

О единственности решения одной системы полиномиальных уравнений над конечным полем

И.С. Фаерштейн¹

Рассматривается система полиномиальных уравнений специального вида над полем $GF(2^m)$ и исследуется единственность её решения с точностью до перестановки переменных.

Ключевые слова: система полиномиальных уравнений, конечные поля, единственность решения.

1. Введение

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 существует такое множество точек X , что $g(x)$ является единственной функцией, принадлежащей классу K и удовлетворяющей соотношению $f(x) = g(x)$ для любого x из множества X . Функция f называется универсальной для класса K , если она порождает любую функцию из данного класса [1].

При решении задачи о построении универсальной функции класса линейных функций, существенно зависящих от фиксированного числа переменных, была поставлена вспомогательная задача исследования систем полиномиальных уравнений определенного вида над полем $GF(2^m)$ на единственность имеющегося решения, состоящего из разных элементов, с точностью до перестановки переменных [2, 3]. Данные системы уравнений представляют собой равенства параметрам сумм нечетных степеней переменных.

Для систем уравнений вида

$$\begin{cases} x_1 + x_2 = a, \\ x_1^3 + x_2^3 = b. \end{cases}$$

¹Фаерштейн Игорь Семенович — аспирант кафедры математической кибернетики факультета ВМК МГУ, e-mail: isfaer@rambler.ru.

Faershtein Igor Semenovich — postgraduate student, Lomonosov Moscow State University, Faculty of Computer Science, Chair of Mathematical Cybernetics.

и

$$\begin{cases} x_1 + x_2 + x_3 + x_4 = a, \\ x_1^3 + x_2^3 + x_3^3 + x_4^3 = b, \\ x_1^5 + x_2^5 + x_3^5 + x_4^5 = c, \\ x_1^7 + x_2^7 + x_3^7 + x_4^7 = d, \end{cases}$$

где $a, b, c \in GF(2^m)$ – константы, $x_1, x_2, x_3 \in GF(2^m)$, $x_i \neq x_j$ при $i \neq j$ – попарно различные переменные.

2. Основные результаты

Рассмотрим систему уравнений над полем Галуа $GF(2^m)$:

$$\begin{cases} x_1 + x_2 + x_3 + x_4 = a, \\ x_1^3 + x_2^3 + x_3^3 + x_4^3 = b, \\ x_1^5 + x_2^5 + x_3^5 + x_4^5 = c, \\ x_1^7 + x_2^7 + x_3^7 + x_4^7 = d, \end{cases} \quad (1)$$

где $a, b, c, d \in GF(2^m)$ – константы, $x_1, x_2, x_3, x_4 \in GF(2^m)$ – переменные.

Решение (x'_1, x'_2, x'_3, x'_4) системы (1) назовём невырожденным, если оно не содержит равных элементов. Решения системы (1), получающиеся друг из друга перестановкой переменных, называются эквивалентными. Будем говорить, что в системе (1) имеется коллизия, если в неё есть два неэквивалентных невырожденных решения. Невырожденное решение называется нулевым (единичным), если оно содержит нулевой (единичный) элемент.

В системе (1) коллизия невозможна.

Доказательство. Выразим уравнения системы (1) через элементарные симметрические многочлены и будем пытаться выразить элементарные симметрические многочлены через правые части системы (1). Рассмотрим уравнение

$$x^4 + s_1x^3 + s_2x^2 + s_3x + s_4 = 0, \quad (2)$$

где элементарные симметрические многочлены s_1, s_2, s_3, s_4 выражены через правые части системы (1). По обратной обобщённой теореме Виета [4] корнями уравнения (2) являются переменные x_1, x_2, x_3, x_4 системы (1). Поскольку уравнение степени 4 может иметь в поле не более 4 корней [5], то система (1) не может иметь невырожденные решения и, как следствие, не может иметь коллизии.

После выражения уравнений системы (1) через элементарные симметрические многочлены получим следующую систему уравнений:

$$\begin{cases} s_1 = a, \\ s_1^3 + s_1 s_2 + s_3 = b, \\ s_1^5 + s_1^3 s_2 + s_1 s_2^2 + s_1^2 s_3 + s_2 s_3 + s_1 s_4 = c, \\ s_1^7 + s_1^5 s_2 + s_1 s_2^3 + s_1^4 s_3 + s_1^2 s_2 s_3 + s_2^2 s_3 + s_1 s_3^2 + s_1^3 s_4 + s_3 s_4 = d, \end{cases} \quad (3)$$

где

$$\begin{aligned} s_1 &= x_1 + x_2 + x_3 + x_4, \quad s_2 = x_1 x_2 + x_1 x_3 + x_1 x_4 + x_2 x_3 + x_2 x_4 + x_3 x_4, \\ s_3 &= x_1 x_2 x_3 + x_1 x_2 x_4 + x_1 x_3 x_4 + x_2 x_3 x_4, \quad s_4 = x_1 x_2 x_3 x_4. \end{aligned}$$

Лемма 1. Пусть $a = 0, b \neq 0$. Тогда в системе (1) коллизия невозможна.

