ПРИКЛАДНАЯ ДИСКРЕТНАЯ МАТЕМАТИКА

2014 Теоретические основы прикладной дискретной математики № 4(26)

DOI 10.17223/20710410/26/4

УДК 519.7

ВЗАИМОСВЯЗЬ КОЭФФИЦИЕНТОВ ПОЛИНОМА НАД ПОЛЕМ И ВЕСА БУЛЕВОЙ ФУНКЦИИ

А. С. Кузьмин, В. И. Ноздрунов

Лаборатория ТВП, г. Москва, Россия

E-mail: vlad_vin@mail.ru

Работа посвящена изучению зависимости коэффициентов многочлена одного переменного, задающего над полем из 2^n элементов булеву функцию, от веса исследуемой функции. Получены точные формулы зависимости коэффициентов многочлена от первых двух коэффициентов веса в двоичном представлении и ограничения на линейные многообразия функций из рассматриваемых специальных классов.

Ключевые слова: *булева функция, бент-функция, многочлен над полем, вес функции, подпространство, многообразия.*

Введение

В 70-х годах прошлого века был введён класс функций, находящихся на наибольшем расстоянии, с точки зрения метрики Хемминга, от класса аффинных функций; такие функции названы О. С. Ротхаузом бент-функциями [1]. В дальнейшем в работе [2] А. Йоссефом и Г. Гонгом построен класс функций, которые находятся на наибольшем расстоянии от мономиальных функций — класс гипер-бент-функций.

Несмотря на многочисленные исследования в этой области, пока не получено полного описания данных классов функций. Этим объясняется актуальность изучения свойств бент-функций и гипер-бент-функций и поиска новых методов их анализа.

При изложении результатов удобно использовать представление булевых функций от n переменных в виде многочленов над полем $\mathrm{GF}(2^n)$. Пусть $P = \mathrm{GF}(2)$ — поле из двух элементов, $Q = \mathrm{GF}(2^n)$ — расширение поля P степени n. Булевы функции $f(x_0, x_1, \ldots, x_{n-1})$ от n переменных можно рассматривать как функции вида $F : Q \to P$. Для простоты будем считать, что $f(0, 0, \ldots, 0) = 0$.

Обозначим через $\varepsilon_0, \varepsilon_1, \ldots, \varepsilon_{n-1}$ базис поля $\mathrm{GF}(2^n)$ как векторного пространства над полем $\mathrm{GF}(2)$, а через $\omega_0, \omega_1, \ldots, \omega_{n-1}$ — базис поля $\mathrm{GF}(2^n)$ над полем $\mathrm{GF}(2)$, двойственный к базису $\varepsilon_0, \varepsilon_1, \ldots, \varepsilon_{n-1}$, т. е.

$$\mathrm{tr}_1^n(\varepsilon_j\omega_k) = \begin{cases} 1, & \text{если } j = k, \\ 0, & \text{если } j \neq k, \end{cases}$$

где $\mathrm{tr}_1^n(x) = \sum\limits_{k=0}^{n-1} x^{2^k}$ — функция «след» из поля $\mathrm{GF}(2^n)$ в поле $\mathrm{GF}(2)$.

Тогда для любого набора булевых величин $x_0, x_1, \ldots, x_{n-1}$ однозначно определён элемент $x \in \mathrm{GF}(2^n)$:

$$x = \sum_{k=0}^{n-1} x_k\varepsilon_k.$$

При этом, в силу двойственности базисов, справедливо соотношение $x_k = \mathrm{tr}_1^n(\omega_k x)$. Таким образом, для булевой функции $f(x_0, x_1, \ldots, x_{n-1})$ имеет место равенство

$$f(x_0, x_1, \ldots, x_{n-1}) = f(\mathrm{tr}_1^n(\omega_0 x), \mathrm{tr}_1^n(\omega_1 x), \ldots, \mathrm{tr}_1^n(\omega_{n-1} x)),$$

задающее эту функцию в виде полинома над полем $\mathrm{GF}(2^n)$ в базисе $\varepsilon_0, \varepsilon_1, \ldots, \varepsilon_{n-1}$.

Обозначим $F(x) = f(\mathrm{tr}_1^n(\omega_0 x), \mathrm{tr}_1^n(\omega_1 x), \ldots, \mathrm{tr}_1^n(\omega_{n-1} x))$. Так как функция F представляется в виде многочлена над полем, то

$$F(x) = \sum_{k=1}^{2^n-1} c_k x^k, \; x \in Q. \tag{1}$$

Здесь коэффициенты c_k принадлежат полю $\mathrm{GF}(2^n)$. Заметим, что $c_0 = 0$, так как $F(0) = 0$, поэтому в формуле (1) сумма начинается с $k = 1$.

Поскольку многочлен $F(x)$ принимает только два значения 0 или 1, то он может быть представлен в виде

$$F(x) = \mathrm{tr}_1^n(\Phi(x)),$$

где $\Phi(x)$ — некоторый полином над полем $\mathrm{GF}(2^n)$. В работе [3] показано, что существует представление функции $F(x)$, в котором многочлен $\Phi(x)$ имеет вид

$$\Phi(x) = \sum_{k \in M} c'_k \xi_k x^k, \; c'_k \in Q_k, \; k \in M. \tag{2}$$

Здесь M — набор минимальных представителей всех различных циклотомических классов по модулю $2^n - 1$ [4, с. 108], $Q_k = \mathrm{GF}(2^r)$, где значение r определяется условиями $r = \min\left\{t : t > 0, \dfrac{2^n - 1}{(2^n - 1, k)} \big| (2^t - 1)\right\}$, а ξ_k — фиксированный элемент поля $\mathrm{GF}(2^n)$, след которого в подполе $\mathrm{GF}(2^r)$ равен 1.

Замечание 1. Из формул (1) и (2), а также из формулы $F(x) = \mathrm{tr}_1^n(\Phi(x))$ следует, что $c_k = c'_k \xi_k$, если $k \in M$. Отсюда следует также, что если $c'_k \xi_k = 0$, то $c_t = 0$ для всех таких t, что t и k лежат в одном циклотомическом классе.

1. Зависимости коэффициентов в представлении в виде многочлена над конечным полем от веса булевой функции

Рассмотрим задачу установления зависимости коэффициентов многочлена $F(x)$ от параметров двоичного разложения веса самой функции $||F|| = n_0 + 2n_1 + 4n_2 + \cdots$, где $n_i \in \{0, 1\}$. Под весом понимается сумма значений функции по всем аргументам, т. е. $||F|| = \sum\limits_{x \in Q} F(x)$, где суммирование ведётся в действительной области.

Утверждение 1. Коэффициент $c_{2^n-1} = 0$ тогда и только тогда, когда $n_0 = 0$.

Доказательство. Очевидно, что $n_0 = \sum\limits_{x \in Q} F(x)$, где суммирование ведётся в поле Q характеристики 2. Тогда

$$n_0 = \sum_{x \in Q} \sum_{k=1}^{2^n-1} c_k x^k.$$

Любой обратимый элемент x поля Q можно представить в виде θ^t для подходящего $t \in \{0, 1, \ldots, 2^n - 2\}$, где θ — примитивный элемент поля Q. Учитывая, что $c_0 = 0$, получаем

$$n_0 = \sum_{t=0}^{2^n-2} \sum_{k=1}^{2^n-1} c_k (\theta^t)^k.$$

Поменяем порядок суммирования и выделим слагаемое, соответствующее $k = 2^n - 1$:

$$n_0 = \sum_{k=1}^{2^n-2} c_k \sum_{t=0}^{2^n-2} (\theta^k)^t + c_{2^n-1} \sum_{t=0}^{2^n-2} (\theta^{2^n-1})^t.$$

Порядок θ равен $2^n - 1$, следовательно, вторая сумма при коэффициенте c_{2^n-1} есть суммирование единиц $2^n - 1$ раз; значит, она равна 1. Теперь, применяя формулу для вычисления суммы геометрической прогрессии, получаем равенство

$$n_0 = \sum_{k=1}^{2^n-2} c_k \frac{\theta^{k(2^n-1)} - 1}{\theta^k - 1} + c_{2^n-1} = c_{2^n-1}.$$

Таким образом, имеем, что $n_0 = 0$ тогда и только тогда, когда $c_{2^n-1} = 0$. ■

Лемма 1 [5]. Пусть $a_i \in \{0, 1\}$, $i \in \{1, 2, \ldots, n\}$ и $\sum\limits_{i=1}^{n} a_i = k = n_0 + 2n_1 + 4n_2 + \ldots$, где суммирование ведётся в области целых чисел. Тогда

$$n_1 = \sum_{1 \leqslant j < s \leqslant n} a_j a_s \pmod 2.$$

Теорема 1. Пусть $F : Q \to P$, $F(0) = 0$ и $||F|| = n_0 + 2n_1 + 4n_2 + \ldots$ Тогда

$$n_1 = c^2_{2^n-1} + \sum_{k=1}^{2^{n-1}-1} c_k c_{2^n-1-k}. \tag{3}$$

Доказательство. Зафиксируем примитивный элемент θ поля Q и аналогично тому, как было сделано в лемме 1, представим элементы поля Q через элемент θ. Пусть x и y — элементы поля Q, $x = \theta^k$, $y = \theta^l$, где k, l — натуральные числа. Будем считать, что $x < y$ тогда и только тогда, когда $k < l$. Согласно лемме 1, имеем

$$n_1 = \sum_{x_1, x_2 \in Q\ :\ x_1 < x_2} F(x_1)F(x_2) = \sum_{x_1 < x_2} \left(\sum_{k=0}^{2^n-1} c_k x_1^k \sum_{l=0}^{2^n-1} c_l x_2^l \right).$$

Так как $F(0) = 0$, то $c_0 = 0$ и справедливо соотношение

$$n_1 = \sum_{0 \leqslant s < t \leqslant 2^n-2} \left(\sum_{k=1}^{2^n-1} c_k (\theta^s)^k \sum_{l=1}^{2^n-1} c_l (\theta^t)^l \right).$$

