Математика и математическое моделирование.
2022. № 1. С. 31–52.
DOI: 10.24108/mathm.0122.0000262

Математика и Математическое моделирование
Сетевое научное издание
http://mathmelpub.ru ISSN 2412-5911

УДК 004.056

О классификации n-разделимых функций многих переменных над конечными полями и одной задаче олимпиады NSUCrypto'2019

Чиликов А. А.[1,2,*]

[1]МГТУ им. Н.Э. Баумана, Москва, Россия
[2]МФТИ, Долгопрудный, Московская область, Россия
[*]chilikov@passware.com

В настоящей статье исследуются неполные разделения булевых отображений и отображений над конечными полями. Техника разделений функций и отображений является эффективным инструментом для создания реализаций криптографических алгоритмов, защищенных от атак по побочным каналам. В рамках данной работы дано полное описание множества функций от n переменных, допускающих разделения на функции от $n-1$ переменной. Полученные результаты обобщаются на случай отображений над произвольными конечными полями.

Ключевые слова: n-разделения, атаки по побочным каналам, маскировка

Представлена в редакцию: 25.05.2022.

1. Введение

Международная Олимпиада по криптографии NSUCrypto проводится с 2014 года, и является одним из интереснейших мероприятий в мире криптографии. Главной площадкой и организатором олимпиады является Новосибирский Государственный Университет. В состав жюри входят авторитетные специалисты-криптографы из России и стран ближнего и дальнего зарубежья. В олимпиаде могут принять участие все интересующиеся криптографией — от школьников до профессионалов-криптографов (разумеется, призовой зачет в этих категориях раздельный).

Участникам предлагаются задачи различного уровня сложности, в том числе и открытые математические проблемы. За первые семь лет участникам было дано около двадцати задач, отмеченных организаторами как нерешенные. По многим из них в ходе олимпиады были достигнуты интересные продвижения. Эти продвижения, вместе с остальными результатами, публикуются и обсуждаются в отчетных публикациях организаторов [1, 2, 3].

В 2019 году в качестве одной из задач была предложена задача об описании «неполных разделений» булевых отображений многих переменных. Эта задача была отмечена как нерешенная. В итоговом отчете [3] организаторы отметили продвижения, достигнутые некоторыми командами. Однако полного решения так и не было предложено. Таким образом, насколько нам известно, данная задача считается нерешенной.

Понятие «неполного разделения» для булева отображения имеет большое прикладное значение в криптографии. В работе [4] исследовался вопрос о возможности использования таких разделений для противодействия атакам по побочным каналам. Идея здесь состоит в следующем: при реализации алгоритма разделить промежуточные переменные на части, дающие в сумме исходное значение, и оперировать над ними независимо. Это позволяет ни в какой момент времени не хранить в явном виде промежуточные значения. Вместо этого операции будут производиться над «долями», которые могут представлять собой, по сути, случайные маски.

Однако такая маскировка требует, чтобы реальная криптографическая функция допускала соответствующее «разделение» на сумму независимых функций. Это условие, в наиболее интересном случае нелинейных функций, весьма нетривиально. Большое количество долей приводит к соответствующему росту сложности реализующей схемы, и соответственно, удорожанию устройства и снижению его производительности. В работе [4] приведены некоторые частные оценки числа необходимых дополнительных функций при заданном количестве «масок». Они оказались весьма быстро растущими. В той же работе было показано, что свойство «неполноты» является одним из необходимых условий для противодействия атакам по энергопотреблению, в частности дифференциальным атакам первого порядка. Дальнейшие исследования по этой теме проводились, в частности, в работах [5], [6], [7].

В рамках данной работы мы исследуем близкий класс объектов — «слабые неполные разделения». Предложено полное описание данного класса объектов. Приводимые результаты справедливы не только для случая булевых функций, но и для случая функций многих переменных над произвольным конечным полем.

2. Основные конструкции

Определение 1. Пусть K — конечное поле; $V = K^m$ — конечномерное линейное пространство над K; f — обратимая функция из V в V; $F = \langle F_1, \ldots, F_n \rangle$ — биективное отображение из V^n в V^n. Тогда:

1. F называется n-разделением (n-sharing) для f, если для любого набора $(x_1, \ldots, x_n) \in$ $\in V^n$ выполняется равенство

$$f\left(\sum_{i=1}^{n} x_i\right) = \sum_{i=1}^{n} F_i(x_1, \ldots, x_n). \tag{1}$$

2. F называется неполным n-разделением (non-complete n-sharing) для f, если оно является n-разделением для f и при этом для любого $i \in \{1, \ldots, n\}$ компонента F_i не зависит существенно от переменной x_i.

Задача, исходно поставленная на NSUCrypto'2019, состояла из трех подзадач:

Вопрос 1. Пусть $V = \mathbb{F}_2^4$, f, g — две аффинно эквивалентные обратимые функции из V в V (т.е. $g = a \circ f \circ b$, где a, b — обратимые аффинные преобразования V). Зная неполное n-разделение F для f, построить неполное n-разделение G для g.

Вопрос 2. Пусть $V = \mathbb{F}_2^4$. Найти точное описание функций $f\colon V \to V$, для которых существует неполное n-разделение F (при $n = 3, 4$).

Вопрос 3. Обобщить результаты на случай $V = \mathbb{F}_2^5$, $V = \mathbb{F}_2^6$.

Ответ на вопрос 1 довольно прост. Для полноты картины мы рассмотрим его в следующем разделе. Некоторые полученные там технические результаты будут полезны в последующих, более сложных задачах.

Вопросы 2 и 3 были отмечены как нерешенные. Постановка вопросов для конкретных пространств V малой размерности над полем $K = \mathbb{F}_2$ наводит на мысль, что предполагалось какое-то вычислительное решение (как минимум, для вопросов 2 и 3). Однако на самом деле рассмотрение вопроса общеалгебраическими методами позволяет значительно упростить ситуацию, а также распространить результаты на значительно более общий случай.

Для удобства формулировки и доказательства последующих результатов введем еще одно определение:

Определение 2. Пусть K — конечное поле; $V = K^m$ — конечномерное линейное пространство над K; f — произвольная функция из V в V; $F = \langle F_1, \ldots, F_n \rangle$ — произвольное отображение из V^n в V^n. Тогда:

1. F называется *слабым* n-разделением (*weak* n-sharing) для f, если для любого набора $(x_1, \ldots, x_n) \in V^n$ выполняется равенство (1).

2. F называется *слабым* неполным n-разделением (*weak* non-complete n-sharing) для f, если оно является слабым n-разделением для f, и при этом для любого $i \in \{1, \ldots, n\}$ компонента F_i не зависит существенно от переменной x_i.

Иными словами, «настоящие» разделения превращаются в слабые при отбрасывании требования обратимости. Или же, формально более точно, «настоящее» n-разделение есть частный случай слабого с дополнительным условием обратимости f и F.

Требование «неполноты» разделения является критически важным, поскольку без него задача становится тривиальной. В самом деле, любая функция $f(x)$ может быть представлена слабым n-разделением $F_1(x_1, \ldots, x_n) = f(x_1 + \ldots + x_n)$, $F_i(x_1, \ldots, x_n) = 0$ при $i = 2, \ldots, n$. Оно не биективно, но проблема легко решаема: $F_i(x_1, \ldots, x_n) = x_i$ при $i = 2, \ldots, n$ и $F_1(x_1, \ldots, x_n) = f(x_1 + \ldots + x_n) - \sum\limits_{i=2}^{n} x_i$ будет «настоящим» n-разделением. Таким образом, разделения, не являющиеся неполными, не представляют значительного интереса с точки зрения математики. Поэтому далее мы будем делать акцент исключительно на неполных разделениях.