Доказательство. Пусть $a = 0$. Тогда система уравнений (3) принимает вид:

$$\begin{cases} s_1 = 0, \\ s_1^3 + s_1 s_2 + s_3 = b, \\ s_1^5 + s_1^3 s_2 + s_1 s_2^2 + s_1^2 s_3 + s_2 s_3 + s_1 s_4 = c, \\ s_1^7 + s_1^5 s_2 + s_1 s_2^3 + s_1^4 s_3 + s_1^2 s_2 s_3 + s_2^2 s_3 + s_1 s_3^2 + s_1^3 s_4 + s_3 s_4 = d. \end{cases}$$

Подставим всюду $s_1 = 0$ и получим:

$$\begin{cases} s_3 = b, \\ s_2 s_3 = c, \\ s_2^2 s_3 + s_3 s_4 = d. \end{cases}$$

Откуда с учетом условия $b \neq 0$ имеем:

$$\begin{cases} b s_2 = c, \\ b s_2^2 + b s_4 = d. \end{cases}$$

$$\begin{cases} s_2 = b^{-1} c, \\ s_4 = b^{-2} c^2 + b^{-1} d. \end{cases}$$

$$\begin{cases} s_1 = 0, \\ s_2 = b^{-1} c, \\ s_3 = b, \\ s_4 = b^{-2} c^2 + b^{-1} d. \end{cases}$$

Элементарные симметрические многочлены однозначно выражаются через правые части системы уравнений, что означает невозможность неэквивалентных решений и, как следствие, невозможность коллизии. \square

Лемма 2. Пусть $a = 0, b = 0$. Тогда в системе (1) коллизия невозможна.

Доказательство. Пусть $a = 0, b = 0$. Тогда система уравнений (3) примет вид:

$$\begin{cases} a = b = c = d = 0, \\ s_1 = 0, \\ s_3 = 0, \\ x_1 + x_2 + x_3 + x_4 = 0, \\ x_1x_2x_3 + x_1x_2x_4 + x_1x_3x_4 + x_2x_3x_4 = 0. \end{cases}$$

$$\begin{cases} s_1 = 0, \\ s_1^3 + s_1s_2 + s_3 = 0, \\ s_1^5 + s_1^3s_2 + s_1s_2^2 + s_1^2s_3 + s_2s_3 + s_1s_4 = c, \\ s_1^7 + s_1^5s_2 + s_1s_2^3 + s_1^4s_3 + s_1^2s_2s_3 + s_2^2s_3 + s_1s_3^2 + s_1^3s_4 + s_3s_4 = d. \end{cases}$$

Подставим всюду $s_1 = 0$ и получим:

$$\begin{cases} s_3 = 0, \\ s_2s_3 = c, \\ s_2^2s_3 + s_3s_4 = d. \end{cases}$$

Подставим всюду $s_3 = 0$ и получим:

$$\begin{cases} c = 0, \\ d = c, \end{cases}$$

Таким образом, в этом случае всегда

$$\begin{cases} a = b = c = d = 0, \\ s_1 = 0, \\ s_3 = 0, \\ x_1 + x_2 + x_3 + x_4 = 0, \\ x_1x_2x_3 + x_1x_2x_4 + x_1x_3x_4 + x_2x_3x_4 = 0. \end{cases}$$

Выразим s_1 и s_3 через исходные переменные системы. Имеем

$$\begin{cases} x_1 + x_2 + x_3 + x_4 = 0, \\ x_1x_2x_3 + x_1x_2x_4 + x_1x_3x_4 + x_2x_3x_4 = 0. \end{cases}$$

Пусть $x_1 = \alpha, x_2 = \beta, \alpha \neq \beta$. (Иначе получается вырожденное решение). Тогда

$$\begin{cases} \alpha + \beta + x_3 + x_4 = 0, \\ \alpha\beta x_3 + \alpha\beta x_4 + \alpha x_3x_4 + \beta x_3x_4 = 0. \end{cases} \quad (4)$$

Выразим $x_3 + x_4$. $x_3 + x_4 = \alpha + \beta$ и подставим во второе уравнение системы (4). Получим $\alpha\beta(\alpha + \beta) + (\alpha + \beta)x_3x_4 = 0$. Так как $\alpha \neq \beta$, то $\alpha + \beta \neq 0$. Тогда $x_3x_4 = \alpha\beta$. Имеем:

$$\begin{cases} x_3 + x_4 = \alpha + \beta, \\ x_3x_4 = \alpha\beta. \end{cases}$$