Далее, поменяв порядок суммирования, будем иметь

$$n_1 = \sum_{k,l=1}^{2^n-1} \sum_{0 \leqslant s < t \leqslant 2^n-2} c_k c_l \theta^{sk+tl} =$$

$$= \sum_{k,l=1}^{2^n-1} c_k c_l \left(\sum_{s=0, 1 \leqslant t \leqslant 2^n-2} \theta^{tl} + \theta^k \sum_{s=1, 2 \leqslant t \leqslant 2^n-2} \theta^{tl} + \ldots + \sum_{s=2^n-3, t=2^n-2} \theta^{sk}\theta^{tl} \right).$$

Применим формулу геометрической прогрессии, выделив отдельно слагаемое, соответствующее $l = 2^n - 1$, так как при нём $\theta^l = 1$:

$$n_1 = \sum_{k=1}^{2^n-1} \sum_{l=1}^{2^n-2} c_k c_l \left(\frac{\theta^l(\theta^{(2^n-2)l} - 1)}{\theta^l - 1} + \ldots + \theta^{(2^n-3)k}\theta^{(2^n-2)l} \right) +$$

$$+ \sum_{k=1, (l=2^n-1)}^{2^n-1} c_k c_l \left(\sum_{1 \leqslant t \leqslant 2^n-2} 1 + \theta^k \sum_{2 \leqslant t \leqslant 2^n-2} 1 + \ldots + \theta^{(2^n-3)k} \right) =$$

$$= \sum_{k=1}^{2^n-1} \sum_{l=1}^{2^n-2} c_k c_l \frac{1}{\theta^l - 1} \sum_{i=1}^{2^n-2} \theta^{il}\theta^{(i-1)k} \left(\theta^{(2^n-1-i)l} - 1 \right) +$$

$$+ \sum_{k=1, (l=2^n-1)}^{2^n-1} c_k c_l \left((2^n - 2) + \theta^k(2^n - 3) + \ldots + \theta^{(2^n-3)k} \right).$$

Пусть

$$A=\sum_{k=1}^{2^n-1}\sum_{l=1}^{2^n-2}c_kc_l\frac{1}{\theta^l-1}\sum_{i=1}^{2^n-2}\theta^{il}\theta^{(i-1)k}\left(\theta^{(2^n-1-i)l}-1\right),$$

$$B=\sum_{k=1,\ (l=2^n-1)}^{2^n-1}c_kc_l\left((2^n-2)+\theta^k(2^n-3)+\ldots+\theta^{(2^n-3)k}\right).$$

Для A имеем

$$A=\sum_{k=1}^{2^n-1}\sum_{l=1}^{2^n-2}\frac{c_kc_l}{\theta^l-1}\sum_{i=1}^{2^n-2}\left(\theta^{l(i+2^n-1-i)+ik}\theta^{-k}-\theta^{(l+k)i}\theta^{-k}\right)=$$

$$=\sum_{k=1}^{2^n-1}\sum_{l=1}^{2^n-2}\frac{c_kc_l}{(\theta^l-1)\theta^k}\sum_{i=1}^{2^n-2}\theta^{ik}-\sum_{k=1}^{2^n-1}\sum_{l=1}^{2^n-2}\frac{c_kc_l}{(\theta^l-1)\theta^k}\sum_{i=1}^{2^n-2}\theta^{(l+k)i}.$$

Снова посчитаем суммы по отдельности, первую обозначим A_1, а вторую — A_2:

$$A_1=\sum_{k,\ l=1}^{2^n-2}\frac{c_kc_l}{\theta^l-1}\frac{\theta^{(2^n-2)k}-1}{\theta^k-1}+\sum_{l=1,(k=2^n-1)}^{2^n-2}\frac{c_kc_l}{(\theta^l-1)\theta^k}\sum_{i=1}^{2^n-2}1. \tag{4}$$

В силу того, что порядок θ равен 2^n-1, имеем $\theta^{(2^n-2)k}=\theta^{-k}$, отсюда следует, что $\dfrac{\theta^{(2^n-2)k}-1}{\theta^k-1}=\dfrac{1}{\theta^k}$. Заметим, что вторая сумма в равенстве (4) содержит множитель (2^n-2), а так как характеристика поля равна 2, то она равна нулю. В итоге

$$A_1=\sum_{k,l=1}^{2^n-2}\frac{c_kc_l}{(\theta^l-1)\theta^k}.$$

Теперь посчитаем A_2, выделим слагаемое, соответствующее $k=2^n-1$:

$$A_2=\sum_{k,l=1}^{2^n-2}\frac{c_kc_l}{(\theta^l-1)\theta^k}\sum_{i=1}^{2^n-2}\theta^{(l+k)i}+\sum_{l=1,(k=2^n-1)}^{2^n-2}\frac{c_kc_l}{\theta^l-1}\sum_{i=1}^{2^n-2}\theta^{il}=$$

$$=\sum_{k,l=1:l+k=2^n-1}^{2^n-2}\frac{c_kc_l}{(\theta^l-1)\theta^k}\sum_{i=1}^{2^n-2}1+\sum_{k,l=1:l+k\neq 2^n-1}^{2^n-2}\frac{c_kc_l}{(\theta^l-1)\theta^k}\sum_{i=1}^{2^n-2}\theta^{(l+k)i}+$$

$$+\sum_{l=1,(k=2^n-1)}^{2^n-2}\frac{c_kc_l}{\theta^l-1}\frac{\theta^l(\theta^{-l}-1)}{\theta^l-1}.$$

Первая из трёх сумм равна нулю, так как $\sum\limits_{i=1}^{2^n-2}1=2^n-2\equiv 0 \pmod 2$, и поэтому

$$A_2=\sum_{k,l=1:l+k\neq 2^n-1}^{2^n-2}\frac{c_kc_l}{(\theta^l-1)\theta^k}\frac{\theta^{l+k}(\theta^{-(l+k)}-1)}{\theta^{l+k}-1}+\sum_{l=1,(k=2^n-1)}^{2^n-2}\frac{c_kc_l}{\theta^l-1}\frac{\theta^l(1-\theta^l)}{\theta^l(\theta^l-1)}=$$

$$=\sum_{k,l=1:l+k\neq 2^n-1}^{2^n-2}\frac{c_kc_l}{(\theta^l-1)\theta^k}+\sum_{l=1,(k=2^n-1)}^{2^n-2}\frac{c_kc_l}{\theta^l-1}.$$

Осталось вычислить сумму B:

$$B=\sum_{k=1,(l=2^n-1)}^{2^n-1}c_kc_l\sum_{i=1}^{2^n-3}\theta^{ik}(2^n-2-i)=$$

$$=\sum_{k=1,(l=2^n-1)}^{2^n-1}c_kc_l(2^n-2)\sum_{i=1}^{2^n-3}\theta^{ik}-\sum_{k=1,(l=2^n-1)}^{2^n-1}c_kc_l\sum_{i=1}^{2^n-3}i\theta^{ik}.$$

Заметим, что первая сумма обращается в нуль, значит,

$$B=\sum_{k=1,(l=2^n-1)}^{2^n-2} c_k c_l \theta^k \sum_{i=1}^{2^n-3} i(\theta^k)^{i-1}+\sum_{k=2^n-1,l=2^n-1} c_k c_l \sum_{i=1}^{2^n-3} i=$$

$$=\sum_{k=1,(l=2^n-1)}^{2^n-2} c_k c_l \theta^k\left(\sum_{i=1}^{2^n-3} x^i\right)'_{x=\theta^k}+c_{2^n-1}^2 \sum_{i=1}^{2^n-3} i=\sum_{k=1,(l=2^n-1)}^{2^n-2} c_k c_l \theta^k\left(\frac{x^{2^n-2}-x}{x-1}\right)'_{x=\theta^k}+c_{2^n-1}^2=$$

$$=c_{2^n-1}^2+\sum_{k=1,(l=2^n-1)}^{2^n-2} c_k c_l \theta^k\left(\frac{((2^n-2)x^{2^n-3}-1)(x-1)-x^{2^n-2}+x}{(x-1)^2}\right)_{x=\theta^k}=$$

$$=c_{2^n-1}^2+\sum_{k=1,(l=2^n-1)}^{2^n-2} c_k c_l \theta^k \frac{-\theta^k+1-\theta^{-k}+\theta^k}{(\theta^k-1)^2}=$$

$$=c_{2^n-1}^2+\sum_{k=1,(l=2^n-1)}^{2^n-2} c_k c_l \frac{\theta^k-1}{(\theta^k-1)^2}=c_{2^n-1}^2+\sum_{k=1,(l=2^n-1)}^{2^n-2} \frac{c_k c_l}{\theta^k-1}.$$

Собирая все подсчитанные суммы вместе, получаем

$$n_1=\sum_{k,l=1}^{2^n-2} \frac{c_k c_l}{(\theta^l-1)\theta^k}+\sum_{k,l=1(l+k\neq 2^n-1)}^{2^n-2} \frac{c_k c_l}{(\theta^l-1)\theta^k}+\sum_{l=1,(k=2^n-1)}^{2^n-2} \frac{c_k c_l}{\theta^l-1}+c_{2^n-1}^2+\sum_{k=1,(l=2^n-1)}^{2^n-2} \frac{c_k c_l}{\theta^k-1}.$$

Первую сумму можно разбить на две области суммирования по $l+k=2^n-1$ и $l+k\neq$ $\neq 2^n-1$:

$$n_1=\sum_{k,l=1,(l+k=2^n-1)}^{2^n-2} \frac{c_k c_l}{(\theta^l-1)\theta^k}+\sum_{k,l=1,(l+k\neq 2^n-1)}^{2^n-2} \frac{c_k c_l}{(\theta^l-1)\theta^k}+\sum_{k,l=1(l+k\neq 2^n-1)}^{2^n-2} \frac{c_k c_l}{(\theta^l-1)\theta^k}+$$

$$+\sum_{l=1,(k=2^n-1)}^{2^n-2} \frac{c_k c_l}{\theta^l-1}+c_{2^n-1}^2+\sum_{k=1,(l=2^n-1)}^{2^n-2} \frac{c_k c_l}{\theta^k-1}.$$