В отличие от «настоящих» разделений, слабые имеют более естественную алгебраическую структуру. А именно, множество слабых неполных n-разделений над $V = K^m$ является линейным пространством над K. Также линейным пространством будет и множество функций $f\colon V \to V$, имеющих слабое (неполное) n-разделение. Более того, существует естественный гомоморфизм между этими двумя множествами.

Мы начнем с рассмотрения вопроса 1 — наиболее простого. Затем мы получим необходимое условие существования слабого неполного n-разделения для произвольных n, K и V. Очевидно, это же условие будет необходимым и для существования неполного n-разделения. Это позволит частично решить вопросы 2 и 3. Дальнейшее продвижение в разрешении этих вопросов будет состоять в построении конкретных примеров слабых неполных n-разделений для произвольных n, K и V. Затем мы покажем, что ранее найденное необходимое условие существования слабого неполного n-разделения является и достаточным. Более того, мы опишем все возможные слабые неполные n-разделения для конкретных функций.

Таким образом, для полного решения вопросов 2 и 3 останется решить лишь вопрос об обратимости построенного слабого n-разделения (точнее, о существовании хотя бы одного обратимого отображения в построенном множестве слабых n-разделений). Далее мы предложим возможный подход к решению этой задачи.

3. Аффинные преобразования

В данном разделе мы рассмотрим связь между разделениями и аффинными преобразованиями. Целью будет получение конструктивного ответа на вопрос 1 из исходной задачи. Попутно мы докажем ряд вспомогательных утверждений, которые окажутся полезными впоследствии.

Лемма 1. Пусть $F = \langle F_1, \ldots, F_n\rangle$ — (слабое) неполное n-разделение функции f и $g = f \circ a$, где a — линейная функция. Тогда $G = \langle G_1, \ldots, G_n\rangle$, где $G_i = F_i \circ a$ также является (слабым) неполным n-разбиением для g.

Доказательство. Очевидно, биективность G эквивиалентна биективности F. Поэтому достаточно установить утверждение лишь для слабых разделений.

Для любых $x_1, \ldots, x_n$ выполняется

$$f(x_1 + \ldots + x_n) = F_1(x_1, \ldots, x_n) + \ldots + F_n(x_1, \ldots, x_n).$$

Следовательно, для любых $x_1, \ldots, x_n$ выполняется

$$g(y_1 + \ldots + y_n) = f(a(y_1) + \ldots + a(y_n)) = \sum_{i=1}^{n} F_i(a(y_1), \ldots, a(y_n)) = \sum_{i=1}^{n} G_i(y_1, \ldots, y_n),$$

где $G_i(y_1, \ldots, y_n) = F_i(a(y_1), \ldots, a(y_n))$. Таким образом, G есть (слабое) n-разделение для g.

Более того, $F_i(x_1, \ldots, x_n)$ не зависит от x_i тогда и только тогда, когда $G_i(y_1, \ldots, y_n) = F_i(a(y_1), \ldots, a(y_n))$ не зависит от y_i. Следовательно, F — неполное (слабое) разделение тогда и только тогда, когда G также неполное (слабое) разделение.

Лемма 2. Пусть $F = \langle F_1, \ldots, F_n \rangle$ — (слабое) неполное разделение для f и $g = b \circ f$, где b — линейная функция. Тогда $G = \langle G_1, \ldots, G_n \rangle$, где $G_i = b \circ F_i$ — (слабое) неполное разделение для g.

Доказательство. Очевидно, биективность G эквивиалентна биективности F. Поэтому достаточно установить утверждение лишь для слабых разделений.

Для любых $x_1, \ldots, x_n$ выполняется

$$f(x_1 + \ldots + x_n) = \sum_{i=1}^{n} F_i(x_1, \ldots, x_n).$$

Следовательно,

$$g(x_1 + \ldots + x_n) = b(f(x_1 + \ldots + x_n)) = b\Big(\sum_{i=1}^{n} F_i(x_1, \ldots, x_n)\Big) = \\ = \sum_{i=1}^{n} (b \circ F_i)(x_1, \ldots, x_n) = \sum_{i=1}^{n} G_i(x_1, \ldots, x_n)$$

где $G_i(x_1, \ldots, x_n) = b \circ F_i(x_1, \ldots, x_n)$. Таким образом, G есть (слабое) n-разделение для g.

Далее, G_i не зависит от x_i тогда и только тогда, когда F_i не зависит от x_i. Следовательно, F — неполное (слабое) разделение для f тогда и только тогда, когда G — неполное (слабое) разделение для g.

Лемма 3. Пусть F — (слабое) неполное разделение для f и $g = b \circ f \circ a$, где b и a — линейные функции. Тогда $G = \langle G_1, \ldots, G_n \rangle$, где $G_i = b \circ F_i \circ a$ — (слабое) неполное разделение для g.

Доказательство. Утверждение сразу следует из лемм 1 и 2.

Следующее утверждение позволяет решить вопрос о связи между разделениями и сдвигами (по входным и выходным значениям).

Лемма 4. Пусть F — (слабое) неполное разделение для f и $f'(x) = f(x + \alpha) + \beta$, где α и β — некоторые константы. Тогда $F' = \langle F'_1, F'_2, \ldots, F'_n \rangle$, где

$$F'_i(x_1, \ldots, x_{n-1}, x_n) = \begin{cases} F_i(x_1, \ldots, x_{n-1}, x_n + \alpha), & i = 1, \ldots, n-1; \\ F_i(x_1, \ldots, x_{n-1}, x_n + \alpha) + \beta, & i = n \end{cases}$$

— (слабое) неполное разделение для f'.

Доказательство. Как и в предыдущих леммах, достаточно установить утверждение лишь для слабых разделений. Непосредственной подстановкой получаем

$$f'(x_1 + \ldots + x_n) = f(x_1 + \ldots + x_n + \alpha) + \beta = \sum_{i=1}^{n} F_i(x_1, \ldots, x_{n-1}, x_n + \alpha) + \beta = \sum_{i=1}^{n} F'_i(x_1, \ldots, x_n).$$

Произвольная аффиная функция может быть представлена в виде суперпозиции линейной функции и сдвига на константу. Пусть $b(x) = b'(x) + \beta$, $a(x) = a'(x) + \alpha$, где a', b' линейны, а α и β — константы.

Теперь мы можем доказать основное утверждение данного раздела.

Теорема 1. Пусть F — (слабое) неполное разделение для f и $g = b \circ f \circ a$, где b и a — аффинные функции. Тогда $G = \langle G_1, \ldots, G_n \rangle$, где

$$G_i(x_1, \ldots, x_n) = \begin{cases} b'(F_i(a'(x_1), \ldots, a'(x_n) + \alpha))), & i = 1, \ldots, n-1; \\ b'(F_i(a'(x_1), \ldots, a'(x_n) + \alpha)) + \beta, & i = n \end{cases}$$

— (слабое) неполное разделение для g.

Д о к а з а т е л ь с т в о. Как и в предыдущих леммах, достаточно установить утверждение лишь для слабых разделений. Имеем

$$g(x) = b(f(a(x))) = b'(f(a'(x) + \alpha)) + \beta.$$

Правая часть в этом равенстве есть суперпозиция двух линейных функций и двух сдвигов. Последовательно применяя леммы 3 и 4, получаем требуемый результат.

4. Необходимое условие для слабых разделений — «правило гиперкуба»

Будем обозначать через $||x||$ вес Хэмминга вектора x. Также пусть

$$\delta_\sigma(x) = \begin{cases} x, & \sigma = 1; \\ 0, & \sigma = 0 \end{cases}$$

и

$$\Delta_\sigma(x) = \langle \delta_{\sigma_1}(x_1), \ldots, \delta_{\sigma_n}(x_n) \rangle.$$

Докажем необходимое условие существования слабого неполного n-разделения.

