Math-Net.Ru

Общероссийский математический портал

А. В. Бухман, О свойствах полиномов периодических функций и сложности распознавания периодичности по полиному булевой функции, *Дискрет. матем.*, 2014, том 26, выпуск 1, 21–31

DOI: <https://doi.org/10.4213/dm1265>

Использование Общероссийского математического портала Math-Net.Ru подразумевает, что вы прочитали и согласны с пользовательским соглашением
<http://www.mathnet.ru/rus/agreement>

Параметры загрузки:

IP: 54.174.149.18

26 апреля 2023 г., 04:02:24

О свойствах полиномов периодических функций и сложности распознавания периодичности по полиному булевой функции

© 2014 г. А. В. Бухман¹

В статье исследуется вопрос об алгоритмической сложности распознавания периодичности булевых функций, заданных полиномами. Функция называется периодической с периодом τ , если она не изменяется при подстановке вместо всех переменных, соответствующих 1 в векторе τ , их отрицаний. Построено два полиномиальных алгоритма проверки того, что заданный вектор является периодом булевой функции. Исследована связь периода функции и длины её полинома. Построено в явном виде полиномиальное сведение задачи о поиске периода к решению системы булевых уравнений.

Работа выполнена при поддержке Российского фонда фундаментальных исследований, проект 13-01-00684.

Ключевые слова: булевы функции, распознавание периодичности, полиномиальные алгоритмы.

1. Введение

Настоящая работа относится к направлению теории булевых функций, которое посвящено исследованию сложности распознавания свойств этих функций. В общем случае задачу можно поставить так: требуется построить эффективный алгоритм, который для булевой функции, поданной ему на вход в виде полинома, определял бы, обладает ли эта функция заданным свойством. При такой постановке проверка большинства свойств, используемых на практике, непосредственно по определению имеет экспоненциальную временную алгоритмическую сложность относительно размера входных данных, то есть размера символической записи полинома. Запись функции в виде полинома выбрана по ряду причин. Каждая булева функция $f(x_1, \dots, x_n)$ может быть задана единственным полиномом Жегалкина. Полиномиальное задание функций часто используется на практике, например, в криптографии [3].

В данной статье рассматривается вопрос о сложности распознавания периодичности булевой функции, заданной полиномом. Здесь будут продолжены исследования, касающиеся распознавания свойств дискретных функций, заданных в некото-

¹Место работы: МГУ им. М. В. Ломоносова
e-mail: antvbx@gmail.com

рой канонической форме. Интересные результаты в этих исследованиях были получены ранее С.Н. Селезневой [1], С.П. Горшковым [2]. В частности, этими авторами были найдены полиномиальные алгоритмы для распознавания ряда важных с точки зрения приложений свойств булевых функций.

В данной работе рассматривается свойство периодичности булевой функции. Функция называется периодической с периодом τ , если она не изменяется при подстановке вместо переменных, соответствующих 1 в векторе τ , их отрицаний. Данное свойство имеет важное значение для задач криптографии. Периодические функции являются функциями, *обладающими линейной структурой*. В [3] отмечено, что наличие у отображения нетривиальных линейных структур свидетельствует об определённых слабостях этого отображения. Построен полиномиальный алгоритм для проверки того, является ли вектор τ периодом функции, заданной полиномом; набор τ и полином функции являются входными параметрами алгоритма. Также в статье построено в явном виде сведение задачи поиска всех периодов функции к решению системы булевых уравнений.

2. Основные определения

Введём основные понятия, которые будут использоваться далее в тексте статьи.

Определение 1. Пусть $E_2 = \{0, 1\}$. Булевой функцией, зависящей от n переменных, будем называть любое отображение вида $f : E_2^n \rightarrow E_2$.

Рассматривается задание функций в виде полиномов.

Определение 2. Мономом (или монотонной элементарной конъюнкцией) над переменными $x_1, \dots, x_n$ называется любое выражение вида $x_{i_1} \dots x_{i_l}$, где $l \geq 1$, $1 \leq i_1, \dots, i_l \leq n$, все переменные различны; 1 также называется мономом.

Равенство мономов рассматривается с точностью до перестановки сомножителей.

Определение 3. Полиномом называется сумма по модулю 2 конечного числа различных мономов или 0 (можно понимать как сумму нулевого числа мономов). Символом $\oplus$ будем обозначать сумму по модулю 2. Длиной полинома называется число его слагаемых. Длину нулевого полинома будем считать равной 0.

Полином Жегалкина булевой функции f (её представление в виде полинома) будем обозначать Π_f .

Равенство полиномов рассматривается с точностью до перестановки слагаемых.