Заметим, что $\sum_{l=1}^{2^n-2} \frac{c_k c_l}{\theta^l-1}=\sum_{k=1}^{2^n-2} \frac{c_k c_l}{\theta^k-1}$. Тогда $n_1=\sum_{k,l=1,(l+k=2^n-1)}^{2^n-2} \frac{c_k c_l}{(\theta^l-1)\theta^k}+c_{2^n-1}^2$. Выразив l через k из равенства $l+k=2^n-1$, получаем

$$n_1=c_{2^n-1}^2+\sum_{k=1}^{2^n-2} \frac{c_k c_{2^n-1-k}}{(\theta^{2^n-1-k}-1)\theta^k}=c_{2^n-1}^2+\sum_{k=1}^{2^n-2} \frac{c_k c_{2^n-1-k}}{1-\theta^k}=$$

$$=c_{2^n-1}^2+\sum_{k=1}^{(2^n-2)/2} \frac{c_k c_{2^n-1-k}}{1-\theta^k}+\sum_{k=(2^n-2)/2+1}^{2^n-2} \frac{c_k c_{2^n-1-k}}{1-\theta^k}=$$

$$=c_{2^n-1}^2+\sum_{k=1}^{(2^n-2)/2} \frac{c_k c_{2^n-1-k}}{1-\theta^k}+\sum_{k=1}^{(2^n-2)/2} \frac{c_k c_{2^n-1-k}}{1-\theta^{-k}}=$$

$$=c_{2^n-1}^2+\sum_{k=1}^{(2^n-2)/2} \frac{c_k c_{2^n-1-k}}{1-\theta^k}+\sum_{k=1}^{(2^n-2)/2} \frac{c_k c_{2^n-1-k}}{\theta^k-1}\theta^k=$$

$$=c_{2^n-1}^2+\sum_{k=1}^{2^{n-1}-1} \frac{c_k c_{2^n-1-k}(1-\theta^k)}{1-\theta^k}=c_{2^n-1}^2+\sum_{k=1}^{2^{n-1}-1} c_k c_{2^n-1-k}.$$

Теорема доказана. ■

Следствие 1. Пусть $F: Q\to P$, $F(0)=0$, F — бент-функция и $||F||=n_0+$ $+2n_1+4n_2+\ldots$ Тогда в равенстве (1) $c_{2^n-1}=0$ при $n\geqslant 4$, а при $n\geqslant 6$ выполняется $c_{2^n-1-2^l}=0$ для всех $l\in\{0,1,\ldots,n-1\}$.

Доказательство. Рассмотрим функцию $G(x) = F(x) + L_a(x)$, где $\{L_a(x) : a \in Q\}$ — множество линейных булевых функций от n переменных. Функцию $G(x)$ можно представить в виде $G(x) = \sum\limits_{k=1}^{2^n-1} g_k x^k$; линейная функция имеет вид $L_a(x) = \sum\limits_{s=0}^{n-1} a^{2^s} x^{2^s}$. Тогда имеем равенство

$$\sum_{k=1}^{2^n-1} g_k x^k = \sum_{k=1}^{2^n-1} c_k x^k + \sum_{s=0}^{n-1} a^{2^s} x^{2^s} = \sum_{k=1, k\neq 2^s, s\in\{0,1,\ldots,n-1\}}^{2^n-1} c_k x^k + \sum_{s=0}^{n-1} \left(a^{2^s} + c_{2^s}\right) x^{2^s}.$$

Известно [6, с. 236], что вес бент-функции от n переменных описывается значениями $2^{n-1} + \varepsilon\, 2^{n/2-1}$, где $\varepsilon \in \{-1, 1\}$. Тогда $c_{2^n-1} = 0$, а при $n/2 - 1 \geqslant 2$ (т. е. при $n \geqslant 6$) коэффициент n_1 в двоичном разложении веса функции F равен 0. Имеем

$$\begin{aligned}\sum_{k=1}^{2^{n-1}-1} g_k g_{2^n-1-k} &= \sum_{k=1, k\neq 2^s, s\in\{0,1,\ldots,n-1\}}^{2^{n-1}-1} c_k c_{2^n-1-k} + \sum_{s=0}^{n-1} \left(c_{2^s} + a^{2^s}\right) c_{2^n-1-2^s} = \\ &= \sum_{k=1}^{2^{n-1}-1} c_k c_{2^n-1-k} + \sum_{s=0}^{n-1} a^{2^s} c_{2^n-1-2^s}.\end{aligned} \tag{5}$$

Так как F и G — бент-функции, то, используя (3), получаем равенства

$$\sum_{k=1}^{2^{n-1}-1} g_k g_{2^n-1-k} = 0, \quad \sum_{k=1}^{2^{n-1}-1} c_k c_{2^n-1-k} = 0.$$

В результате из (5) следует, что $\sum\limits_{s=0}^{n-1} a^{2^s} c_{2^n-1-2^s} = 0$ для всех $a \in Q$. Таким образом, имеем многочлен степени 2^{n-1} относительно a. Он не может иметь в поле больше чем 2^{n-1} корней, а в наших условиях он имеет 2^n корней, значит, $c_{2^n-1-2^s} = 0$ для всех $s \in \{0, 1, \ldots, n-1\}$. ■

Следствие 2. Пусть $F : Q \to P$, $F(0) = 0$, F — гипер-бент-функция и $||F|| = n_0 + 2n_1 + 4n_2 + \ldots$ Тогда при $n \geqslant 4$ имеет место $c_{2^n-1} = 0$, а при $n \geqslant 6$ выполняется $c_{2^n-1-v2^l} = 0$ для всех $l \in \{0, 1, \ldots, n-1\}$ и для всех v, таких, что $(v, 2^n - 1) = 1$.

Доказательство. Рассмотрим функцию $G(x) = F(x) + L_a^{(v)}(x)$, где $L_a^{(v)}(x)$ — собственная мономиальная функция [7] и $(v, 2^n - 1) = 1$; $G(x)$ при этом является гипер-бент-функцией. Тогда имеем равенство

$$G(x) = \sum_{k=1}^{2^n-1} c_k x^k + \sum_{s=0}^{n-1} a^{2^s} x^{v2^s}.$$

Заметим, что гипер-бент-функция является бент-функцией. При $n \geqslant 6$ аналогично следствию 1 получаем, что $\sum\limits_{s=0}^{n-1} a^{2^s} c_{2^n-1-v2^s} = 0$ для всех $a \in Q$. Отсюда следует, что $c_{2^n-1-v2^l} = 0$ для всех $l \in \{0, 1, \ldots, n-1\}$ и для всех v со свойством $(v, 2^n - 1) = 1$. ■

Для получения соотношения для третьего разряда в двоичном разложении веса функции используется следующая лемма.

Лемма 2 [5]. Пусть $a_i \in \{0, 1\}$, $\sum\limits_{i=1}^{n} a_i = k = n_0 + 2n_1 + 4n_2 + \ldots$, где $n_j \in \{0, 1\}$; при этом $k \geqslant 4$. Тогда $n_2 = \sum\limits_{1\leqslant t<l<h<f\leqslant n} a_k a_l a_h a_f$, где сумма берётся по модулю 2.

При вычислении следующего разряда в разложении веса пока не удалось получить такого же красивого и компактного результата, как в теореме 1. Представим результат вычислений, сами расчёты приведены в Приложении.

Теорема 2. Пусть $F : Q \to P$, $F(0) = 0$ и $||F|| = n_0 + 2n_1 + 4n_2 + \ldots$ Тогда