Теорема 2. Пусть V — линейное пространство над полем K; $f\colon V \to V$ — произвольная функция. Пусть существует слабое неполное n-разделение $F = \langle F_1, \ldots, F_n \rangle$ для f. Тогда для f выполняется следующее равенство («правило гиперкуба»):

$$\sum_{\sigma \in \{0,1\}^n} (-1)^{||\sigma||} \cdot f\left(\sum_{i=1}^{n} \delta_{\sigma_i}(x_i)\right) = 0 \tag{2}$$

при любых $x_1, \ldots, x_n \in V$.

Д о к а з а т е л ь с т в о. По определению слабого неполного n-разделения мы имеем

$$f(x_1 + \ldots + x_n) = \sum_{i=1}^{n} F_i(x_1, \ldots, x_n).$$

Следовательно,

$$\sum_{\sigma \in \{0,1\}^n} (-1)^{||\sigma||} \cdot f\left(\sum_{i=1}^{n} \delta_{\sigma_i}(x_i)\right) = \sum_{\sigma \in \{0,1\}^n} (-1)^{||\sigma||} \cdot \left(\sum_{i=1}^{n} F_i(\Delta_\sigma(x))\right) =$$

$$= \sum_{i=1}^{n} \sum_{\sigma \in \{0,1\}^n} (-1)^{||\sigma||} F_i(\Delta_\sigma(x)).$$

Функция F_i не зависит от переменной x_i. Значит, $F_i(\Delta_\sigma(x)) = F_i(\Delta_{\sigma'}(x))$, где $\sigma = \langle\sigma_1, \ldots, \sigma_i, \ldots, \sigma_n\rangle$ и $\sigma' = \langle\sigma_1, \ldots, \overline{\sigma_i}, \ldots, \sigma_n\rangle$. В результате каждое слагаемое в левой части (2) встречается дважды — один раз со знаком «плюс», а второй — со знаком «минус». Следовательно, сумма равна 0.

В дальнейшем знакопеременную сумму в левой части соотношения (2) иногда для краткости будем обозначать $\mathrm{HSum}(f, x_1, \ldots, x_n)$.

Определение 3. Пусть K — произвольное поле; V — линейное пространство над K; $f\colon V \to V$ — произвольное отображение. Назовем его n-гиперкубическим отображением если для него выполняется условие (2) («правило гиперкуба»).

Теперь представим несколько несложных, но полезных результатов об n-гиперкубических отображениях.

Определение 4. Пусть V — линейное пространство над полем K, $u_1, \ldots, u_n \in V$ — произвольный набор векторов.

1. Мультимножество, состоящее из всевозможных сумм вида $u_{i_1} + \ldots + u_{i_s}$, где $s \leq n$, $i_1 < \ldots < i_s$ (с учетом кратности их вхождений, как элементов V), будем называть *n-мерным гиперкубом*. Обозначим его $\mathrm{HCube}(u_1, \ldots, u_n)$.

2. Элементы этого мультимножества будем называть вершинами.

3. Если все такие суммы различны, будем называть гиперкуб *невырожденным*.

4. Если хотя бы две из указанных сумм совпадают, будем называть гиперкуб *вырожденным*.

Понятие невырожденности имеет важное значение для случая двоичных полей. Это иллюстрируется следующим фактом.

Лемма 5. Пусть $V = K^m$ — линейное пространство над полем K; $\mathrm{char}\, K = 2$; $f\colon V \to V$ — произвольное отображение. Тогда справедливы следующие утверждения:

1) для любого набора векторов $u_1, \ldots, u_n \in V$ сумма $\mathrm{HSum}(f, u_1, \ldots, u_n)$ зависит только от вершин соответствующего гиперкуба $\mathrm{H} = \mathrm{HCube}(u_1, \ldots, u_n)$ и равна $\sum\limits_{v \in \mathrm{H}} f(v)$. В частности, если два набора задают один и тот же гиперкуб, то и соответствующие суммы одинаковы;

2) любая вершина гиперкуба встречается в нем одинаковое количество раз, и это количество является степенью двух;

3) если гиперкуб $\mathrm{HCube}(u_1, \ldots, u_n)$ вырожден, то сумма $\mathrm{HSum}(f, u_1, \ldots, u_n)$ равна нулю;

4) отображение f является m-гиперкубическим в том и только том случае, когда $\sum\limits_{v \in V} f(v) = 0$;

5) если $m > 1$ или $K \neq \mathbb{F}_2$, то любое биективное отображение является m-гиперкубическим.

Доказательство. В двоичном случае знакопеременная сумма $\mathrm{HSum}(f, u_1, \ldots, u_n)$ совпадает с обычной суммой тех же слагаемых. Очевидно, что она зависит только от набора

вершин (с учетом кратности), но не от их конкретного представления в виде сумм. Это доказывает пункт 1.

Следующей целью будет доказательство пункта 2. Для этого зафиксируем некоторый вектор $\lambda = \langle \lambda_1, \ldots, \lambda_n \rangle \in K^n$ и рассмотрим отображение $\pi\colon K^n \to V$, которое задано правилом

$$\pi(\langle \lambda_1, \ldots, \lambda_n \rangle) = \sum_{i=1}^{n} \lambda_i u_i.$$

Оно является гомоморфизмом линейных пространств. Следовательно, $\operatorname{Im}\pi \cong K^n / \operatorname{Ker}\pi$. При этом количество элементов в прообразе каждой вершины одинаково и равно $|\operatorname{Ker}\pi| = 2^k$ для некоторого k (поскольку $\operatorname{Ker}\pi$ — подпространство в K^n). Что и требовалось доказать.

Пункт 3 следует пунктов 1 и 2. В самом деле, если гиперкуб вырожден, то по определению хотя бы одна из его вершин встречается как минимум дважды. Следовательно, в силу пункта 2, количество ее вхождений равно 2^k, $k \geq 1$, т.е. четно. Но тогда и все вершины встречаются четное количество раз. А значит, сумма по ним равна 0. В силу пункта 1, эта сумма совпадает с $\operatorname{HSum}(f, u_1, \ldots, u_n)$.

Пункт 3 позволяет при проверке n-гиперкубичности отображения исключить из рассмотрения все вырожденные гиперкубы размерности n. Невырожденный гиперкуб, очевидно, содержит в точности 2^n различных вершин. Следовательно, существует единственный невырожденный гиперкуб размерности m. Он в точности совпадает с самим пространством V. В силу пункта 1, сумма $\sum\limits_{v \in V} f(v)$ совпадает с $\operatorname{HSum}(f, u_1, \ldots, u_n)$. Поэтому условие m-гиперкубичности эквивалентно $\sum\limits_{v \in V} f(v) = 0$. Таким образом, пункт 4 следует из пунктов 3 и 1.

Пункт 5 выводится из пункта 4 прямым подсчетом. В самом деле, биективность f означает, что

$$\sum_{v \in V} f(v) = \sum_{u \in V} u.$$

Легко проверить, что сумма всех векторов любого линейного пространства над конечным полем, за исключением случая $V = \mathbb{F}_2$, равна нулю.

Таким образом, все утверждения леммы полностью доказаны.

5. Достаточность «правила гиперкуба» для слабых разделений

Докажем теперь, что «правило гиперкуба» является также и достаточным условием существования слабого неполного n-разделения. Для начала рассмотрим простейший случай $n = 3$. Это позволит проиллюстрировать основную идею при помощи конкретного численного примера.

Лемма 6. Пусть V — линейное пространство над полем K; $f\colon V \to V$ — некоторая функция, удовлетворяющая условию (2) для $n = 3$. Тогда существует слабое неполное n-разделение $F = \langle F_1, \ldots, F_n \rangle$.