Переменные x_3 и x_4 однозначно выражаются через свои сумму и произведение, то есть

$$\begin{cases} x_3 = \alpha, \\ x_4 = \beta. \end{cases}$$

или

$$\begin{cases} x_3 = \beta, \\ x_4 = \alpha. \end{cases}$$

То есть система (1) может иметь только вырожденные решения, а поэтому не может иметь коллизий. \square

Лемма 3. Пусть $a^5 + a^2b + a^{-1}b^2 + c \neq 0$. Тогда в системе (1) коллизия невозможна.

Доказательство. Так как выражение $a^5 + a^2b + a^{-1}b^2 + c$ имеет смысл, то $a \neq 0$. Подставим значение $s_1 = a$ в остальные уравнения системы (3) и получим систему уравнений:

$$\begin{cases} a^3 + as_2 + s_3 = b, \\ a^5 + a^3s_2 + as_2^2 + a^2s_3 + s_2s_3 + as_4 = c, \\ a^7 + a^5s_2 + as_2^3 + a^4s_3 + a^2s_2s_3 + s_2^2s_3 + as_2^2 + a^3s_4 + s_3s_4 = d. \end{cases} \quad (5)$$

Выразим s_3 . $s_3 = a^3 + as_2 + b$ и подставим в остальные уравнения системы (5). Получим систему уравнений:

$$\begin{cases} a^2b + a^3s_2 + bs_2 + as_4 = c, \\ a^4b + a^5s_2 + a^2bs_2 + bs_2^2 + a^7 + a^3s_2^2 + ab^2 + as_2s_4 + bs_4 = d. \end{cases} \quad (6)$$

Так как $a \neq 0$, выразим s_4 . $s_4 = ab + a^2s_2 + a^{-1}bs_2 + a^{-1}c$. Подставим значение s_4 в оставшееся уравнение системы (6) и получим

$$s_2(a^5 + a^2b + a^{-1}b^2 + c) = d + a^4b + a^7 + a^{-1}bc.$$

Так как $a^5 + a^2b + a^{-1}b^2 + c \neq 0$, то

$$s_2 = (a^5 + a^2b + a^{-1}b^2 + c)^{-1}(d + a^4b + a^7 + a^{-1}bc).$$

Тогда

$$\begin{cases} s_3 = a^3 + a(a^5 + a^2b + a^{-1}b^2 + c)^{-1}(d + a^4b + a^7 + a^{-1}bc) + b, \\ s_4 = ab + (a^2 + a^{-1}b)(a^5 + a^2b + a^{-1}b^2 + c)^{-1}(d + a^4b + a^7 + a^{-1}bc) + a^{-1}c. \end{cases}$$

Таким образом,

$$\begin{cases} s_1 = a, \\ s_2 = (a^5 + a^2b + a^{-1}b^2 + c)^{-1}(d + a^4b + a^7 + a^{-1}bc), \\ s_3 = a^3 + a(a^5 + a^2b + a^{-1}b^2 + c)^{-1}(d + a^4b + a^7 + a^{-1}bc) + b, \\ s_4 = ab + (a^2 + a^{-1}b)(a^5 + a^2b + a^{-1}b^2 + c)^{-1}(d + a^4b + a^7 + a^{-1}bc) + a^{-1}c. \end{cases}$$

Элементарные симметрические многочлены однозначно выражаются через правые части системы уравнений, что означает невозможность неэквивалентных решений и, как следствие, невозможность коллизии. \square

Лемма 4. Пусть для правых частей системы (1) выполнены соотношения $a \neq 0$ и

$$a^6 + a^3b + b^2 + ac = 0. \quad (7)$$

Тогда в системе (1) коллизия невозможна.

Доказательство. Сделаем в условии (7) замены на левые части системы (1). После приведения подобных членов получим условие

$$\sum_{i \neq j, i \neq k, j \neq k} x_i^3 x_j^2 x_k = 0. \quad (8)$$

Пусть невырожденное решение является нулевым. Тогда в равенстве (8) останется шесть слагаемых из двадцати четырех. Пусть $x_4 = 0$. Вынесем в (8) произведение $x_1 x_2 x_3$ и сократим на него. Имеем

$$\sum_{i \neq j} x_i^2 x_j = 0. \quad (9)$$

Сделав в (9) замену $x_1 = x, x_2 = xp, x_3 = xq$, и сократив на x^3 , получим

$$p(1+p) + q(1+q) + pq(p+q) = 0$$

или

$$(p+q)(p+1)(q+1) = 0.$$

Последнее противоречит невырожденности решения.