Введём обозначение K_α для монома $x_{i_1} \dots x_{i_l}$, соответствующего набору $\alpha = (\alpha_1, \dots, \alpha_n)$, переменная x_{i_j} входит в этот моном тогда и только тогда, когда $\alpha_{i_j} = 1$.

Индексом $\text{ind}(K)$ монома $K = x_{i_1} \dots x_{i_l}$ будем называть множество $\{x_{i_1}, \dots, x_{i_l}\}$.

Введём частичный порядок на множестве наборов из E_2^n . Для двух наборов $\alpha = (\alpha_1, \dots, \alpha_n), \beta = (\beta_1, \dots, \beta_n) \in E_2^n$ будем писать $\alpha \leq \beta$, если $\alpha_1 \leq \beta_1, \dots, \alpha_n \leq \beta_n$. Введём частичный порядок на множестве мономов от переменных $x_1, \dots, x_n : K_\alpha \leq K_\beta$, если $\alpha \leq \beta$. Будем писать $K_\alpha < K_\beta$, если $K_\alpha \leq K_\beta$ и мономы K_α, K_β не равны. Для монома K и полинома Π будем писать $K \in \Pi$, если K является слагаемым полинома Π .

Пусть $f(x_1, \dots, x_n)$ – булева функция и $\tau \in E_2^n, \tau = (\tau_1, \dots, \tau_n)$, где $\tau_i \in E_2$. Функцию $f(x_1 \oplus \tau_1, \dots, x_n \oplus \tau_n)$ для краткости далее в статье будет обозначать

$f(x \oplus \tau)$. Пусть K – некоторый моном, обозначим через $K \setminus K_\alpha$ такой моном, что $\text{ind}(K \setminus K_\alpha) = \text{ind}(K) \setminus \text{ind}(K_\alpha)$.

Пусть $K = x_{i_1} \dots x_{i_k}$ – моном над переменными $x_1, \dots, x_n$ и $\tau \in E_2^n, \tau = (\tau_1, \dots, \tau_n)$. Пусть $\Pi_{K(x \oplus \tau)}$ – полином функции $(x_{i_1} \oplus \tau_{i_1}) \dots (x_{i_k} \oplus \tau_{i_k})$.

Введём определение периодической булевой функции согласно [4].

Определение 4. Булева функция f называется *периодической с периодом τ* , если $f(x \oplus \tau) = f(x)$.

Для всякого набора $\alpha \in E_2^n$ определим его *тень*

$$s(\alpha) = \{\beta \in E_2^n \mid \beta < \alpha, |\beta| = |\alpha| - 1\},$$

где $|\alpha|$ – число единиц в наборе α . Для множества наборов T тень определяется следующим образом:

$$s(T) = \bigcup_{\alpha \in T} s(\alpha).$$

Для оценки сложности алгоритмов нам потребуется описать алгоритмическую модель. В силу специфики решаемой задачи удобно будет использовать RAM машину, она подробно описана в книге [8]. При этом мы не будем записывать алгоритмы в виде явных программ для RAM машины, потому что эти программы получаются громоздкими и не наглядными. Вместо этого, как и в работах [1, 2], мы будем описывать алгоритмы в терминах некоторых простейших процедур RAM машины (например, перемножение мономов, поиск среди мономов наименьшего и т.д.), которые без труда могут быть реализованы читателем при необходимости.

3. Полиномиальный алгоритм проверки периодичности функции

Сформулируем два предложения, на которые будем в дальнейшем ссылаться. Доказательства этих предложений опущены, так как они не вызывают затруднений.

Предложение 1. Для произвольного монома K над переменными $x_1, \dots, x_n$ и набора $\gamma \in E_2^n$ полином $\Pi_{K(x \oplus \gamma)}$ содержит слагаемое $K^* < K$ тогда и только тогда, когда $\text{ind}(K) \setminus \text{ind}(K^*) \subseteq \text{ind}(K_\gamma)$.

Предложение 2. Пусть f – периодическая булева функция с периодом τ и K^* – произвольный моном. Тогда число слагаемых K полинома функции f , обладающих свойствами

$$- K^* < K$$

$$- \text{ind}(K) \setminus \text{ind}(K^*) \subseteq \text{ind}(K_\tau),$$

чётно (например, равно 0).

Пусть τ – период функции f , моном K – некоторое слагаемое полинома Π_f . Пусть моном K'' является слагаемым полинома $\Pi_{K(x \oplus \tau)}$. В силу предложения 2 найдётся нечётное число слагаемых K' отличных от K и таких, что $K'' \in \Pi_{K'(x \oplus \tau)}$. Заметим,

что $\text{ind}(K') \cap \text{ind}(K) \supseteq \text{ind}(K'')$ для всех таких слагаемых K' . На самом деле выполняется более строгое условие: среди таких K' будет нечётное число слагаемых K^* , для которых $K^* \cap K = K''$. Это формально доказано в лемме 1. Но прежде чем перейти к доказательству, отметим, что условие $K^* \in \Pi_{K(x \oplus \tau)}$ равносильно двум условиям $K > K^*$ и $\text{ind}(K) \setminus \text{ind}(K^*) \subseteq \text{ind}(K_\tau)$.