Доказательство. Мы построим искомое n-разделение явно. Сначала, для упрощения рассуждений, рассмотрим случай $f(0) = 0$. Обозначим через $\Phi(t_1, \ldots, t_{n-1})$ функцию, определенную согласно формуле

$$\Phi(t_1, \ldots, t_{n-1}) = \sum_{k=0}^{n-1} (-1)^k \cdot f\Big(\sum_{i=1}^{k} t_i\Big),$$

и положим

$$F_i(x_1, \ldots, x_n) = \Phi(x_{i+1}, \ldots, x_n, x_1, \ldots, x_{i-1}).$$

Тогда $F = \langle F_1, \ldots, F_n \rangle$ является слабым неполным n-разделением для f.

В самом деле, рассмотрим сумму

$$\sum_{i=1}^{3} F_i(x_1, x_2, x_3) = \Phi(x_2, x_3) + \Phi(x_3, x_1) + \Phi(x_1, x_2) =$$
$$= f(x_2 + x_3) - f(x_2) + f(x_3 + x_1) - f(x_3) + f(x_1 + x_2) - f(x_1).$$

Очевидно, эта сумма равна $\mathrm{HSum}(f, x_1, x_2, x_3) + f(x_1 + x_2 + x_3) - f(0)$, т.е. сумме по гиперкубу (левой части (2)) плюс $f(x_1 + x_2 + x_3) - f(0)$. Однако $f(0) = 0$ и сумма по гиперкубу, в силу условия (2)), также равна 0. Следовательно,

$$f(x_1 + x_2 + x_3) = \sum_{i=1}^{3} F_i(x_1, x_2, x_3),$$

что и означает, что F есть слабое n-разделение для f (при $n = 3$). По построению очевидно, что F_i не зависит от x_i. Следовательно F — слабое неполное n-разделение.

Осталось рассмотреть случай $f(0) \neq 0$. Для этого достаточно сначала построить слабое неполное n-разделение для $\tilde{f}(x) = f(x) - f(0)$, а затем воспользоваться леммой 4.

Отметим, что лемма 6 позволяет построить слабое n-разделение, но ничего не говорит о его обратимости. Таким образом, вопрос о построении «настоящих» n-разделений остается открытым (даже для $n = 3$).

Ближайшей нашей целью будет обобщение леммы 6 на случай произвольного n.

Вернемся вновь к формуле (2) и отметим, что она дает нам явное представление для $f(x_1 + \ldots + x_n)$ в виде знакопеременной суммы слагаемых вида $\sum\limits_{i \in I} f(x_i)$ (при некотором специально подобранном наборе подмножеств $I \subset \{0, 1\}^n$). Утверждение леммы 6 получено в результате явной группировки слагаемых в подходящие F_i. Используем аналогичный метод для произвольного n.

Лемма 7. Пусть V — линейное пространство над полем K; $f\colon V \to V$ — некоторая функция, удовлетворяющая условию (2) для некоторого n. Тогда существует слабое неполное n-разделение $F = \langle F_1, \ldots, F_n \rangle$.

Доказательство. В силу (2) имеем

$$f(x_1 + \ldots + x_n) = -\sum_{I} (-1)^{n-|I|} \cdot f\Big(\sum_{i \in I} x_i\Big),$$

где суммирование производится по всем $I \subset \{0,1\}^n$, $I \neq \{0,1\}^n$. Сопоставим каждому такому I индекс ϱ_I, такой, что $\varrho_I \notin I$ (это всегда можно сделать, поскольку $I \neq \{0,1\}^n$). Теперь определим $F_k(x_1, \dots x_n)$ по следующему правилу:

$$F_k(x_1, \dots x_n) = -\sum_{I, \varrho_I = k} (-1)^{n-|I|} \cdot f\Big(\sum_{i \in I} x_i\Big).$$

В силу выбора ϱ_I, никакое из слагаемых в F_k не зависит от x_k. В то же время сумма всех F_k содержит все слагаемые вида $(-1)^{n-|I|} \cdot f\left(\sum\limits_{i \in I} x_i\right)$ в точности по одному разу. Таким образом,

$$\sum_{k=1}^{n} F_k(x_1, \dots x_n) = f(x_1 + \dots + x_n)$$

Следовательно, $F = \langle F_1, \dots, F_n \rangle$ является слабым неполным n-разделением для f.

Таким образом, «правило гиперкуба» дает необходимое и достаточное условие существования слабого неполного n-разделения для f. Более того, оно позволяет построить конкретные примеры таких разделений. Однако эти примеры, разумеется, не единственны. Более того, вышеуказанные рассуждения не дают возможности понять, есть ли среди возможных слабых n-разделений «настоящие» (т.е. биекции).

Для решения этих вопросов необходимо дать более точное описание множества возможных слабых n-разделений. Мы сделаем это в следующем разделе.

Зафиксируем основной результат данного раздела в виде следующего утверждения.

Теорема 3. Пусть V — линейное пространство над полем K; $f\colon V \to V$ — произвольное отображение. Тогда существует слабое неполное n-разделение $F = \langle F_1, \dots, F_n \rangle$ для f в том и только в том случае, когда f удовлетворяет условию (2) для данного n.

Доказательство. Утверждение сразу следует из леммы 7 и теоремы 2.

Из этого результата мы сразу несколько интересных следствий.

Следствие 1. Пусть в ранее введенных обозначениях $\operatorname{char} K = 2$, $V = K^m$. Тогда $f : V \to V$ имеет слабое неполное m-разделение тогда и только тогда, когда $\sum\limits_{v \in V} f(v) = 0$. В частности, если если $m \geq 2$ или $K \neq \mathbb{F}_2$, любое биективное отображение из V в V имеет слабое неполное m-разделение.

Доказательство. Утверждение следует из Теоремы 3 и пунктов 4 и 5 Леммы 5. Теорема доказана.

Для того, чтобы сформулировать следующее следствие, нам необходимо ввести еще одно полезное определение.

Определение 5. Пусть K — поле; $\tilde{K}$ — его простое подполе; $V = K^m$ — линейное пространство над K. На V естественным образом введена структура линейного пространства над $\tilde{K}$.

1. Отображение $f\colon V \to V$ назовем квазилинейным, если оно является линейным как отображение $\tilde{K}$-линейных пространств.

2. Отображение $f\colon V \to V$ назовем квазиаффинным, если оно является суммой квазилинейного отображения и константы.

Следствие 2. Отображение $f\colon V \to V$ имеет слабое неполное 2-разделение в том и только в том случае, когда f — квазиаффинное отображение. Если при этом $f(0) = 0$, то отображение квазилинейно.

Доказательство. Если отображеие квазиаффинно, то для него выполняется правило гиперкуба размерности 2. Это легко проверяется прямым подсчетом. В совокупности с теоремой 3 это доказывает достаточность. Требование квазилинейности автоматически влечет $f(0) = 0$.

Осталось установить необходимость условия квазиаффинности (и квазилинейности, соответственно).

Более простой является вторая часть утверждения. Пусть $f(0) = 0$. Тогда правило гиперкуба для размерности 2 означает аддитивность функции:

$$f(u + v) = f(u) + f(v) - f(0) = f(u) + f(v).$$

Для частного случая $u = kv$, где $k \in \mathbb{Z}$ отсюда легко вывести соотношение $f(ku) = kf(u)$. В случае положительной характеристики этого достаточно для $\tilde{K}$-линейности отображения. В случае характеристики 0 также имеем

$$b \cdot f((a/b) \cdot x) = f(a \cdot x) = a \cdot f(x)$$

при любых $a,\ b \in \mathbb{Z},\ b \neq 0$. Следовательно, $f(\lambda x) = \lambda f(x)$ при любом $\lambda \in \mathbb{Q}$.

Таким образом, 2-гиперкубическая функция, удовлетворяющая условию $f(0) = 0$, является квазилинейной.