$$
\begin{aligned}
n_2 = (c_{2^n-1})^4 &+ \sum_{f,h,l,k\neq 2^n-1} \frac{c_kc_lc_hc_f}{(\theta^f-1)(\theta^h-1)(\theta^l-1)(\theta^k-1)\theta^h\theta^{2l}\theta^{3k}}(1-\theta^{3k})+\\
&+ \sum_{f,h,l,k+l\neq 2^n-1} \frac{c_kc_lc_hc_f\theta^l}{(\theta^f-1)(\theta^h-1)(\theta^l-1)(\theta^{k+l}-1)\theta^h\theta^{3(k+l)}}(1-\theta^{3(k+l)})+\\
&+ \sum_{\substack{f,h,k\neq 2^n-1\\ l=2^n-1}} \frac{c_kc_lc_hc_f\theta^k}{(\theta^f-1)(\theta^h-1)(\theta^k-1)^2\theta^h\theta^{3k}}(1-\theta^{3k})+\\
&+ \sum_{f,h,l+h,k\neq 2^n-1} \frac{c_kc_lc_hc_f}{(\theta^f-1)(\theta^h-1)(\theta^{l+h}-1)(\theta^k-1)\theta^h\theta^{2l}\theta^{3k}}(1-\theta^{3k})+\\
&+ \sum_{f,h,l+h,k+l+h\neq 2^n-1} \frac{c_kc_lc_hc_f}{(\theta^f-1)(\theta^h-1)(\theta^{l+h}-1)(\theta^{k+l+h}-1)\theta^h\theta^{2l}\theta^{3k}}(1-\theta^{3(k+l+h)})+\\
&+ \sum_{\substack{f,h,k\neq 2^n-1\\ l+h=2^n-1}} \frac{c_kc_lc_hc_f\theta^k\theta^h}{(\theta^f-1)(\theta^h-1)(\theta^k-1)^2\theta^{3k}}(1-\theta^{3k})+\\
&+ \sum_{\substack{f,l,l+k\neq 2^n-1\\ h=2^n-1}} \frac{c_kc_lc_hc_f}{(\theta^f-1)(\theta^l-1)^2(\theta^{k+l}-1)^2\theta^l\theta^{3k}}(1-\theta^{3(k+l)})+\\
&+ \sum_{\substack{f,l,l+k\neq 2^n-1\\ h=2^n-1}} \frac{c_kc_lc_hc_f\theta^{2l}\theta^k}{(\theta^f-1)(\theta^l-1)^2(\theta^{l+k}-1)^2}\,\frac{1-\theta^{3(l+k)}}{\theta^{3(l+k)}}+\\
&+ \sum_{\substack{f,l,k\neq 2^n-1\\ h=2^n-1}} \frac{c_kc_lc_hc_f}{(\theta^f-1)(\theta^l-1)^2(\theta^k-1)\theta^l}\,\frac{1-\theta^{3k}}{\theta^{3k}} + \sum_{\substack{f,k\neq 2^n-1\\ h,l=2^n-1}} \frac{c_kc_lc_hc_f}{(\theta^f-1)(\theta^k-1)^3\theta^k}(1-\theta^{3k})+\\
&+ \sum_{\substack{f,l,k\neq 2^n-1\\ h+f\neq 2^n-1}} \frac{c_kc_lc_hc_f(1-\theta^{3k})}{(\theta^f-1)(\theta^{h+f}-1)(\theta^l-1)(\theta^k-1)\theta^h\theta^{2l}\theta^{3k}}+\\
&+ \sum_{\substack{f,l,k+l\neq 2^n-1\\ h+f\neq 2^n-1}} \frac{c_kc_lc_hc_f\theta^l(1-\theta^{3(k+l)})}{(\theta^f-1)(\theta^{h+f}-1)(\theta^l-1)(\theta^{k+l}-1)\theta^h\theta^{3(k+l)}}+\\
&+ \sum_{\substack{f,h+f,k\neq 2^n-1\\ l=2^n-1}} \frac{c_kc_lc_hc_f\theta^k(1-\theta^{3k})}{(\theta^f-1)(\theta^{h+f}-1)(\theta^k-1)^2\theta^h\theta^{3k}}+\\
&+ \sum_{\substack{f,h+f,k\neq 2^n-1\\ l+h+f\neq 2^n-1}} \frac{c_kc_lc_hc_f(1-\theta^{3k})}{(\theta^f-1)(\theta^{h+f}-1)(\theta^{l+h+f}-1)(\theta^k-1)\theta^h\theta^{2l}\theta^{3k}}+\\
&+ \sum_{\substack{f,k+l+h+f\neq 2^n-1\\ h+f,l+h+f\neq 2^n-1}} \frac{c_kc_lc_hc_f(1-\theta^{3(l+h+f+k)})}{(\theta^f-1)(\theta^{h+f}-1)(\theta^{l+h+f}-1)(\theta^{l+h+f+k}-1)\theta^h\theta^{2l}\theta^{3k}}+\\
&+ \sum_{\substack{f,h+f,k\neq 2^n-1\\ l+h+f=2^n-1}} \frac{c_kc_lc_hc_f\theta^{h+k}\theta^{2f}(1-\theta^{3k})}{(\theta^f-1)(\theta^{h+f}-1)(\theta^k-1)^2\theta^{3k}} + \sum_{\substack{f,l,l+k\neq 2^n-1\\ h+f=2^n-1}} \frac{c_kc_lc_hc_f\theta^f(1-\theta^{3(k+l)})}{(\theta^f-1)(\theta^l-1)^2(\theta^{k+l}-1)^2\theta^l\theta^{3k}}+\\
&+ \sum_{\substack{f,l,l+k\neq 2^n-1\\ h+f=2^n-1}} \frac{c_kc_lc_hc_f\theta^f\theta^{2l}\theta^k}{(\theta^f-1)(\theta^l-1)^2(\theta^{l+k}-1)^2}\,\frac{1-\theta^{3(l+k)}}{\theta^{3(l+k)}}+
\end{aligned}
$$

$$+\sum_{\substack{f,l,k\neq 2^n-1\\ h+f=2^n-1}} \frac{c_k c_l c_h c_f \theta^f}{(\theta^f-1)(\theta^l-1)^2(\theta^k-1)\theta^l}\,\frac{1-\theta^{3k}}{\theta^{3k}} + \sum_{\substack{f,k\neq 2^n-1\\ h+f,l=2^n-1}} \frac{c_k c_l c_h c_f \theta^f}{(\theta^f-1)(\theta^k-1)^3\theta^k}(1-\theta^{3k})+$$

$$+\sum_{\substack{h,l+h,k\neq 2^n-1\\ f=2^n-1}} \frac{c_k c_l c_h c_f (1-\theta^{3k})}{(\theta^h-1)^2(\theta^{l+h}-1)^2(\theta^k-1)\theta^{2l}\theta^{3k}}+$$

$$+\sum_{\substack{h,l+h,l+h+k\neq 2^n-1\\ f=2^n-1}} \frac{c_k c_l c_h c_f \theta^{2h}\theta^k (1-\theta^{3(l+h+k)})}{(\theta^h-1)^2(\theta^{l+h}-1)^2(\theta^{l+h+k}-1)^2\theta^{3k}}+$$

$$+\sum_{\substack{h,l+h,l+h+k\neq 2^n-1\\ f=2^n-1}} \frac{c_k c_l c_h c_f (1-\theta^{3(l+h+k)})}{(\theta^h-1)^2(\theta^{l+h}-1)^2(\theta^{l+h+k}-1)^2\theta^{2l}\theta^{3k}} + \sum_{\substack{h,k\neq 2^n-1\\ f,l+h=2^n-1}} \frac{c_k c_l c_h c_f \theta^{2h}(1-\theta^{3k})}{(\theta^h-1)^2(\theta^k-1)^3\theta^{2k}}+$$

$$+\sum_{\substack{h,h+l,h+l+k\neq 2^n-1\\ f=2^n-1}} \frac{c_k c_l c_h c_f \theta^{2l}}{(\theta^h-1)^2(\theta^{h+l}-1)^2}\,\frac{1-\theta^{3(l+h+k)}}{\theta^{3(l+k)}(\theta^{l+h+k}-1)^2}+$$

$$+\sum_{\substack{h,h+l,h+l+k\neq 2^n-1\\ f=2^n-1}} \frac{c_k c_l c_h c_f \theta^{l}}{(\theta^h-1)^2(\theta^{h+l}-1)^2}\,\frac{1-\theta^{3(l+h+k)}}{\theta^{2(l+k)}(\theta^{l+h+k}-1)^2}+$$

$$+\sum_{\substack{h,h+l,k\neq 2^n-1\\ f=2^n-1}} \frac{c_k c_l c_h c_f (1-\theta^{3k})}{(\theta^h-1)^2(\theta^{h+l}-1)^2(\theta^k-1)\theta^l\theta^{3k}} + \sum_{\substack{h,k\neq 2^n-1\\ f,h+l=2^n-1}} \frac{c_k c_l c_h c_f \theta^h(1-\theta^{3k})}{(\theta^h-1)^2(\theta^k-1)^3\theta^k}+$$

$$+\sum_{\substack{k,h,l\neq 2^n-1\\ f=2^n-1}} \frac{c_k c_l c_h c_f}{(\theta^h-1)^2(\theta^l-1)\theta^{2l}}\,\frac{1-\theta^{3k}}{(\theta^k-1)\theta^{3k}} + \sum_{\substack{h,l,l+k\neq 2^n-1\\ f=2^n-1}} \frac{c_k c_l c_h c_f \theta^l}{(\theta^h-1)^2(\theta^l-1)}\,\frac{1-\theta^{3(l+k)}}{(\theta^{l+k}-1)\theta^{3(l+k)}}+$$

$$+\sum_{\substack{h,k\neq 2^n-1\\ f,l=2^n-1}} \frac{c_k c_l c_h c_f \theta^k}{(\theta^h-1)^2}\,\frac{1-\theta^{3k}}{(\theta^k-1)^2\theta^{3k}} + \sum_{\substack{l,k+l\neq 2^n-1\\ f,h=2^n-1}} \frac{c_k c_l c_h c_f}{(\theta^l-1)^3}\,\frac{1-\theta^{3(k+l)}}{\theta^{3k}(\theta^{k+l}-1)^2}+$$

$$+\sum_{\substack{l,k+l\neq 2^n-1\\ f,h=2^n-1}} \frac{c_k c_l c_h c_f \theta^k}{(\theta^l-1)^3}\,\frac{1-\theta^{3(k+l)}}{\theta^{3k}(\theta^{k+l}-1)^2} + \sum_{\substack{l,k\neq 2^n-1\\ f,h=2^n-1}} \frac{c_k c_l c_h c_f}{(\theta^l-1)^3}\,\frac{1-\theta^{3k}}{\theta^{3k}(\theta^k-1)}+$$

$$+\sum_{\substack{l,l+k\neq 2^n-1\\ f,h=2^n-1}} \frac{c_k c_l c_h c_f}{(\theta^l-1)(\theta^{l+k}-1)}\,\frac{1-\theta^{3(l+k)}}{\theta^k(\theta^{l+k}-1)^2} + \sum_{\substack{f,h,l=2^n-1\\ k\neq 2^n-1}} \frac{c_k c_l c_h c_f}{(\theta^k-1)^4}(1-\theta^{3k}).$$

Доказательство приводится в Приложении.

2. Структурные характеристики бент-функций и гипер-бент-функций

В качестве структурных характеристик рассматриваются вес функции и веса её ограничений на различных подпространствах и многообразиях. Пусть $n = 2\lambda$, где $\lambda \in \mathbb{N}$. Фиксируя какие-либо переменные или значения линейных комбинаций переменных функции $f(x_0, x_1, \ldots, x_{n-1})$ значениями 0 или 1, получаем вес соответствующей ей функции $F(x)$ на подпространстве или многообразии. При определённой фиксации $n-s$ переменных, где s делит n, получаем подполе $\mathrm{GF}(2^s)$. Тогда для функции $g(x_{i_1}, \ldots, x_{i_s})$, которая получается из функции f фиксацией $n-s$ переменных, существуют аналогичные приведённым во введении представления в виде полинома от одного переменного над полем. При этом должна существовать зависимость между коэффициентами полиномов, заданных над полем $\mathrm{GF}(2^n)$ и полем $\mathrm{GF}(2^\lambda)$.