Лемма 1. Пусть f – булева функция, зависящая от n переменных, и $\tau \in E_2^n$ – период этой функции. Для любого слагаемого K полинома Π_f и любого набора γ : $K > K_\gamma > K \setminus K_\tau$ и в полиноме Π_f нет слагаемых $K' : K > K' > K_\gamma$, выполняется следующее условие: в полиноме Π_f содержится нечётное число слагаемых K^* , для которых $\text{ind}(K) \cap \text{ind}(K^*) = \text{ind}(K_\gamma)$ и $\text{ind}(K^*) \setminus \text{ind}(K_\gamma) \subseteq \text{ind}(K_\tau)$.

Доказательство. Доказательство проведём индукцией по $r = |\text{ind}(K)| - |\text{ind}(K_\gamma)|$.

База индукции: $r = 1$. Введём обозначения для множеств, которые нам потребуются для доказательства:

$$\mathcal{K}_\gamma = \{K^* \in \Pi_f \mid K^* > K_\gamma, \text{ind}(K^*) \setminus \text{ind}(K_\gamma) \subseteq \text{ind}(K_\tau)\},$$

$$\mathcal{K}_K = \{K^* \in \Pi_f \mid K^* \geq K, \text{ind}(K^*) \setminus \text{ind}(K) \subseteq \text{ind}(K_\tau)\},$$

$$\mathcal{K}_{K,\gamma} = \{K^* \in \Pi_f \mid \text{ind}(K) \cap \text{ind}(K^*) = \text{ind}(K_\gamma), \text{ind}(K^*) \setminus \text{ind}(K_\gamma) \subseteq \text{ind}(K_\tau)\}.$$

Чтобы доказать лемму надо доказать, что $|\mathcal{K}_{K,\gamma}|$ есть нечётное число.

Нетрудно показать, что имеет место равенство

$$\mathcal{K}_\gamma = \mathcal{K}_K \cup \mathcal{K}_{K,\gamma}, \quad (1)$$

кроме того, $\mathcal{K}_K \cap \mathcal{K}_{K,\gamma} = \emptyset$.

База индукции будет доказана, если мы покажем, что мощность множества $\mathcal{K}_{K,\gamma}$ нечётна.

Множество $\mathcal{K}_\gamma$ содержит чётное число элементов в силу предложения 2.

Полином $\Pi_{f(x \oplus \tau)}$ в силу того, что τ является периодом функции f , содержит слагаемое K . Заметим, что в силу предложения 2 мощность множества

$$\{K^* \in \Pi_f \mid K^* > K, \text{ind}(K^*) \setminus \text{ind}(K) \subseteq \text{ind}(K_\tau)\}$$

есть чётное число. И полином Π_f содержит слагаемое K . Тогда множество $\mathcal{K}_K$ содержит нечётное число элементов. Учитывая, что множества $\mathcal{K}_{K,\gamma}, \mathcal{K}_K$ не пересекаются и верно равенство (1), заключаем, что $|\mathcal{K}_{K,\gamma}| = |\mathcal{K}_\gamma| - |\mathcal{K}_K|$ – нечётное число.

Утверждение для $r = 1$ доказано.

Пусть утверждение верно для $r \leq t$, докажем его для $r = t + 1$.

Рассмотрим такое слагаемое K^* полинома Π_f , что полином $K^*(x \oplus \tau)$ содержит слагаемое K_γ . Пусть β – такой набор, что $\text{ind}(K_\beta) = \text{ind}(K^*) \cap \text{ind}(K)$. Тогда $K \geq K_\beta \geq K_\gamma$ и $\text{ind}(K^*) \setminus \text{ind}(K_\beta) \subseteq \text{ind}(K_\tau)$. Обозначим через $\mathcal{K}_{K,\beta}$ множество тех слагаемых полинома K^* , для которых $\text{ind}(K_\beta) = \text{ind}(K^*) \cap \text{ind}(K)$ и $\text{ind}(K^*) \setminus \text{ind}(K_\beta) \subseteq \text{ind}(K_\tau)$. Множество $\mathcal{K}_\gamma$ таких слагаемых K' полинома Π_f , что $\text{ind}(K') \setminus K_\gamma \subseteq \text{ind}(K_\tau)$, в силу предложения 2 имеет чётную мощность. Кроме того, нетрудно проверить, что выполнено равенство

$$\mathcal{K}_\gamma = \mathcal{K}_K \cup \bigcup_{\beta: K_\gamma \leq K_\beta < K} \mathcal{K}_{K,\beta}.$$