Для доказательства первой части утверждения достаточно представить целевую функцию в виде $f(x) = \tilde{f}(x) + C$, где $C = f(0)$. Очевидно, что $\tilde{f}$ будет 2-гиперкубической с условием $\tilde{f}(0) = 0$, и следовательно, квазилинейной. Это означает, что f — квазиаффинна.

Замечание 1. Помимо самостоятельной ценности, следствие 2 также интересно тем, что приводит нас к идее описания отображений, допускающих разделения заданного порядка, через их полиномиальное представление над расширенным полем. Эта идея станет центральной для результатов последующих разделов.

Замечание 2. Утверждения из предыдущих разделов, по-видимому, обобщаются на случай, когда K — произвольное коммутативное кольцо, а $V = K^m$ — свободный модуль над ним.

6. Полное описание слабых n-разделений

Для начала введем несколько дополнительных обозначений. Через $\hat{\mathcal{V}}$ обозначим множество всех отображений $f\colon V \to V$, имеющих слабые неполные n-разделения, а через

$\hat{\mathcal{W}}$ — множество отображений $F\colon V^n \to V^n$, являющихся слабыми неполными n-разделениями для некоторой функции. Несложно проверить, что $\hat{\mathcal{V}}$ и $\hat{\mathcal{W}}$ являются линейными пространствами над K.

Каждое отображение $F \in \hat{\mathcal{W}}$ является неполным слабым n-разделением для некоторой функции $f \in \hat{\mathcal{V}}$. Таким образом, имеется естественный гомоморфизм $\phi\colon \hat{\mathcal{W}} \to \hat{\mathcal{V}}$, отображающий $F = \langle F_1, \ldots, F_n\rangle$ в соответствующую f. Он задается правилом

$$(\phi(F))(x_1 + \ldots + x_n) = \sum_{i=1}^{n} F_i(x_1, \ldots, x_n).$$

Этот гомоморфизм сюръективен, но не инъективен. Его ядро состоит из всех слабых неполных n-разделений для нулевой функции.

Обозначим через $\mathcal{W}_{ij}$ множество отображений $F\colon V^n \to V$, которые не зависят существенно от переменных x_i и x_j. Тогда имеет место следующий факт.

Теорема 4. $F = \langle F_1, \ldots, F_n\rangle \in \operatorname{Ker}\phi$ тогда и только тогда, когда существуют $F_{ij} \in \mathcal{W}_{ij}$, такие, что

$$F_i = \sum_{j=1}^{n} F_{ij}, F_{ij} = -F_{ji}, F_{ii} = 0. \tag{3}$$

Доказательство. Пусть выполнены условия (3). Прямой подсчет показывает, что $\sum\limits_{i=1}^{n} F_i(x_1, \ldots, x_n) = 0$. Также, поскольку F_{ij} не зависит явно от x_i и x_j, то и F_i не зависит от x_i. Следовательно, $F = \langle F_1, \ldots, F_n\rangle$ есть слабое неполное n-разделение для 0, а значит — лежит в ядре ϕ.

Наоборот, пусть имеется некоторое n-разделение для нуля. Нужно показать, что условия (3) выполняются. Докажем это по индукции. Ясно, что утверждение имеет содержательный смысл лишь при $n > 1$.

База индукции. Пусть $n = 2$. В этом случае имеем $F_1(x_2) + F_2(x_1) = 0$. Положим $C = F_1(0)$. Тогда $F_1(0) + F_2(x_1) = C + F_2(x_1) = 0$, т.е. $F_2(t) = -C$ при всех t. Далееб $F_1(x_2) + F_2(0) = F_1(x_2) - C = 0$, т.е. $F_1(t) = C$ при всех t. Осталось положить $F_{12} = C = -F_{21}$ и проверить выполнение (3) прямым подсчетом.

Шаг индукции. Пусть утверждение верно для n. Рассмотрим теперь некоторое $n+1$-разделение для нуля, и покажем, что для него также выполнены условия (3). Имеет место равенство

$$\sum_{i=1}^{n} F_i(x_1, \ldots, x_n, x_{n+1}) = -F_{n+1}(x_1, \ldots, x_n, x_{n+1}) \tag{4}$$

Для любой функции $G\colon V^{n+1} \to V$ определим два отображения $G \mapsto G'$ и $G \mapsto G''$ согласно правилам

$$G'(x_1, \ldots, x_n, x_{n+1}) = G(x_1, \ldots, x_n, 0),$$
$$G''(x_1, \ldots, x_n, x_{n+1}) = G(x_1, \ldots, x_n, x_{n+1}) - G(x_1, \ldots, x_n, 0).$$

Очевидно, что $G = G' + G''$ и отображения $G \mapsto G'$, $G \mapsto G''$ являются гомоморфизмами линейных пространств.

Теперь разобъем каждую из функций $F_i(x_1, \ldots, x_n, x_{n+1})$ в сумму $F'_i(x_1, \ldots, x_n, x_{n+1}) = F_i(x_1, \ldots, x_n, 0)$ и $F''_i(x_1, \ldots, x_n, x_{n+1}) = F_i(x_1, \ldots, x_n, x_{n+1}) - F_i(x_1, \ldots, x_n, 0)$.

Отметим, что для F'_i переменная x_{n+1} всегда фиктивна. Для функции F''_i переменная x_{n+1} будет существенной тогда и только тогда, когда она существенна для F_i. В частности, для $i = n+1$ она фиктивна. Это означает, что $F''_{n+1}(x_1, \ldots, x_n, x_{n+1}) = 0$ и $F'_{n+1}(x_1, \ldots, x_n, x_{n+1}) = F_{n+1}(x_1, \ldots, x_n, x_{n+1})$.

В силу вышеуказанных соображений равенство (4) можно преобразовать в два:

$$\sum_{i=1}^{n} F'_i(x_1, \ldots, x_n, x_{n+1}) = -F_{n+1}(x_1, \ldots, x_n, x_{n+1}), \tag{5}$$

$$\sum_{i=1}^{n} F''_i(x_1, \ldots, x_n, x_{n+1}) = 0. \tag{6}$$

Теперь отметим, что в левой части равенства (5) функции F'_i не зависят от x_i (поскольку F_i не зависят от x_i). Положим $F_{i,n+1} = F'_i \in \mathcal{W}_{i,n+1}$, $F_{n+1,i} = -F_{i,n+1}$. Равенство (5) в точности совпадает с условием (3) при $i = n+1$.

Левая часть равенства (6), в свою очередь, в точности представляет собой условие (4) для набора F''_i (т.е. $\langle F''_1, \ldots, F''_n \rangle$ есть n-разделение для нуля). В силу предположения индукции, найдутся такие F''_{ij}б для которых $F''_i = \sum\limits_{i=1}^{n} F''_{ij}$, $F''_{ij} = -F''_{ji}$, $F''_{ii} = 0$ и $F'_{ij} \in \mathcal{W}_{ij}$. Полагая теперь $F_{ij} = F''_{ij}$ и пользуясь равенством $F_i = F'_i + F''_i$, получаем, что условия (3) выполнены также и для $i = 1, \ldots, n$.

Ранее доказанная лемма 7 дает возможность построить конкретное слабое n-разделение для любой функции, удовлетворяющей условию (2). В совокупности с теоремой 4 мы получаем полное конструктивное описание множества всех слабых неполных n-разделений для любой функции. Помимо самостоятельной ценности, этот результат дает также возможность исследовать вопрос о существовании в этом множестве «настоящих» (т.е. биективных) n-разделений.

7. n-разделимые функции и расширения конечных полей

Как мы установили выше, «правило гиперкуба» является необходимым и достаточным условием существования слабого неполного n-разделения. Однако остается неясным, как по виду функции f эффективно проверить выполнение этого условия. Целью данного раздела будет получение эффективного алгоритма такой проверки.

Для этого нам потребуется еще несколько определений и вспомогательных утверждений.