Для установления этой зависимости необходимо описать значения веса функции $f(x_0, x_1, \ldots, x_{n-1})$ на различных подпространствах. Обозначим (α, x) скалярное произведение векторов $\alpha \in V_n$ и $x \in V_n$; $f|_T$ — ограничение функции f на пространстве или многообразии T.

Лемма 3. Пусть $\alpha \in V_n \setminus \{\mathbf{0}\}$. Тогда вес функции $f(x_0, x_1, \ldots, x_{n-1}) \cdot (\alpha, x)$ равен весу $f|_W$, где $W = \{x \in V_n : (\alpha, x) = 1\}$.

Для дальнейшего изложения результатов приведём вспомогательное утверждение.

Утверждение 2. Пусть $k \geqslant 2$ и $f_i(x)$ — булевы функции от n переменных, $i = 1, \ldots, k$. Тогда

$$||f_1 \cdot \ldots \cdot f_k|| = \frac{1}{2^{k-1}} \sum_{t=1}^{k} (-1)^{t-1} \sum_{1 \leqslant i_1 < i_2 < \ldots < i_t \leqslant k} ||f_{i_1} + \ldots + f_{i_t}||.$$

Доказательство. Докажем утверждение методом математической индукции по параметру $k \geqslant 2$. База индукции при $k = 2$ получается из известной формулы

$$||f + g|| = ||f|| + ||g|| - 2||f \cdot g||.$$

Шаг индукции. Пусть утверждение верно при $k \leqslant m - 1$, покажем, что оно верно и для $k = m$. Имеет место равенство $||f_1 \cdot \ldots \cdot f_k|| = ||(f_1 \cdot f_k) \cdot \ldots \cdot (f_{k-1} \cdot f_k)||$. Обозначим $g_i = (f_i \cdot f_k)$, $i = 1, \ldots, k - 1$. Тогда по предположению индукции

$$||g_1 \cdot \ldots \cdot g_{k-1}|| = \frac{1}{2^{k-2}} \sum_{t=1}^{k-1} (-1)^{t-1} \sum_{1 \leqslant i_1 < \ldots < i_t \leqslant k-1} ||g_{i_1} + \ldots + g_{i_t}|| =$$
$$= \frac{1}{2^{k-2}} \sum_{t=1}^{k-1} (-1)^{t-1} \sum_{1 \leqslant i_1 < \ldots < i_t \leqslant k-1} ||f_k(f_{i_1} + \ldots + f_{i_t})||.$$

Теперь снова воспользуемся формулой $||f \cdot g|| = \frac{1}{2}\,(||f|| + ||g|| - ||f + g||)$. Получаем равенство

$$||f_1 \cdot \ldots \cdot f_k|| = \frac{1}{2^{k-1}} \sum_{t=1}^{k-1} (-1)^{t-1} \sum_{1 \leqslant i_1 < \ldots < i_t \leqslant k-1} ||f_k|| +$$
$$+ \frac{1}{2^{k-1}} \sum_{t=1}^{k-1} (-1)^{t-1} \sum_{1 \leqslant i_1 < \ldots < i_t \leqslant k-1} ||f_{i_1} + \ldots + f_{i_t}|| +$$
$$+ \frac{1}{2^{k-1}} \sum_{t=1}^{k-1} (-1)^{t} \sum_{1 \leqslant i_1 < \ldots < i_t \leqslant k-1} ||f_k + f_{i_1} + \ldots + f_{i_t}||.$$

Первую из трёх сумм свернём по биному Ньютона, а в третьей преобразуем индексы суммирования:

$$||f_1 \cdot \ldots \cdot f_k|| = \frac{1}{2^{k-1}} ||f_k|| + \frac{1}{2^{k-1}} \sum_{t=1}^{k-1} (-1)^{t-1} \sum_{1 \leqslant i_1 < \ldots < i_t < k} ||f_{i_1} + \ldots + f_{i_t}|| +$$
$$+ \frac{1}{2^{k-1}} \sum_{t=2}^{k} (-1)^{t-1} \sum_{1 \leqslant i_1 < \ldots < i_t = k} ||f_{i_1} + \ldots + f_{i_t}||.$$

Объединяя все слагаемые в одну сумму, получаем

$$||f_1 \cdot \ldots \cdot f_k|| = \frac{1}{2^{k-1}} \sum_{t=1}^{k} (-1)^{t-1} \sum_{1 \leqslant i_1 < i_2 < \ldots < i_t \leqslant k} ||f_{i_1} + \ldots + f_{i_t}||.$$

Утверждение доказано. ■

Известно [6, с. 236], что вес бент-функции f от n переменных описывается значениями $||f|| = 2^{n-1} + \varepsilon 2^{n/2-1}$, где $\varepsilon \in \{1, -1\}$. Известно также, что сумма линейной и бент-функции снова является бент-функцией. Из этого следует, что $||f + g|| = 2^{n-1} + \varepsilon' 2^{n/2-1}$, где g — произвольная линейная функция; $\varepsilon' \in \{1, -1\}$.

Теорема 3. Пусть f — бент-функция, $k \geqslant 2$, $g_1, \ldots, g_{k-1}$ — линейные функции, такие, что для любого $t \in \{1, \ldots, k-1\}$ и для любых $1 \leqslant i_1 < \ldots < i_t \leqslant k-1$ сумма $g_{i_1} + \ldots + g_{i_t}$ тождественно не равна 0. Пусть также вес функции f равен $||f|| = 2^{n-1} + \varepsilon_0 \cdot 2^{n/2-1}$, вес функции $f + g_{i_1} + \ldots + g_{i_t}$ равен $||f + g_{i_1} + \ldots + g_{i_t}|| = 2^{n-1} + \varepsilon_{i_1,\ldots,i_t} \cdot 2^{n/2-1}$, где $t \in \{1, \ldots, k-1\}$, $\varepsilon_0, \varepsilon_{i_1,\ldots,i_t} \in \{1, -1\}$. Тогда

$$||f \cdot g_1 \cdot \ldots \cdot g_{k-1}|| = 2^{n-k} + \frac{2^{n/2}}{2^k} \left[\varepsilon_0 + \sum_{t=1}^{k-1} (-1)^t \sum_{1 \leqslant i_1 < \ldots < i_t \leqslant k-1} \varepsilon_{i_1,\ldots,i_t} \right]. \tag{6}$$

Доказательство. Используя утверждение 2 и выделяя слагаемые, содержащие функцию f, получаем

$$||f \cdot g_1 \cdot \ldots \cdot g_{k-1}|| = \frac{1}{2^{k-1}} \left(||f|| + \sum_{t=1}^{k-1} (-1)^{t-1} \sum_{1 \leqslant i_1 < \ldots < i_t \leqslant k-1} ||g_{i_1} + \ldots + g_{i_t}|| + \right.$$
$$\left. + \sum_{t=1}^{k-1} (-1)^t \sum_{1 \leqslant i_1 < \ldots < i_t \leqslant k-1} ||g_{i_1} + \ldots + g_{i_t} + f|| \right).$$

Сумма линейных функций является линейной функцией и её вес равен 2^{n-1}. Подставляя значения весов функций, получаем равенство

$$||f \cdot g_1 \cdot \ldots \cdot g_{k-1}|| = \frac{1}{2^{k-1}} \left(2^{n-1} + \varepsilon_0 2^{n/2-1} + 2^{n-1} \sum_{t=1}^{k-1} (-1)^{t-1} C_{k-1}^t + \right.$$
$$\left. + \sum_{t=1}^{k-1} (-1)^t \sum_{1 \leqslant i_1 < \ldots < i_t \leqslant k-1} \left(2^{n-1} + \varepsilon_{i_1,\ldots,i_t} 2^{n/2-1} \right) \right).$$

Заметим, что

$$2^{n-1} \sum_{t=1}^{k-1} (-1)^{t-1} C_{k-1}^t = -2^{n-1} \sum_{t=1}^{k-1} (-1)^t C_{k-1}^t = -2^{n-1} \left((1-1)^{k-1} - 1 \right) = 2^{n-1}.$$

Возвращаясь к исходному равенству, получаем

$$||f \cdot g_1 \cdot \ldots \cdot g_{k-1}|| = \frac{1}{2^{k-1}} \left(2^{n-1} + \varepsilon_0 2^{n/2-1} + \sum_{t=1}^{k-1} (-1)^t \sum_{1 \leqslant i_1 < \ldots < i_t \leqslant k-1} \varepsilon_{i_1,\ldots,i_t} 2^{n/2-1} \right).$$

Теорема доказана. ■

Замечание 2. При $k < n/2$ получаем, что вес ограничения функции f на многообразиях и подпространствах размерности больше $n/2$ кратен 2. Однако это верно и при $k = n/2$. Для этого достаточно показать, что выражение в скобках в равенстве (6) сравнимо с нулем по модулю 2. Обозначим данную сумму по модулю 2 через S:

$$S = 1 + \sum_{t=1}^{k-1} \sum_{1 \leqslant i_1 < \ldots < i_t \leqslant k-1} 1 \pmod 2.$$

Внутренняя сумма равна биномиальному коэффициенту C_{k-1}^t. Чётные биномиальные коэффициенты сравнимы с нулем по модулю 2, а количество нечётных биномиальных коэффициентов чётно, при этом 1 в начале формулы равна недостающему коэффициенту при $t = 0$. Таким образом, получаем, что $S = 0 \pmod 2$.

Заметим, что так как гипер-бент-функция, в частности, является бент-функцией, то теорема верна и для гипер-бент-функций.

Рассмотрим два примера бент-функций и покажем, что при определённых фиксациях переменных можно получить более сильные по сравнению с теоремой 3 результаты.