Заметим, что если неэквивалентные решения (x'_1, x'_2, x'_3, x'_4) и $(x''_1, x''_2, x''_3, x''_4)$ являются невырожденными, то при $\mu \neq 0$ наборы $(x'_1\mu, x'_2\mu, x'_3\mu, x'_4\mu)$ и $(x''_1\mu, x''_2\mu, x''_3\mu, x''_4\mu)$ являются решениями системы

$$\begin{cases} x_1 + x_2 + x_3 + x_4 = a\mu, \\ x_1^3 + x_2^3 + x_3^3 + x_4^3 = b\mu^3, \\ x_1^5 + x_2^5 + x_3^5 + x_4^5 = c\mu^5, \\ x_1^7 + x_2^7 + x_3^7 + x_4^7 = d\mu^7, \end{cases}$$

Положив при этом $\mu = (x'_4)^{-1}$, получим, что из наличия невырожденной коллизии в системе (1) следует наличие невырожденной единичной коллизии для некоторой системы, полученной из (1) изменением правых частей уравнений.

Докажем невозможность выполнения условия (7) в системе (1) при наличии единичного решения. Пусть $x_4 = 1$. Сделаем в (8) замену

$$x_1 = z, x_2 = zp, x_3 = zq. \quad (10)$$

При делении на z^3 условие (8) принимает вид

$$\begin{aligned} z^3(p^3q^2 + p^2q^3 + p^3q + pq^3 + p^2q + pq^2) + z^2(p^3q^2 + p^2q^3 + p^3 + q^3 + p^2 + q^2) + \\ + z(p^3q + pq^3 + p^3 + q^3 + p + q) + (p^2q + pq^2 + p^2 + q^2 + p + q) = 0. \end{aligned}$$

Разделив левую часть последнего равенства на $(p+q)(p+1)(q+1)$, получим

$$z^3pq + z^2(pq + p + q) + z(p + q + 1) + 1 = 0.$$

Сделав в последнем условии замену, обратную (10), и сгруппировав слагаемые, получим

$$(x_1 + 1)(x_2 + 1)(x_3 + 1) = 0.$$

Последнее соотношение противоречит предположению невырожденности единичного решения при $x_4 = 1$. Лемма доказана. \square

Таким образом, во всех случаях коллизия невозможна, что доказывает теорему. \square

Автор выражает благодарность профессору Вороненко А.А. за постановку задачи.

Список литературы

- [1] Вороненко А.А. Об универсальных частичных функциях для класса линейных функций. // Дискретная математика. Т. 24. Вып. 3. 2012. С. 62–65.
- [2] Вороненко А.А., Окунева А.С. Универсальные функции для классов линейных функций двух переменных. // Дискретная математика. Т. 32. Вып. 1. 2020. С. 3–7.
- [3] Вороненко А.А., Окунева А.С. Универсальные функции для классов линейных функций трех переменных. // Прикладная математика и информатика. – Т. 51. – М.: Макс Пресс, 2020. С. 114–121.
- [4] Винберг Э.Б. Алгебра многочленов. Учебное пособие для студентов-заочников III-IV курсов физико-математических факультетов педагогических институтов. – М.: Просвещение, 1980. 176 с.
- [5] Винберг Э.Б. Курс алгебры. 2-е изд., стереотип. – М.: МЦНМО, 2013. 590 с.

On the uniqueness of the solution of a system of polynomial equations over a finite field

Faershtein I.S.

A system of polynomial equations of a special form over the field $GF(2^m)$ is considered and the uniqueness of its solution up to a permutation of variables is investigated.

Keywords: system of polynomial equations, finite fields, uniqueness of solution.

References

- [1] Voronenko A.A. On universal partial functions for a class of linear functions. // Discrete Mathematics. Vol. 24. Issue. 3. 2012. P. 62–65. (In Russian).
- [2] Voronenko A.A., Okuneva A.S. Universal functions for classes of linear functions of two variables. // Discrete Mathematics. Vol. 32. Issue. 1. 2020. P. 3–7. (In Russian).
- [3] Voronenko A.A., Okuneva A.S. Universal functions for classes of linear functions of three variables. // Applied Mathematics and Computer Science. – Vol. 51. – Moscow: Max Press, 2020. P. 114–121. (In Russian).

- [4] Vinberg E.B. Algebra of polynomials. Textbook for part-time students of the III-IV courses of physics and mathematics faculties of pedagogical institutes. – Moscow Prosveshchenie, 1980. 176 p. (In Russian).
- [5] Vinberg E.B. Course of algebra. 2nd ed., stereotype. – Moscow: MCCME, 2013. 590 p. (In Russian).