Определение 6. Пусть K — конечное поле; $V = K^m$ — конечномерное линейное пространство над K; $f\colon V \to V$ — произвольная функция. Для любого $t \in V$ определим «t-разность» $\Delta_t f$ по правилу

$$(\Delta_t f)(x) = f(x+t) - f(x).$$

Следующие результаты обосновывают наш интерес к изучению разностей в контексте нашей исходной задачи об описании n-разделений.

Лемма 8. Пусть K — конечное поле; $V = K^m$ — конечномерное линейное пространство над K. Тогда функция $f\colon V \to V$ удовлетворяет правилу гиперкуба для n в том и только в том случае, когда для любого $t \in V$ функция $\Delta_t f$ удовлетворяет правилу гиперкуба для $(n-1)$.

Доказательство. Необходимость. Пусть f удовлетворяет правилу гиперкуба. Для произвольного $t \in V$ рассмотрим сумму $\mathrm{HSum}(\Delta_t f, x_1, \ldots, x_{n-1})$. Прямым подсчетом легко проверить, что выполняется равенство

$$\mathrm{HSum}(\Delta_t f, x_1, \ldots, x_{n-1}) = \mathrm{HSum}(f, x_1, \ldots, x_{n-1}, t) = 0$$

Следовательно, при любом $t \in V$ для $\Delta_t f$ выполняется правило гиперкуба для $n-1$.

Достаточность. Легко видеть, что

$$\mathrm{HSum}(f, x_1, \ldots, x_{n-1}, x_n) = \mathrm{HSum}(\Delta_{x_n} f, x_1, \ldots, x_{n-1}) = 0$$

Лемма 9. Пусть K — конечное поле; $V = K^m$ — конечномерное линейное пространство над K. Тогда функция $f\colon V \to V$ имеет слабое n-разделение в том и только в том случае, когда для любого $t \in V$ функция $\Delta_t f$ имеет слабое $(n-1)$-разделение.

Доказательство. Это сразу следует из леммы 8 и теоремы 3.

Таким образом, техника t-разностей позволяет нам описать множество функций, имеющих слабые неполные n-разделения.

Очевидно, что Δ_t является K-линейным оператором на пространстве функций из V в V. Нашей ближайшей целью будет описать ядро и образ этого оператора. Мы сделаем это для наиболее интересного случая, когда основное поле K конечно. Для этого нам будет необходимо рассмотреть пространство V как конечное поле.

В самом деле, если $K = \mathbb{F}_q$, то конечное поле $\mathbb{F}_{q^m}$ изоморфно $V = K^m$ как линейное пространство. Таким образом, любая функция $f\colon V \to V$ может быть рассмотрена также как функция из $\mathbb{F}_{q^m}$ в $\mathbb{F}_{q^m}$. Разумеется, конкретный вид этой функции будет зависеть от выбора конкретного способа построения поля $\mathbb{F}_{q^m}$, а также от выбора базиса. Однако наши последующие результаты не будут от этого зависеть.

Из вышеприведенных рассуждений следует, что Δ_t будет оператором на пространстве функций из $\mathbb{F}_{q^m}$ в $\mathbb{F}_{q^m}$. Он имеет следующие свойства.

Лемма 10 (свойства t-разности). Пусть K — конечное поле; $V = K^m$ — конечномерное линейное пространство над K. Тогда для любого $t \in V$ и для любых $f\colon V \to V$, $g\colon V \to V$, $\lambda \in K$ верны следующие свойства:

1) $\Delta_t(f+g) = (\Delta_t f) + (\Delta_t g)$;

2) $\Delta_t(\lambda f) = \lambda(\Delta_t f)$;

3) $\Delta_t(fg) = (\Delta_t f) \cdot g + f \cdot (\Delta_t g) + (\Delta_t f) \cdot (\Delta_t g)$.

Доказательство. Легко проверяется прямым подсчетом.

Известно, что любая функция из F_{q^m} в F_{q^m} может быть однозначно представлена в виде многочлена степени не выше $q^m - 1$. Имеет место следующий факт.

Лемма 11. Для любого непостоянного отображения $f\colon F_{q^m} \to F_{q^m}$ и любого $t \in F_{q^m}$ выполнено $\deg \Delta_t(f) \leq \deg f - 1$.

Доказательство. В силу линейности Δ_t очевидно, что достаточно доказать утверждение лишь для мономов. Сделаем это по индукции.

База индукции. Очевидно, что $\Delta_t(x) = t$ и $\deg t = 0 = (\deg x) - 1$. Таким образом, для мономов степени

Шаг индукции. Пусть утверждение верно для x^n. Тогда

$$\Delta_t(x^{n+1}) = x^n \cdot \Delta_t(x) + \Delta_t(x^n) \cdot x + \Delta_t(x^n) \cdot \Delta_t(x).$$

При этом $\deg \Delta_t(x^n) \leq n - 1$ и $\deg \Delta_t(x) = 0$. Таким образом, степень всех слагаемых в правой части не превышает $n = \deg x^{n+1} - 1$. Что и требовалось доказать.

Теперь введем еще одно определение.

Определение 7. Пусть $p = \operatorname{char} \mathbb{F}_q$ — характеристика основного поля (т.е. $q = p^k$). Тогда:

1) p-адическим весом $w_p(n)$ целого числа n назовем сумму цифр в его p-ичной записи;

2) p-адическим весом $w_p(x^n)$ монома x^n назовем $w_p(n)$;

3) p-адическим весом $w_p(f)$ многочлена $f(x) \neq 0$ назовем максимальный из весов входящих в него мономов.

Вес нулевой функции, вообще говоря, не определен. Но для наших целей можно положить его равным -1 (или же любому отрицательному целому числу).

Очевидно, что для любых $i,\ j \in \mathbb{Z}$ выполнено $w_p(i+j) \leq w_p(i) + w_p(j)$ и $w_p(ip) = w_p(i)$. В силу этого для любых многочленов f, g выполнено $w_p(fg) \leq w_p(f) + w_p(g)$. Также ясно, что $w_p(f+g) \leq \max(w_p(f), w_p(g))$.

Следующее утверждение связывает понятия t-разности и p-адического веса с автоморфизмом Фробениуса $x \mapsto x^p$.

Лемма 12. В вышеуказанных обозначениях имеют место следующие свойства:

1) $w_p(f^p) = w_p(f)$;

2) $w_p(\Delta_t(f^p)) = w_p((\Delta_t(f))^p)$.

Доказательство. Легко проверяется прямым подсчетом.

Теперь мы готовы доказать следующее утверждение.

Лемма 13. Пусть $p = \operatorname{char} \mathbb{F}_q$ — характеристика основного поля (т.е. $q = p^k$). Тогда для любого $t \in \mathbb{F}_{q^m}$ и любого $f : \mathbb{F}_{q^m} \to \mathbb{F}_{q^m}$ выполнено

$$w_p(\Delta_t(f)) \leq w_p(f) - 1.$$

Доказательство. Очевидно, что достаточно доказать утверждение только для мономов. Сделаем это по индукции.

Для случаев $n = 0$ и $n = 1$ утверждение легко проверяется прямым подсчетом. Осталось доказать индуктивный переход.

Пусть $n \geq 2$ и для всех значений $k < n$ утверждение леммы выполняется. Нужно доказать, что $w_p(\Delta_t(x^n)) \leq w_p(x^n) - 1$.