1) $f(x_1,\ldots,x_{2\lambda}) = \sum\limits_{i=1}^{\lambda} x_{2i-1}x_{2i}$. Функции такого вида являются совершенно нелинейными, а следовательно, бент-функциями [4]. Заметим, что при фиксации любой переменной x_{2j} единицей получаем, что переменная x_{2j-1} входит линейно, а значит, получаемая подфункция сбалансирована. Аналогично происходит при фиксации $x_{2j-1} = 1$. При фиксации переменной x_{2j} (или переменной x_{2j-1}) нулём получаем, что подфункция не зависит от переменной x_{2j-1} (или от x_{2j} соответственно). Таким образом, вес функции f чётен на всех подпространствах степени больше первой и функция равновероятна на всех многообразиях степени больше первой, получаемых при фиксации хотя бы одной переменной $x_j = 1$.

2) $f(x_1,\ldots,x_{2\lambda}) = \sum\limits_{i=1}^{\lambda} x_i x_{i+\lambda} + h(x_1,\ldots,x_\lambda)$. Функция f является бент-функцией для любой функции h [6]. При фиксации любой из переменных x_t, $t \in \{1,\ldots,\lambda\}$, единицей получаем, что переменная $x_{t+\lambda}$ входит линейно и, следовательно, получаемая при данной фиксации подфункция сбалансирована. При фиксации любой из переменных x_t, $t \in \{1,\ldots,\lambda\}$, нулём получаем, что подфункция не зависит от переменной $x_{t+\lambda}$.

Таким образом, функция f равновероятна на 2^λ многообразиях степени выше первой, которые получаются выбором и фиксацией переменных x_j, $j \in \{1,\ldots,\lambda\}$, единицей. Вес функции f чётен на всех подпространствах, получаемых при фиксации хотя бы одной переменной x_t, $t \in \{1,\ldots,\lambda\}$, нулём.

ЛИТЕРАТУРА

1. *Rothaus O. S.* On bent functions // J. Combinatorial Theory. 1976. V. 20(A). P. 300–305.
2. *Youssef A. and Gong G.* Hyper-bent functions // LNCS. 2001. V. 2045. P. 406–419.
3. *Логачев О. А., Сальников А. А., Ященко В. В.* О свойствах сумм Вейля на конечных полях и конечных абелевых группах // Дискретная математика. 1999. Т. 11. № 2. С. 66–85.
4. *Мак-Вильямс Ф. Дж., Слоэн Н. Дж. А.* Теория кодов, исправляющих ошибки. М.: Связь, 1979.
5. *Rueppel R. A.* Analysis and Design of Stream Ciphers. Berlin: Springer, 1986. 244 p.
6. *Логачев О. А., Сальников А. А., Ященко В. В.* Булевы функции в теории кодирования и криптологии. М.: МЦНМО, 2004.
7. *Кузьмин А. С., Марков В. Т., Нечаев А. А., Шишков А. Б.* Приближение булевых функций мономиальными // Дискретная математика. 2006. Т. 18. № 1. С. 9–29.

ПРИЛОЖЕНИЕ

Доказательство теоремы 2

Сначала докажем вспомогательную лемму.

Лемма 4. Пусть $s,t \in \mathbb{N}$ и $s \leqslant t$. Тогда

$$\sum_{i=s}^{t} ix^{i-1} = \frac{tx^{t+1} - (t+1)x^t - (s-1)x^s + sx^{s-1}}{(x-1)^2}.$$

Доказательство. Заметим, что $\sum\limits_{i=s}^{t} ix^{i-1} = \left(\sum\limits_{i=s}^{t} x^i\right)'$. Используя формулу геометрической прогрессии, получим

$$\left(\sum_{i=s}^{t} x^i\right)' = \left(x^s\frac{x^{t-s-1}-1}{x-1}\right)' = \left(\frac{x^{t+1}-x^s}{x-1}\right)'.$$

Возьмём производную: $\left(\dfrac{x^{t+1}-x^s}{x-1}\right)' = \dfrac{(t+1)x^{t+1}-sx^s-(t+1)x^t+sx^{s-1}-x^{t+1}+x^s}{(x-1)^2}$. После приведения подобных слагаемых получим требуемую формулу. ■

Доказательство теоремы 2.

$$n_2 = \sum_{\substack{x_1,x_2,x_3,x_4\in Q:\\ x_1<x_2<x_3<x_4}} F(x_1)F(x_2)F(x_3)F(x_4) = \sum_{x_1<x_2<x_3<x_4}\left(\sum_{k=1}^{2^n-1} c_k {x_1}^k \sum_{l=1}^{2^n-1} c_l {x_2}^l \sum_{h=1}^{2^n-1} c_h {x_3}^h \sum_{f=1}^{2^n-1} c_f {x_4}^f\right).$$

Представим элементы x_1,x_2,x_3,x_4 через примитивный элемент θ поля Q и поменяем порядки суммирования:

$$n_2 = \sum_{0\leqslant s<t<p<v\leqslant 2^n-2}\left(\sum_{k,l,h,f=1}^{2^n-1} c_kc_lc_hc_f(\theta^s)^k(\theta^t)^l(\theta^p)^h(\theta^v)^f\right) = \sum_{k,l,h,f=1}^{2^n-1} c_kc_lc_hc_f \sum_{0\leqslant s<t<p<v\leqslant 2^n-2} \theta^{sk}\theta^{tl}\theta^{ph}\theta^{vf} =$$
$$= \sum_{k,l,h,f=1}^{2^n-1} c_kc_lc_hc_f \sum_{s=0}^{2^n-5}\left(\theta^{sk}\sum_{t=s+1}^{2^n-4}\left[\theta^{tl}\sum_{p=t+1}^{2^n-3}\left(\theta^{ph}\sum_{v=p+1}^{2^n-2}\theta^{vf}\right)\right]\right).$$

Далее многократно будем применять лемму 4 и, чтобы избежать деления на ноль, будем выделять слагаемые, для которых в показателе θ присутствует 2^n-1, так как $\theta^{2^n-1}=1$:

$$n_2 = \sum_{\substack{k,l,h,f=1\\ f\neq 2^n-1}}^{2^n-1} c_kc_lc_hc_f \sum_{s=0}^{2^n-5}\left(\theta^{sk}\sum_{t=s+1}^{2^n-4}\left[\theta^{tl}\sum_{p=t+1}^{2^n-3}\theta^{ph}\frac{\theta^{(p+1)f}(\theta^{(2^n-2-p)f}-1)}{\theta^f-1}\right]\right)+$$
$$+\sum_{\substack{k,l,h=1\\ f=2^n-1}}^{2^n-1} c_kc_lc_hc_f \sum_{s=0}^{2^n-5}\left(\theta^{sk}\sum_{t=s+1}^{2^n-4}\left[\theta^{tl}\sum_{p=t+1}^{2^n-3}\theta^{ph}(2^n-2-p)\right]\right).$$

Всюду далее для сокращения формы записи вместо $\sum\limits_{\substack{k,l,h,f=1\\ f\neq 2^n-1}}^{2^n-1}$ будем писать $\sum\limits_{f\neq 2^n-1}$; продолжим:

$$n_2 = \sum_{f\neq 2^n-1} c_kc_lc_hc_f \sum_{s=0}^{2^n-5}\left(\theta^{sk}\sum_{t=s+1}^{2^n-4}\left[\theta^{tl}\sum_{p=t+1}^{2^n-3}\frac{\theta^{ph}-\theta^f\cdot\theta^{p(h+f)}}{\theta^f-1}\right]\right)+$$
$$+\sum_{f=2^n-1} c_kc_lc_hc_f \sum_{s=0}^{2^n-5}\left(\theta^{sk}\sum_{t=s+1}^{2^n-4}\left[\theta^{tl}\sum_{p=t+1}^{2^n-3}\theta^{ph}p\right]\right) = \sum_{f\neq 2^n-1}\frac{c_kc_lc_hc_f}{\theta^f-1}\sum_{s=0}^{2^n-5}\left(\theta^{sk}\sum_{t=s+1}^{2^n-4}\left[\theta^{tl}\sum_{p=t+1}^{2^n-3}\theta^{ph}\right]\right)+$$
$$+\sum_{f\neq 2^n-1}\frac{c_kc_lc_hc_f\theta^f}{\theta^f-1}\sum_{s=0}^{2^n-5}\left(\theta^{sk}\sum_{t=s+1}^{2^n-4}\left[\theta^{tl}\sum_{p=t+1}^{2^n-3}\theta^{p(h+f)}\right]\right)+\sum_{f=2^n-1} c_kc_lc_hc_f\sum_{s=0}^{2^n-5}\left(\theta^{sk}\sum_{t=s+1}^{2^n-4}\left[\theta^{tl}\sum_{p=t+1}^{2^n-3}p\theta^{ph}\right]\right).$$

Обозначим суммы:

$$A = \sum_{f\neq 2^n-1}\frac{c_kc_lc_hc_f}{\theta^f-1}\sum_{s=0}^{2^n-5}\left(\theta^{sk}\sum_{t=s+1}^{2^n-4}\left[\theta^{tl}\sum_{p=t+1}^{2^n-3}\theta^{ph}\right]\right);$$
$$B = \sum_{f\neq 2^n-1}\frac{c_kc_lc_hc_f\theta^f}{\theta^f-1}\sum_{s=0}^{2^n-5}\left(\theta^{sk}\sum_{t=s+1}^{2^n-4}\left[\theta^{tl}\sum_{p=t+1}^{2^n-3}\theta^{p(h+f)}\right]\right);$$
$$D = \sum_{f=2^n-1} c_kc_lc_hc_f\sum_{s=0}^{2^n-5}\left(\theta^{sk}\sum_{t=s+1}^{2^n-4}\left[\theta^{tl}\sum_{p=t+1}^{2^n-3}p\theta^{ph}\right]\right).$$