Множества $\mathcal{K}_{K,\beta}$, соответствующие разным β , не пересекаются. Следовательно,

$$|\mathcal{K}_{K,\gamma}| = |\mathcal{K}_\gamma| - \left(\sum_{\beta: K_\gamma < K_\beta < K} |\mathcal{K}_{K,\beta}| \right) - |\mathcal{K}_K|.$$

Для всех таких наборов β , что $K \geq K_\beta > K_\gamma$, выполнено предположение индукции, то есть мощность множества $\mathcal{K}_{K,\beta}$ – нечётное число. Различных β , удовлетворяющих условию $K \geq K_\beta > K_\gamma$, нечётное число, а именно, $2^{t+1} - 1$. Значит, мощность множества $\mathcal{K}_{K,\gamma}$ есть нечётное число, что завершает доказательство леммы.

Следствие 1. Пусть функция f – периодическая и τ – её период. Тогда для каждого монома $K \in \Pi_f$ множество мономов K_γ , удовлетворяющих условиям

1) $K > K_\gamma > K \setminus K_\tau$,

2) ни один из мономов $K' : K > K' > K_\gamma$, не является слагаемым полинома Π_f содержит не более l элементов, где l – длина полинома функции f .

Доказательство. Для множества, описанного в следствии 1, введём обозначение $\mathcal{K}'$. В лемме 1 при фиксированном $K \in \Pi_f$ для каждого слагаемого $K_\gamma \in \mathcal{K}'$ было построено множество, состоящее из слагаемых полинома, которое обозначалось через $\mathcal{K}_{K,\gamma}$.

Из доказательства леммы 1 можно сделать вывод, что для любого $K_\gamma \in \mathcal{K}'$ верно соотношение $|\mathcal{K}_{K,\gamma}| \geq 1$, следовательно,

$$|\mathcal{K}'| = \sum_{\gamma: K_\gamma \in \mathcal{K}'} 1 \leq \sum_{\gamma: K_\gamma \in \mathcal{K}'} |\mathcal{K}_{K,\gamma}|. \quad (2)$$

Ещё в доказательстве леммы 1 было отмечено, что $\mathcal{K}_{K,\gamma_1} \cap \mathcal{K}_{K,\gamma_2} = \emptyset$ для различных $K_{\gamma_1}, K_{\gamma_2} \in \mathcal{K}'$. Значит, верно соотношение:

$$\sum_{\gamma: K_\gamma \in \mathcal{K}'} |\mathcal{K}_{K,\gamma}| \leq l. \quad (3)$$

Объединяя вместе (2) и (3), получаем $|\mathcal{K}'| \leq l$.

Замечание 1. Пусть f – периодическая функция, τ – её период, и моном $K \in \Pi_f$. Тогда длина полинома $\Pi_{K(x \oplus \tau)}$ не превосходит l^2 (где l – длина полинома функции f).

Доказательство. Пусть K' такое слагаемое полинома Π_f , что $K' \in \Pi_{K(x \oplus \tau)}$. Каждому такому слагаемому можно поставить в соответствие множество всевозможных мономов от n переменных, обладающих свойствами, описанными в условии следствия 1. Эти множества не будут попарно пересекаться и в объединении дадут всё множество слагаемых полинома $\Pi_{K(x \oplus \tau)}$. В каждом множестве, в силу следствия 1, не более l слагаемых, и всего множеств не более l . Получаем, что число слагаемых полинома $\Pi_{K(x \oplus \tau)}$ не превосходит l^2 .

Возможность построения полиномиального алгоритма для задачи проверки того, является ли заданный вектор τ периодом функции, заданной полиномом, следует из замечания 1.

Утверждение 1. *Существует RAM машина, которая получив на вход запись полинома булевой функции f и набора τ из нулей и единиц, определяет за полиномиальное время, является ли τ периодом f .*

Доказательство. Алгоритм состоит из следующих шагов.

У1. Проверяем, что для каждого слагаемого K полинома Π_f полином $\Pi_{K(x \oplus \tau)}$ содержит не больше l^2 слагаемых, где l – длина полинома Π_f . Если хотя бы для одного слагаемого это условие нарушается, то τ , согласно замечанию 1, не может быть периодом функции. Алгоритм завершает свою работу и выдаёт ответ НЕТ.

У2. Вычисляем полином $\Pi_{f(x \oplus \tau)}$. Для этого сначала для каждого слагаемого $K \in \Pi_f$ находим полином $\Pi_{K(x \oplus \tau)}$. Мы получим полином с не более, чем l^3 слагаемыми. В полученном полиноме приведём подобные слагаемые. Данное действие займёт $O(N^6)$ шагов RAM машины ($N = ln$, где l – длина полинома функции f , n – число переменных). Сравним полученный полином с исходным. Если они совпадают, то τ является периодом функции, иначе – нет.

