. Ben-Or M., Goldwasser S., Wigderson A. Completeness theorems for non-cryptographic fault-tolerant distributed computation //*Providing Sound Foundations for Cryptography: On the Work of Shafi Goldwasser and Silvio Micali*. – 2019. – С. 351-371.
8. Hansel G., “Sur le nombre des fonctions booleennes monotones de n variables”, *C. R. Acad. Sci. Paris*, 262 (1966), 1088–1090; пер. с англ.: [Ансель Ж., “О числе монотонных функций n переменных”, *Кибернетический сборник. Новая серия.*, М.: Мир, 1968, 53–57.]