Посчитаем их отдельно:

$$A = \sum_{f\neq 2^n-1}\frac{c_kc_lc_hc_f}{\theta^f-1}\sum_{s=0}^{2^n-5}\theta^{sk}\sum_{t=s+1}^{2^n-4}\theta^{tl}\sum_{p=t+1}^{2^n-3}\theta^{ph} = \sum_{f,h\neq 2^n-1}\frac{c_kc_lc_hc_f}{\theta^f-1}\sum_{s=0}^{2^n-5}\theta^{sk}\sum_{t=s+1}^{2^n-4}\theta^{tl}\theta^{(t+1)h}\frac{\theta^{(2^n-3-t)h}-1}{\theta^h-1}+$$
$$+\sum_{\substack{f\neq 2^n-1\\ h=2^n-1}}\frac{c_kc_lc_hc_f}{\theta^f-1}\sum_{s=0}^{2^n-5}\theta^{sk}\sum_{t=s+1}^{2^n-4}\theta^{tl}(2^n-3-t) = \sum_{f,h\neq 2^n-1}\frac{c_kc_lc_hc_f}{\theta^f-1}\sum_{s=0}^{2^n-5}\theta^{sk}\sum_{t=s+1}^{2^n-4}\theta^{tl}\frac{\theta^{-h}-\theta^{th}\theta^h}{\theta^h-1}+$$

$$+\sum_{\substack{f\neq 2^n-1\\ h=2^n-1}}\frac{c_kc_lc_hc_f}{\theta^f-1}\sum_{s=0}^{2^n-5}\theta^{sk}\sum_{t=s+1}^{2^n-4}(t+1)\theta^{tl}=\sum_{f,h\neq 2^n-1}\frac{c_kc_lc_hc_f}{(\theta^f-1)(\theta^h-1)\theta^h}\sum_{s=0}^{2^n-5}\theta^{sk}\sum_{t=s+1}^{2^n-4}\theta^{tl}+$$

$$+\sum_{f,h\neq 2^n-1}\frac{c_kc_lc_hc_f}{(\theta^f-1)(\theta^h-1)}\theta^h\sum_{s=0}^{2^n-5}\theta^{sk}\sum_{t=s+1}^{2^n-4}\theta^{t(l+h)}+\sum_{\substack{f\neq 2^n-1\\ h=2^n-1}}\frac{c_kc_lc_hc_f}{\theta^f-1}\sum_{s=0}^{2^n-5}\theta^{sk}\sum_{t=s+1}^{2^n-4}(t+1)\theta^{tl}.$$

Обозначим первую после последнего знака равенства сумму A_1, вторую — A_2, третью — A_3:

$$A_1=\sum_{f,h\neq 2^n-1}\frac{c_kc_lc_hc_f}{(\theta^f-1)(\theta^h-1)\theta^h}\sum_{s=0}^{2^n-5}\theta^{sk}\sum_{t=s+1}^{2^n-4}\theta^{tl}=\sum_{f,h,l\neq 2^n-1}\frac{c_kc_lc_hc_f}{(\theta^f-1)(\theta^h-1)\theta^h}\sum_{s=0}^{2^n-5}\theta^{sk}\frac{\theta^{-2l}-\theta^{ls}\theta^l}{\theta^l-1}+$$

$$+\sum_{\substack{f,h\neq 2^n-1\\ l=2^n-1}}\frac{c_kc_lc_hc_f}{(\theta^f-1)(\theta^h-1)\theta^h}\sum_{s=0}^{2^n-5}\theta^{sk}(2^n-4-s)=\sum_{f,h,l\neq 2^n-1}\frac{c_kc_lc_hc_f}{(\theta^f-1)(\theta^h-1)(\theta^l-1)\theta^h\theta^{2l}}\sum_{s=0}^{2^n-5}\theta^{sk}+$$

$$+\sum_{f,h,l\neq 2^n-1}\frac{c_kc_lc_hc_f}{(\theta^f-1)(\theta^h-1)(\theta^l-1)\theta^h}\theta^l\sum_{s=0}^{2^n-5}\theta^{s(k+l)}+\sum_{\substack{f,h,l\neq 2^n-1\\ l=2^n-1}}\frac{c_kc_lc_hc_f}{(\theta^f-1)(\theta^h-1)\theta^h}\sum_{s=0}^{2^n-5}s\theta^{sk}=$$

$$=\sum_{f,h,l,k\neq 2^n-1}\frac{c_kc_lc_hc_f}{(\theta^f-1)(\theta^h-1)(\theta^l-1)\theta^h\theta^{2l}}\,\frac{\theta^{(2^n-4)k}-1}{\theta^k-1}+\sum_{\substack{f,h,l\neq 2^n-1\\ k=2^n-1}}\frac{c_kc_lc_hc_f}{(\theta^f-1)(\theta^h-1)(\theta^l-1)\theta^h\theta^{2l}}\underbrace{(2^n-4)}_{=0}+$$

$$+\sum_{f,h,l,k+l\neq 2^n-1}\frac{c_kc_lc_hc_f}{(\theta^f-1)(\theta^h-1)(\theta^l-1)\theta^h}\theta^l\,\frac{\theta^{(2^n-4)(k+l)}-1}{\theta^{k+l}-1}+0+$$

$$+\sum_{\substack{f,h\neq 2^n-1\\ l=2^n-1}}\frac{c_kc_lc_hc_f}{(\theta^f-1)(\theta^h-1)\theta^h}\sum_{s=0}^{2^n-5}s\theta^{(s-1)k}\theta^k=\sum_{f,h,l,k\neq 2^n-1}\frac{c_kc_lc_hc_f}{(\theta^f-1)(\theta^h-1)(\theta^l-1)(\theta^k-1)\theta^h\theta^{2l}\theta^{3k}}(1-\theta^{3k})+$$

$$+\sum_{f,h,l,k+l\neq 2^n-1}\frac{c_kc_lc_hc_f\theta^l}{(\theta^f-1)(\theta^h-1)(\theta^l-1)(\theta^{k+l}-1)\theta^h\theta^{3(k+l)}}(1-\theta^{3(k+l)})+$$

$$+\sum_{\substack{f,h\neq 2^n-1\\ l=2^n-1}}\frac{c_kc_lc_hc_f\theta^k}{(\theta^f-1)(\theta^h-1)\theta^h}\sum_{s=0}^{2^n-5}s(\theta^k)^{(s-1)}.$$

С помощью леммы 4 вычислим сумму $\sum\limits_{s=0}^{2^n-5}s(\theta^k)^{s-1}$ при $k\neq 2^n-1$, так как при $k=2^n-1$ она равна нулю:

$$\sum_{s=0}^{2^n-4}s(\theta^k)^{s-1}=\left(\sum_{s=1}^{2^n-4}x^s\right)'_{x=\theta^k}=\frac{1-\theta^{3k}}{\theta^{3k}(\theta^k-1)^2}.$$

Получаем, что

$$A_1=\sum_{f,h,l,k\neq 2^n-1}\frac{c_kc_lc_hc_f}{(\theta^f-1)(\theta^h-1)(\theta^l-1)(\theta^k-1)\theta^h\theta^{2l}\theta^{3k}}(1-\theta^{3k})+$$

$$+\sum_{f,h,l,k+l\neq 2^n-1}\frac{c_kc_lc_hc_f\theta^l}{(\theta^f-1)(\theta^h-1)(\theta^l-1)(\theta^{k+l}-1)\theta^h\theta^{3(k+l)}}(1-\theta^{3(k+l)})+$$

$$+\sum_{\substack{f,h,k\neq 2^n-1\\ l=2^n-1}}\frac{c_kc_lc_hc_f\theta^k}{(\theta^f-1)(\theta^h-1)(\theta^k-1)^2\theta^h\theta^{3k}}(1-\theta^{3k}).$$

Вычисление суммы A_2 повторяет вычисление A_1. Поэтому с учётом замены $l\mapsto l+h$ имеем

$$A_2=\sum_{f,h,l+h,k\neq 2^n-1}\frac{c_kc_lc_hc_f}{(\theta^f-1)(\theta^h-1)(\theta^{l+h}-1)(\theta^k-1)\theta^h\theta^{2l}\theta^{3k}}(1-\theta^{3k})+$$

$$+\sum_{f,h,l+h,k+l+h\neq 2^n-1}\frac{c_kc_lc_hc_f}{(\theta^f-1)(\theta^h-1)(\theta^{l+h}-1)(\theta^{k+l+h}-1)\theta^h\theta^{2l}\theta^{3k}}(1-\theta^{3(k+l+h)})+$$

$$+\sum_{\substack{f,h,k\neq 2^n-1\\ l+h=2^n-1}}\frac{c_kc_lc_hc_f\theta^k\theta^h}{(\theta^f-1)(\theta^h-1)(\theta^k-1)^2\theta^{3k}}(1-\theta^{3k}).$$

Теперь вычислим $A_3=\sum\limits_{\substack{f\neq 2^n-1\\ h=2^n-1}}\dfrac{c_kc_lc_hc_f}{\theta^f-1}\sum\limits_{s=0}^{2^n-5}\theta^{sk}\sum\limits_{t=s+1}^{2^n-4}(t+1)\theta^{tl}$. Для этого воспользуемся леммой 4 и посчитаем сумму $\sum\limits_{t=s+1}^{2^n-4}(t+1)\theta^{tl}$ при $l\neq 2^n-1$:

$$\sum_{t=s+1}^{2^n-4}(t+1)\theta^{tl} = \left(\sum_{t=s+1}^{2^n-4} x^{t+1}\right)'_{x=\theta^l} = \frac{(s+1)\theta^{l(s+2)} - s\theta^{l(s+1)} - \theta^{-l}}{(\theta^l-1)^2}.$$