Далее приведём более быстрый алгоритм.

Алгоритм 1:

Шаг 1. Полагаем K равным первому слагаемому полинома.

Шаг 2. Перебираем все такие мономы K' , что $K \geq K' \geq K \setminus K_\tau$ и не существует слагаемого $\hat{K} \in \Pi_f : K > \hat{K} \geq K'$. Если окажется, что таких K' больше l , то завершаем работу алгоритма, выдаём ответ НЕТ, в противном случае выполняем Шаг 3.

Шаг 3. Для всех K' , найденных на шаге 2, проверяем количество слагаемых полинома $K^* \in \Pi_f : K^* > K' \geq K^* \setminus K_\tau$ и $\text{ind}(K^*) \setminus \text{ind}(K') \subseteq K_\tau$. Если это условие не выполнено, то завершаем работу алгоритма и выдаём ответ НЕТ. Иначе переходим к шагу 4.

Шаг 4. Проверяем, является ли K последним слагаемым полинома Π_f . Если это так, то завершаем алгоритм и выдаём ответ ДА. Если нет, то берём следующее за K слагаемое полинома Π_f . Полагаем K равным выбранному слагаемому. Переходим к шагу 2.

Теорема 1. *Алгоритм 1 выдаёт ответ ДА, когда функция f – периодическая с периодом τ . И ответ НЕТ, когда f не является периодической с периодом τ .*

Доказательство. Покажем, что алгоритм 1 выдаёт ответ ДА тогда и только тогда, когда поданный на вход полином задаёт функцию, периодическую с периодом τ .

Если алгоритм выдаёт ответ ДА, то $\Pi_f = \Pi_{f(x \oplus \tau)}$. Полином $\Pi_{f(x \oplus \tau)}$ может содержать только такие слагаемые K' , что $K \geq K' \geq K \setminus K_\tau$, где K – есть некоторое слагаемое полинома Π_f . Так как алгоритм выдаёт ответ ДА, то все мономы вида K' проверены и для них $K' \in \Pi_f$ тогда и только тогда, когда $K' \in \Pi_{f(x \oplus \tau)}$.

Если алгоритм выдал ответ НЕТ, то возможны 2 случая:

1. Нашлось такое слагаемое полинома $K \in \Pi_f$, что количество мономов, удовлетворяющих условиям шага 2, больше либо равно l . Такая функция не будет периодической по следствию 1.

2. Для некоторого слагаемого $K \in \Pi_f$ нашёлся такой моном K^* , что $K \geq K^* \geq K \setminus K_\tau$ и для K^* нарушено условие шага 3. Это равносильно тому, что полином функции $f(x \oplus \tau) \oplus f(x)$ содержит слагаемое K^* .

Теорема 2. *Сложность алгоритма 1 есть $O(N^3)$.*

Доказательство. В алгоритме мы для каждого слагаемого полинома, поданного на вход, проделываем шаги 2 и 3. Опишем более подробно, как выполнять перебор мономов K' на шаге 2.

У нас есть слагаемое полинома K . Рассмотрим булев куб, состоящий из мономов $K' : K \geq K' \geq K \setminus K_\tau$. Поставим этому кубу в соответствие граф. Будем обходить этот граф в глубину из вершины, соответствующей K (алгоритмы обхода в глубину описаны, например, в [9]).

Для каждой посещаемой вершины будем проверять условия шага 2 алгоритма 1: если они выполнены, то будем говорить, что вершина имеет тип 1, иначе она имеет тип 2. Если мы встретили вершину типа 2, то мы не обходим её потомков, а возвращаемся к её предку и продолжаем обход. Все вершины типа 2 лежат в тени множества вершин типа 1. А количество вершин типа 1, которые мы проверим согласно шагу 2, не более l . Значит, вершин типа 2 мы обошли не более, чем ln . В итоге действия шагов 2 и 3 алгоритма 1 мы выполняем для не более чем $l(n+1)$ вершины.

Для каждого слагаемого K' проверка условий шагов 2 и 3 требует $O(N)$ действий. Итак, для каждого из l слагаемых полинома мы проверяем на шагах 2 и 3 не более $l(n+1)$ вершин и для каждой вершины мы выполняем $O(N)$ шагов RAM-машины. В итоге получаем сложность $O(N^3)$.