Разделим n с остатком на p и получим представление $n = ap + b$. Если $b = 0$, то $n = ap$ и, следовательно, по предположению индукции и лемме 12

$$w_p(\Delta_t(x^n)) = w_p(\Delta_t(x^a)) \leq w_p(x^a) - 1 = w_p(x^n) - 1.$$

В случае $b \neq 0$ мы имеем $\Delta_t(x^n) = \Delta_t(x^{n-1} \cdot x)$ и по формуле произведения и свойствам веса получаем

$$w_p(\Delta_t(x^n)) \leq \max\Big(w_p(\Delta(x^{n-1})) + 1, w_p(x^{n-1}), w_p(\Delta(x^{n-1}))\Big) = \\ = \max\Big(w_p(\Delta(x^{n-1})) + 1, w_p(x^{n-1})\Big). \quad (7)$$

С другой стороны, легко видеть, что $w_p(x^n) = w_p(a) + b$ и $w_p(x^{n-1}) = w_p(a) + b - 1$. В силу индуктивного предположения $w_p(\Delta(x^{n-1})) \leq w_p(x^{n-1}) - 1 = w_p(a) + b - 2$. Подставляя эти значения в неравенство (7), получаем

$$w_p(\Delta_t(x^n)) \leq \max(w_p(a) + b - 2 + 1, w_p(a) + b - 1) = (w_p(a) + b) - 1 = w_p(x^n) - 1,$$

что и требовалось доказать.

В сочетании с леммой 9 это сразу дает необходимое условие существования n-разделений: *для существования слабого неполного n-разделения функции f необходимо, чтобы ее вес $w_p(f)$ не превышал $n - 1$.*

Следующей нашей целью будет показать, что это условие является и достаточным.

Лемма 14. Пусть $p = \operatorname{char} \mathbb{F}_q$ — характеристика основного поля (т.е. $q = p^k$). Тогда для любого неконстантого $f\colon \mathbb{F}_{q^m} \to \mathbb{F}_{q^m}$ существует $t \in \mathbb{F}_{q^m}$, такое, что

$$w_p(\Delta_t(f)) = w_p(f) - 1.$$

Доказательство. Пусть $w_p(f) = 1$. Тогда f есть сумма константы и мономов вида x^{p^k}. Константа не влияет на значение $\Delta_t f$. Поэтому, не умаляя общности, положим $f(0) = 0$. Очевидно, что $\Delta_t x^{p^k} = t^{p^k}$. Поэтому $\Delta_t f = f(t)$. При фиксированном значении t это константа. Если она отлична от нуля, то ее вес равен 0. Поскольку $\deg f \leq q^{m-1}$, то f в поле $\mathbb{F}_{q^m}$ имеет не более чем q^{m-1} корней. Следовательно, существует $\hat{t} \in \mathbb{F}_{q^m}$, не являющееся корнем f, и $w_p(\Delta_{\hat{t}} f) = 0$.

Пусть теперь $w_p(f) = k > 1$. Обозначим через l степень максимального из мономов, входящих в f с ненулевым коэффициентом, и имеющего максимальный вес $w_p(l) = k$.

Легко видеть, что $\Delta_t x^l$ имеет вид $\Delta_t x^l = ltx^{l-1} + \ldots + t^l$, где $l \neq 0 \bmod p$. Также ясно, что $w_p(l-1) = w_p(l) - 1 = w_p(f) - 1$.

Покажем, что этот же моном с ненулевым коэффициентом входит в $\Delta_t f$. В самом деле, для всех остальных мономов x^i, таких, что $w_p(i) = w_p(l)$, имеем $i < l$ и в силу леммы 11 $\deg \Delta_t x^i \leq i - 1 < l - 1$, так что сокращение невозможно. А для всех мономов вида x^i, для которых $w_p(i) < w_p(l)$, в силу леммы 13 имеем $w_p(\Delta_t x^i) \leq w_p(i) - 1 < k - 1$, сокращение опять же невозможно. Таким образом, коэффициент при x^{l-1} в $\Delta_t f$ в точности равен произведению lt и коэффициента при x^l в f, т.е. и в этом случае $w_p(\Delta_t f) = k-1 = w_p(f)-1$. Лемма полностью доказана.

Теперь мы готовы доказать следующий факт.

Теорема 5. Пусть $f\colon \mathbb{F}_{q^m} \to \mathbb{F}_{q^m}$ и $p = \operatorname{char} \mathbb{F}_{q^m}$. Тогда f имеет слабое неполное n-разделение в том и только том случае, когда $w_p(f) \leq n - 1$.

Доказательство. Сразу следует из лемм 9, 13 и 14.

Интересным с точки зрения криптографии следствием теоремы 5 является следующий факт.

Следствие 3. Преобразование, заданное S-блоком шифра AES, имеет слабое неполное 8-разделение, но не имеет неполных 7-разделений.

Доказательство. Известно [8, 9, 10], что преобразование, заданное S-блоком шифра AES, является суперпозицией $\mathbb{F}_2$-аффинного преобразования и инволютивного отображения $x \to x^{(-1)}$, заданного по правилу

$$x^{(-1)} = \begin{cases} 0, & x = 0; \\ x^{-1}, & x \neq 0. \end{cases}$$

Легко проверить, что $x^{(-1)} = x^{254}$. Это означает, что преобразование, заданное S-блоком шифра AES, аффинно эквивалентно преобразованию $f(x) = x^{254}$. Но $w_2(254) = 7$ и, следовательно, в силу теоремы 5, преобразование $x \to x^{254}$ имеет слабое неполное 8-разделение, но не имеет (слабых) неполных 7-разделений. Далее остается воспользоваться теоремой 1.

Заключение

В настоящей работе исследован вопрос о возможности представления функции от n переменных над конечным полем в виде неполного разделения, т.е. суммы функций от $n-1$ переменных. Этот вопрос, с прикладной точки зрения, важен для противодействия атакам по побочным каналам на конкретные реализации криптографических алгоритмов.

В работе получен эффективно проверяемый критерий представимости отображения в виде суммы отображений от меньшего числа переменных. Указанный критерий может быть использован для построения реализаций криптографических алгоритмов, защищенных от атак по побочным каналам. Также данный подход позволяет в ряде случаев обнаружить и

количественно оценить принципиальную уязвимость конкретных криптографических конструкций к атакам по побочным каналам.

Также данный результат может быть интересен с теоретической точки зрения. В частности, представляется интересным его применение для решения задачи эффективной декомпозиции функций. Данная функциональность может быть применена, например, в современных системах компьютерной алгебры, символьных вычислений и машинного обучения.

Работа выполнена при финансовой поддержке Российского Научного Фонда (грант 17-11-01377).

Список литературы

1. Tokareva N.N., Gorodilova A.A., Agievich S.V., Idrisova V.A., Kolomeec N.A., Kutsenko A.V., Oblaukhov A.K., Shushuev G.I. Mathematical methods in solutions of the problems presented at the Third International Students' Olympiad in Cryptography // Прикладная дискретная математика. 2018. № 40. С. 34–58. DOI: 10.17223/20710410/40/4
2. Gorodilova A.A., Agievich S.V., Carlet C., Gorkunov E.V., Idrisova V.A., Kolomeec N.A., Kutsenko A.V., Nikova S., Oblaukhov A.K., Picek S., Preneel B., Rijmen V., Tokareva N.N. Problems and solutions from the Fourth International Student's Olympiad in Cryptography (NSUCRYPTO) // Cryptologia. 2019. Vol. 43, no. 2. Pp. 138–174. DOI: 10.1080/01611194.2018.1517834
3. Городилова А.А., Токарева Н.Н., Агиевич С.В., Карле К., Горкунов Е.В., Идрисова В.А., Коломеец Н.А., Куценко А.В., Лебедев Р.К., Никова С., Облаухов А.К., Панкратова И.А., Пудовкина М.А., Реймен В., Удовенко А.Н. О шестой международной олимпиаде по криптографии NSUCRYPTO // Дискретный анализ и исследование операций. 2020. Т. 27, № 4. С. 21–57. DOI: 10.33048/daio.2020.27.689
4. Nikova S., Rechberger Ch., Rijmen V. Threshold implementations against side-channel attacks and glitches // Information and communications security: 8th Intern. conf. on information and communications security: ICICS 2006 (Raleigh, NC, USA, December 4-7, 2006): Proc. B.: Springer, 2006. Pp. 529–545. DOI: 10.1007/11935308_38
5. Bilgin B., Gierlichs B., Nikova S., Nikov V., Rijmen V. Higher-order threshold implementations // Advances in cryptology – ASIACRYPT 2014 - 20th Intern. conf. on the theory and application of cryptology and information security (Kaoshiung, Taiwan, R.O.C., December 7-11, 2014): Proc. Pt. II. B.: Springer, 2014. Pp. 326–343. DOI: 10.1007/978-3-662-45608-8_18
6. De Cnudde Th., Reparaz O., Bilgin B., Nikova S., Nikov V., Rijmen V. Masking AES with $d + 1$ shares in hardware // 2016 ACM workshop on theory of implementation security: TIS'2016 (Vienna, Austria, October 24, 2016): Proc. N.Y.: ACM, 2016. P. 43. DOI: 10.1145/2996366.2996428