4. Сведение задачи о поиске периода функции к решению системы уравнений

В предыдущем разделе речь шла о построении алгоритма для проверки того, что заданный набор τ является периодом функции. Таким образом, вектор τ должен подаваться на вход (то есть быть известен до начала работы алгоритма), что накладывает дополнительные ограничения. В связи с этим возникает вопрос: какова сложность алгоритма, который получив на вход функцию в виде полинома, выдал бы ответ, есть ли у неё какой-то период. Или ещё более общий вопрос: какова сложность алгоритма, который, получив на вход полином булевой функции, выдавал бы на выходе все её периоды.

В данном разделе мы займёмся построением алгоритма, который будет находить все возможные периоды функции. Точнее, основной результат – явное полиномиальное сведение задачи о поиске всех периодов функции к задаче решения системы булевых уравнений. То есть для каждой функции будет построена система уравнений, каждое ненулевое решение которой является периодом функции, и обратно: любой период функции является решением системы. Причем сложность этого построения и размер получающейся системы уравнений полиномиальны относительно длины записи полинома Жегалкина исходной функции.

Задача решения систем булевых уравнений активно исследовалась. Подходы к решению данной задачи освещены в ряде монографий (например, [5, 3]), кроме того, для её решения есть большое количество достаточно быстрых на практике эвристических методов и программных продуктов [6, 7].

Для набора $\alpha \in E_2^n$ и функции f запишем уравнение, которое мы будем обозначать T_f^α ,

$$\bigoplus_{K \in \Pi_f : K > K_\alpha} K \setminus K_\alpha = 0.$$

Утверждение 2. Пусть $\alpha \in E_2^n$, f – булева функция, зависящая от n переменных. Если полином функции f содержит слагаемое K_α , то полином функции $f(x \oplus \tau)$ содержит слагаемое K_α тогда и только тогда, когда уравнение T_f^α выполнено на наборе τ .

Если полином функции f не содержит слагаемого K_α , то полином функции $f(x \oplus \tau)$ содержит слагаемое K_α тогда и только тогда, когда T_f^α не выполнено на наборе τ .

Доказательство. Пусть $K > K_\alpha$. Заметим, что моном $K \setminus K_\alpha$ обращается в 1 на наборе τ тогда и только тогда, когда полином $\Pi_{K(x \oplus \tau)}$ содержит слагаемое K_α . Тогда левая часть уравнения T_f^α обращается в 0, если в полиноме $\Pi_{f(x \oplus \tau)}$ есть чётное число таких слагаемых $K > K_\alpha$, что полином $\Pi_{K(x \oplus \tau)}$ содержит слагаемое K_α . Тогда, если исходный полином содержит моном K_α , то $\Pi_{f(x \oplus \tau)}$ содержит K_α тогда и только тогда, когда уравнение T_f^α выполнено на наборе τ . Аналогично выводится и второй пункт утверждения.

Будем обозначать через T_f систему уравнений $\{T_f^\alpha, \alpha \in Q\}$, где $Q = \{\alpha \in E_2^n | \exists K \in \Pi_f : K > K_\alpha\}$.

Теорема 3. Пусть f – булева функция от n переменных. Тогда любое ненулевое решение системы T_f является периодом функции f , и обратно, если τ – период функции f , то он является решением системы T_f .

Доказательство. Пусть τ – период функции f . Покажем, что для любого $\alpha \in Q$ уравнение T_f^α обращается в равенство на наборе τ . В силу утверждения 1 выполнение уравнения T_f^α на наборе τ равносильно тому, что $K_\alpha \in \Pi_f$ тогда и только тогда, когда $K_\alpha \in \Pi_{f(x \oplus \tau)}$. А так как функция f периодическая с периодом τ , последняя эквивалентность справедлива.

Пусть τ – решение системы T_f . Покажем, что при этом условия полиномы Π_f и $\Pi_{f(x \oplus \tau)}$ совпадают. Пусть K – некоторый моном от переменных $x_1, \dots, x_n$. Для него справедливо одно из следующих трёх условий:

1. Не существует такого слагаемого $K' \in \Pi_f$, что $K' \geq K$. Такой моном не входит в состав полинома Π_f и одновременно не входит в $\Pi_{f(x \oplus \tau)}$.

2. Моном K является слагаемым полинома Π_f , и не существует $K' \in \Pi_f : K' > K$. Такой моном входит в оба полинома Π_f и $\Pi_{f(x \oplus \tau)}$.

3. Существует $K' \in \Pi_f$ такое, что $K' > K$. Тогда возьмём такой набор α , что $K_\alpha = K$. На основании утверждения 1 выполнение уравнения T_f^α на наборе τ влечёт за собой эквивалентность: $K \in \Pi_f$ тогда и только тогда, когда $K \in \Pi_{f(x \oplus \tau)}$.

Теорема 3 сводит задачу о нахождении всех периодов функции f к решению системы уравнений. Однако система T_f^α может содержать экспоненциальное, относительно длины записи полинома, количество уравнений. Чтобы показать это, построим последовательность функций и посчитаем число уравнений в соответствующей последовательности систем уравнений. Рассмотрим последовательность функций $\{g_s(x_1, \dots, x_{2^s-1}) = x_1 \oplus x_2 x_3 \oplus \dots \oplus x_{2^{s-1}} \dots x_{2^s-1}\}$, $s = 2, 3, 4, \dots$. Система T_{g_s} содержит уравнения $T_{g_s}^\beta$ для β таких, что $K_\beta \leq x_{2^{s-1}} \dots x_{2^s-1}$, то есть в этой системе более 2^{2^s-1} уравнений, при этом полином исходной функции содержит s слагаемых и зависит от $2^s - 1$ переменных. Далее будет рассмотрен вопрос об упрощении системы T_f .

Пусть $f \in P_2^n$. Опишем вспомогательное множество $H'_f \subset E_2^n$. Оно состоит из всех наборов $\gamma \in E_2^n$, для которых существуют такие $K', K'' \in \Pi_f$ и $K' \neq K''$, что $\text{ind}(K_\gamma) = \text{ind}(K') \cap \text{ind}(K'')$. Пусть $\tilde{\Pi}_f$ – подмножество E_2^n , состоящее из всех наборов, соответствующих слагаемым полинома Π_f . Выберем $H = H' \cup \tilde{\Pi}_f$. Положим $H^+ = s(H) \cup H$, где $s(H)$ – тень множества H .

Утверждение 3. Пусть $f \in P_2^n$, и моном K_β таков, что $\beta \notin H^+$ и существует $K' \in \Pi_f : K' > K_\beta$. Тогда найдётся такое $\alpha \in H^+ \setminus H$, что $K < K_\alpha < K'$.

Фактически в утверждении говорится, что если взять некоторое множество булева куба и произвольный элемент β , меньший некоторого элемента множества, то в тени этого множества найдётся элемент α , который будет больше, чем β . Доказательство утверждения 3 не вызывает затруднений, поэтому опущено.

Рассмотрим систему уравнений, состоящую из уравнений T_f^α , где $\alpha \in H^+$. Эту систему уравнений для функции f мы будем обозначать T_f^+ . Система T_f^+ содержит не более $(l^2 + l)(n + 1)$ уравнений. Таким образом, длина записи получившейся системы не превосходит полинома от длины записи полинома функции f .

Лемма 2. Пусть K_α – слагаемое полинома Π_f , наборы γ, τ таковы, что моном $K_\alpha \setminus K_\gamma$ обращается в 1 на наборе τ . Кроме того, для любого такого набора β , что $K_\alpha > K_\beta \geq K_\gamma$ моном K_β не является слагаемым полинома Π_f , и выполнены все уравнения T_f^β и уравнение T_f^α на наборе τ . Тогда мощность множества таких слагаемых K' полинома Π_f , что $K' \setminus K_\gamma$ равно 1 на наборе τ и $\text{ind}(K_\alpha) \cap \text{ind}(K') = \text{ind}(K_\gamma)$, нечетна.

Доказательство. Проведём доказательство индукцией по разности $|\alpha| - |\gamma|$

Базис: $|\alpha| - |\gamma| = 1$.

Обозначим через $\mathcal{K}_{\beta, K}$ множество таких слагаемых K^* полинома Π_f , что

- $\text{ind}(K^*) \cap \text{ind}(K) = \text{ind}(K_\beta)$;
- $K^* \setminus K_\beta$ обращается в 1 на наборе τ .

Обозначим через $\mathcal{K}_\beta$ множество таких слагаемых $K^* > K_\beta$ полинома Π_f , что моном $K^* \setminus K_\beta$ обращается в 1 на наборе τ

Нетрудно проверить, что $\mathcal{K}_\gamma = \{K_\alpha\} \cup \mathcal{K}_\alpha \cup \mathcal{K}_{K, \gamma}$. Три множества, стоящие в правой части равенства, не пересекаются, поэтому

$$|\mathcal{K}_{K, \gamma}| = |\mathcal{K}_\gamma| - |\mathcal{K}_\alpha| - 1.$$

Множество $\mathcal{K}_\alpha$ имеет чётное число элементов в силу того, что выполнено уравнение T_f^α . Множество $\mathcal{K}_\gamma$ имеет чётное число элементов в силу того, что выполнено уравнение T_f^γ . Следовательно, множество $\mathcal{K}_{K, \gamma}$ состоит из нечётного числа элементов.

Шаг индукции.