7. Dhooghe S., Nikova S., Rijmen V. Threshold implementations in the robust probing model // 2019 ACM workshop on theory of implementation security: TIS'2019 (London, UK, November 11, 2019): Proc. N.Y.: ACM, 2019. Pp. 30–37. DOI: 10.1145/3338467.3358949
8. Dworkin M.J., Barker E.B., Nechvatal J.R., Foti J., Bassham L.E., Roback E., Dray J.F. jr. Advanced Encryption Standard (AES) // Federal Inf. Process. Stds. (NIST FIPS)–197. Published November 26, 2001. DOI: 10.6028/NIST.FIPS.197
9. Daemen J., Rijmen V. The design of Rijndael. AES – The Advanced Encryption Standard. B.: Springer, 2002. 238 p. DOI: 10.1007/978-3-662-04722-4
10. Murphy S., Robshaw M.J.B. Essential algebraic structure within the AES // Advances in cryptology – CRYPTO 2002: 22nd Annual intern. cryptology conf. (Santa Barbara, CA, USA, August 18-22, 2002): Proc. B.: Springer, 2002. Pp. 1–16. DOI: 10.1007/3-540-45708-9_1

Mathematics and Mathematical Modeling, 2022, no. 1, pp. 31–52.
DOI: **10.24108/mathm.0122.0000262**

Mathematics & Mathematical Modelling
Electronic journal
http://mathmelpub.ru ISSN 2412-5911

On a Classification of n-sharings of Multivariate Mappings over Finite Fields and One NSUCrypto'2019 Olympiad Problem

Chilikov A. A.[1,2,*]

[1]Bauman Moscow State Technical University, Russia
[2]Moscow Institute of Physics and Technology, Russia
[*]chilikov@passware.com

Keywords: n-sharings; side-channel attacks; masking

Received: 25.05.2022.

A problem of great importance that arises in designing and implementation of a cryptosystem is countering side channel attacks. Often an appropriate mathematical algorithm, implemented on a specific physical device to work in the physical environment, becomes vulnerable to such attacks.

The "function sharings" technique is a prospective and efficient way to avoid this problem. In this work we investigate "non-complete sharings" of Boolean functions and mappings, and functions and mappings over finite fields. We provide a complete description of the set of functions with n variables which have a sharings.

Our main results are following. We create and investigate a new concept of "weak" non-complete n -sharing; We state a connection between "weak" and "classical" sharings and explain the advantage of new concept from the algebraic point-of-view; We state and prove a criteria of the existence of a weak n-sharing for an arbitrary function; We provide an explicit description of the set of function which have weak sharings in terms of algebraic normal form; We state a simple variants of this description for "border" cases: $n = 2$, $n = m$ and binary fields; We apply these results to the AES S-box and completely solve the problem "is there a non-complete k-sharing for AES". And we believe that the same way can be used successfully for other cryptographic algorithms.

These results can be used to design new cryptosystems which are resisted to side-channel attacks. From the other side this approach can help to assess previously designed cryptographic solutions.

References

1. Tokareva N.N., Gorodilova A.A., Agievich S.V., Idrisova V.A., Kolomeec N.A., Kutsenko A.V., Oblaukhov A.K., Shushuev G.I. Mathematical methods in solutions of the problems presented at the Third International Students' Olympiad in Cryptography. *Prikladnaia Diskretnaia Matematika* [Applied Discrete Mathematics], 2018, no. 40, pp. 34–58. DOI: 10.17223/20710410/40/4

2. Gorodilova A.A., Agievich S.V., Carlet C., Gorkunov E.V., Idrisova V.A., Kolomeec N.A., Kutsenko A.V., Nikova S., Oblaukhov A.K., Picek S., Preneel B., Rijmen V., Tokareva N.N. Problems and solutions of the Fourth International Student's Olympiad in Cryptography (NSUCRYPTO). *Cryptologia*, 2019, vol. 43, no. 2, pp. 138–174. DOI: 10.1080/01611194.2018.1517834

3. Gorodilova A.A., Tokareva N.N., Agievich S.V., Carlet C., Gorkunov E.V., Idrisova V.A., Kolomeec N.A., Kutsenko A.V., Lebedev R.K., Nikova S., Oblaukhov A.K., Pankratova I.A., Pudovkina M.A., Rijmen V., Udovenko A.N. On the Sixth International Olympiad in Cryptography NSUCRYPTO. *J. of Applied and Industrial Mathematics*, 2020, vol. 14, no. 4, pp. 623–647. DOI: 10.1134/S1990478920040031

4. Nikova S., Rechberger Ch., Rijmen V. Threshold implementations against side-channel attacks and glitches. *Information and communications security: 8th Intern. conf. on information and communications security*: ICICS 2006 (Raleigh, NC, USA, December 4-7, 2006): Proc. B.: Springer, 2006. Pp. 529–545. DOI: 10.1007/11935308_38

5. Bilgin B., Gierlichs B., Nikova S., Nikov V., Rijmen V. Higher-order threshold implementations. *Advances in Cryptology – ASIACRYPT 2014 – 20th Intern. conf. on the theory and application of cryptology and information security* (Kaoshiung, Taiwan, R.O.C., December 7-11, 2014): Proc. Pt. II. B.: Springer, 2014. Pp. 326–343. DOI: 10.1007/978-3-662-45608-8_18

6. De Cnudde Th., Reparaz O., Bilgin B., Nikova S., Nikov V., Rijmen V. Masking AES with $d + 1$ shares in hardware. *2016 ACM workshop on theory of implementation security: TIS'2016* (Vienna, Austria, October 24, 2016): Proc. N.Y.: ACM, 2016. P. 43. DOI: 10.1145/2996366.2996428

7. Dhooghe S., Nikova S., Rijmen V. Threshold implementations in the robust probing model. *2019 ACM workshop on theory of implementation security: TIS'2019* (London, UK, November 11, 2019): Proc. N.Y.: ACM, 2019. Pp. 30–37. DOI: 10.1145/3338467.3358949

8. Dworkin M.J., Barker E.B., Nechvatal J.R., Foti J., Bassham L.E., Roback E., Dray J.F. jr. Advanced Encryption Standard (AES). Federal Inf. Process. Stds. (NIST FIPS)–197. Published November 26, 2001. DOI: 10.6028/NIST.FIPS.197

9. Daemen J., Rijmen V. The design of Rijndael. AES – The Advanced Encryption Standard. B.: Springer, 2002. 238 p. DOI: 10.1007/978-3-662-04722-4

10. Murphy S., Robshaw M.J.B. Essential algebraic structure within the AES. *Advances in cryptology – CRYPTO 2002: 22nd Annual intern. cryptology conf.* (Santa Barbara, CA, USA, August 18-22, 2002): Proc. B.: Springer, 2002. Pp. 1–16. DOI: 10.1007/3-540-45708-9_1