Пусть утверждение доказано для всех γ , удовлетворяющих условиям леммы и таких, что $|\alpha| - |\gamma| < s$. Докажем утверждение для всех γ , удовлетворяющих условиям теоремы и таких, что $|\alpha| - |\gamma| = s$. Для этого заметим, что справедливо соотношение

$$\mathcal{K}_\gamma = \mathcal{K}_\alpha \cup \bigcup_{\beta: K_\gamma \leq K_\beta < K_\alpha} \mathcal{K}_{K, \beta}.$$

Множества $\mathcal{K}_\alpha, \mathcal{K}_\gamma$ содержат чётное число элементов в силу того, что выполнены уравнения T_f^α, T_f^γ . Каждое множество $\mathcal{K}_{K,\beta}$ для всех $K_\gamma < K_\beta < K_\alpha$ содержит нечётное число элементов по предположению индукции. Так как

$$|\mathcal{K}_{K,\gamma}| = |\mathcal{K}_\gamma| - |\mathcal{K}_\alpha| - \sum_{\beta: K_\gamma \leq K_\beta < K_\alpha} |\mathcal{K}_{K,\beta}|,$$

то $|\mathcal{K}_{K,\gamma}|$ есть чётное число.

Теорема 4. Система T_f^+ эквивалентна системе T_f .

Доказательство. Для доказательства нам нужно показать, что всякое решение T_f^+ является решением T_f .

Пусть τ – решение T_f^+ , но не решение T_f . Тогда найдётся уравнение T_f^α в T_f , которое не выполнено для τ . Пусть K^* – такое слагаемое полинома функции f , что $K^* \setminus K_\alpha$ входит в уравнение T_f^α и на наборе τ моном $K^* \setminus K_\alpha$ обращается в 1 (такое слагаемое обязательно есть, так как на наборе τ не выполняется уравнение T_f^α). Из определения $K \setminus K_\alpha$ следует, что $K^* > K_\alpha$.

Выберем, в соответствии с утверждением 3, такой набор $\gamma \in H^+ \setminus H$, что $K^* > K_\gamma > K_\alpha$. Без ограничения общности можно считать, что K^* – минимальное из таких слагаемых, то есть нет таких $K' \in P_f$, что $K^* > K' > K_\gamma$.

Покажем, что хотя бы на одном из таких наборов β , что $K^* > K_\beta \geq K_\gamma$, нарушается уравнение T_f^β на наборе τ . Этот факт будет доказан, если мы докажем импликацию: если для всех таких наборов β , что $K^* > K_\beta > K_\gamma$, уравнения выполняются, то уравнение T_f^γ нарушается на наборе τ .

Данную импликацию будем доказывать от противного. Предположим, что T_f^γ выполнено на наборе τ . Тогда для наборов γ, τ и монома K^* выполнены все условия леммы 2. Следовательно, найдётся такое слагаемое K' , что $K' \setminus K_\gamma$ равно 1 на наборе τ и

$$\text{ind}(K') \cap \text{ind}(K^*) = \text{ind}(K_\gamma). \quad (4)$$

Пришли к противоречию, так как $\gamma \notin H$, а значит, не может существовать такое K' , что выполнено (4). Полученное противоречие завершает доказательство теоремы.

Список литературы

1. Селезнева С.Н., О сложности распознавания полноты множества булевых функций, реализованных полиномами Жегалкина. *Дискретная математика* (1997) **9**, №4, 24–31.
2. Горшков С.П., О сложности распознавания мультиаффинности, бижонктивности, слабой положительности и слабой отрицательности булевой функции. *Обозр. прикл. и промышл. матем. Сер. Дискр. матем.* (1997) **4**, №2, 216–237.
3. Логачев О., Сальников А., Смышляев С., Яценко В., *Булевы функции в теории кодирования и криптологии* (2-е изд., дополн., ред.). МЦНМО, Москва, 2012.
4. Леонтьев В.К., О некоторых задачах, связанных с булевыми полиномами. *Журнал вычислительной математики и математической физики* (1999) **9**, №6, 1045–1054.
5. Bard G., *Algebraic Cryptanalysis*, ISBN: 978-0-387-88756-2. Springer, 2009.
6. Bettale L., Faugere J., Perret L., Hybrid approach for solving multivariate systems over finite fields. *In Journal of Mathematical Cryptology* (2009) **3**, 177–197.

7. Wolf C., Thomae E., Small Linearization: Memory Friendly Solving of Non-Linear Equations over Finite Fields. *IACR Cryptology ePrint Archive* (2011 669–669).
8. Ахо А., Хопкофт Дж., Ульман Дж., *Построение и анализ вычислительных алгоритмов*. Мир, Москва, 1979.
9. Кормен Т., Лейзерсон Ч., Ривест Р., Штайн К., *Алгоритмы: построение и анализ = Introduction to Algorithms*. Вильямс, Москва, 2005.

Статья поступила 12.03.2013.