Подставляя полученное выражение в A_3, имеем

$$A_3 = \sum_{\substack{f,l\neq 2^n-1\\ h=2^n-1}} \frac{c_k c_l c_h c_f}{\theta^f - 1} \sum_{s=0}^{2^n-5} \theta^{sk} \frac{(s+1)\theta^{l(s+2)} - s\theta^{l(s+1)} - \theta^{-l}}{(\theta^l-1)^2} + \sum_{\substack{f\neq 2^n-1\\ h,l=2^n-1}} \frac{c_k c_l c_h c_f}{\theta^f - 1} \sum_{s=0}^{2^n-5} \theta^{sk} \sum_{t=s+2}^{2^n-3} t =$$

$$= \sum_{\substack{f,l\neq 2^n-1\\ h=2^n-1}} \frac{c_k c_l c_h c_f}{(\theta^f-1)(\theta^l-1)^2} \sum_{s=0}^{2^n-5}(s+1)\theta^{s(l+k)}\theta^{2l} + \sum_{\substack{f,l\neq 2^n-1\\ h=2^n-1}} \frac{c_k c_l c_h c_f}{(\theta^f-1)(\theta^l-1)^2} \sum_{s=0}^{2^n-5} s\theta^{s(l+k)}\theta^{l} +$$

$$+ \sum_{\substack{f,l\neq 2^n-1\\ h=2^n-1}} \frac{c_k c_l c_h c_f}{(\theta^f-1)(\theta^l-1)^2} \sum_{s=0}^{2^n-5} \theta^{sk}\theta^{-l} + \sum_{\substack{f\neq 2^n-1\\ h,l=2^n-1}} \frac{c_k c_l c_h c_f}{(\theta^f-1)} \sum_{s=0}^{2^n-5} \theta^{sk} \sum_{t=s+2}^{2^n-3} t.$$

Обозначим последние четыре суммы $A_{3.1}$, $A_{3.2}$, $A_{3.3}$, $A_{3.4}$ соответственно; вычислим их:

$$A_{3.1} = \sum_{\substack{f,l\neq 2^n-1\\ h=2^n-1}} \frac{c_k c_l c_h c_f}{(\theta^f-1)(\theta^l-1)^2} \sum_{s=0}^{2^n-5}(s+1)\theta^{s(l+k)}\theta^{2l} =$$

$$= \sum_{\substack{f,l,l+k\neq 2^n-1\\ h=2^n-1}} \frac{c_k c_l c_h c_f \theta^{2l}}{(\theta^f-1)(\theta^l-1)^2} \left(\sum_{s=0}^{2^n-5}(s+1)x^s\right)'_{x=\theta^{l+k}} + \sum_{\substack{f,l\neq 2^n-1\\ h,l+k=2^n-1}} \frac{c_k c_l c_h c_f \theta^{2l}}{(\theta^f-1)(\theta^l-1)^2} \sum_{s=1}^{2^n-5} s.$$

С учетом равенства $\sum\limits_{s=0}^{2^n-5}(s+1)x^s = \left(\sum\limits_{s=1}^{2^n-4} x^s\right)'$ имеем

$$A_{3.1} = \sum_{\substack{f,l,l+k\neq 2^n-1\\ h=2^n-1}} \frac{c_k c_l c_h c_f}{(\theta^f-1)(\theta^l-1)^2(\theta^{k+l}-1)^2\theta^l\theta^{3k}}(1-\theta^{3(k+l)}).$$

Рассмотрим $A_{3.2}$:

$$A_{3.2} = \sum_{\substack{f,l\neq 2^n-1\\ h=2^n-1}} \frac{c_k c_l c_h c_f}{(\theta^f-1)(\theta^l-1)^2} \sum_{s=0}^{2^n-5} s(\theta^{l+k})^{s-1}\theta^l\theta^{l+k} = \sum_{\substack{f,l,l+k\neq 2^n-1\\ h=2^n-1}} \frac{c_k c_l c_h c_f \theta^{2l}\theta^k}{(\theta^f-1)(\theta^l-1)^2} \left(\sum_{s=1}^{2^n-5} x^s\right)'_{x=\theta^{l+k}} + 0 =$$

$$= \sum_{\substack{f,l,l+k\neq 2^n-1\\ h=2^n-1}} \frac{c_k c_l c_h c_f \theta^{2l}\theta^k}{(\theta^f-1)(\theta^l-1)^2} \frac{1-\theta^{-3(l+k)}}{(\theta^{l+k}-1)^2} = \sum_{\substack{f,l,l+k\neq 2^n-1\\ h=2^n-1}} \frac{c_k c_l c_h c_f \theta^{2l}\theta^k}{(\theta^f-1)(\theta^l-1)^2(\theta^{l+k}-1)^2} \frac{1-\theta^{3(l+k)}}{\theta^{3(l+k)}}.$$

Теперь вычислим $A_{3.3}$:

$$A_{3.3} = \sum_{\substack{f,l\neq 2^n-1\\ h=2^n-1}} \frac{c_k c_l c_h c_f}{(\theta^f-1)(\theta^l-1)^2} \sum_{s=0}^{2^n-5}\theta^{sk}\theta^{-l} = \sum_{\substack{f,l,k\neq 2^n-1\\ h=2^n-1}} \frac{c_k c_l c_h c_f}{(\theta^f-1)(\theta^l-1)^2\theta^l} \frac{\theta^{(2^n-4)k}-1}{\theta^k-1} + 0 =$$

$$= \sum_{\substack{f,l,k\neq 2^n-1\\ h=2^n-1}} \frac{c_k c_l c_h c_f}{(\theta^f-1)(\theta^l-1)^2(\theta^k-1)\theta^l} \frac{1-\theta^{3k}}{\theta^{3k}}.$$

Осталось вычислить $A_{3.4}$:

$$A_{3.4} = \sum_{\substack{f\neq 2^n-1\\ h,l=2^n-1}} \frac{c_k c_l c_h c_f}{(\theta^f-1)} \sum_{s=0}^{2^n-5}\theta^{sk} \sum_{t=s+2}^{2^n-3} t = \sum_{\substack{f\neq 2^n-1\\ h,l=2^n-1}} \frac{c_k c_l c_h c_f}{(\theta^f-1)} \sum_{t=2}^{2^n-3} t \sum_{s=0}^{t-2}\theta^{sk} =$$

$$= \sum_{\substack{f,k\neq 2^n-1\\ h,l=2^n-1}} \frac{c_k c_l c_h c_f}{(\theta^f-1)} \sum_{t=2}^{2^n-3} t\frac{\theta^{(t-1)k}-1}{\theta^k-1} + \sum_{\substack{f\neq 2^n-1\\ h,l,k=2^n-1}} \frac{c_k c_l c_h c_f}{(\theta^f-1)} \sum_{t=2}^{2^n-3} \underbrace{t(t-1)}_{=0} =$$

$$= \sum_{\substack{f,k\neq 2^n-1\\ h,l=2^n-1}} \frac{c_k c_l c_h c_f}{(\theta^f-1)(\theta^k-1)} \sum_{t=2}^{2^n-3} t(\theta^k)^{t-1} + \sum_{\substack{f,k\neq 2^n-1\\ h,l=2^n-1}} \frac{c_k c_l c_h c_f}{(\theta^f-1)(\theta^k-1)} \underbrace{\sum_{t=2}^{2^n-3} t}_{=0} =$$

$$= \sum_{\substack{f,k\neq 2^n-1\\ h,l=2^n-1}} \frac{c_k c_l c_h c_f}{(\theta^f-1)(\theta^k-1)} \left(\sum_{t=2}^{2^n-3} x^t\right)'_{x=\theta^k}.$$

Для завершения вычисления $A_{3.4}$ осталось применить лемму 4 и вычислить

$$\left(\sum_{t=2}^{2^n-3} x^t\right)'_{x=\theta^k} = \frac{1+\theta^{3k}}{\theta^k(\theta^k-1)^2}.$$

В итоге получаем $A_{3.4} = \sum\limits_{\substack{f,k\neq 2^n-1\\ h,l=2^n-1}} \dfrac{c_kc_lc_hc_f}{(\theta^f-1)(\theta^k-1)^3\theta^k}(1-\theta^{3k})$.

Собирая все суммы вместе, получаем

$$A = A_1+A_2+A_3 = \sum_{f,h,l,k\neq 2^n-1} \frac{c_kc_lc_hc_f}{(\theta^f-1)(\theta^h-1)(\theta^l-1)(\theta^k-1)\theta^h\theta^{2l}\theta^{3k}}(1-\theta^{3k}) +$$
$$+\sum_{f,h,l,k+l\neq 2^n-1} \frac{c_kc_lc_hc_f\theta^l}{(\theta^f-1)(\theta^h-1)(\theta^l-1)(\theta^{k+l}-1)\theta^h\theta^{3(k+l)}}(1-\theta^{3(k+l)}) +$$
$$+\sum_{\substack{f,h,k\neq 2^n-1\\ l=2^n-1}} \frac{c_kc_lc_hc_f\theta^k}{(\theta^f-1)(\theta^h-1)(\theta^k-1)^2\theta^h\theta^{3k}}(1-\theta^{3k}) +$$
$$+\sum_{f,h,l+h,k\neq 2^n-1} \frac{c_kc_lc_hc_f}{(\theta^f-1)(\theta^h-1)(\theta^{l+h}-1)(\theta^k-1)\theta^h\theta^{2l}\theta^{3k}}(1-\theta^{3k}) +$$
$$+\sum_{f,h,l+h,k+l+h\neq 2^n-1} \frac{c_kc_lc_hc_f}{(\theta^f-1)(\theta^h-1)(\theta^{l+h}-1)(\theta^{k+l+h}-1)\theta^h\theta^{2l}\theta^{3k}}(1-\theta^{3(k+l+h)}) +$$
$$+\sum_{\substack{f,h,k\neq 2^n-1\\ l+h=2^n-1}} \frac{c_kc_lc_hc_f\theta^k\cdot\theta^h}{(\theta^f-1)(\theta^h-1)(\theta^k-1)^2\theta^{3k}}(1-\theta^{3k}) + \sum_{\substack{f,l,l+k\neq 2^n-1\\ h=2^n-1}} \frac{c_kc_lc_hc_f}{(\theta^f-1)(\theta^l-1)^2(\theta^{k+l}-1)^2\theta^l\theta^{3k}}(1-\theta^{3(k+l)}) +$$
$$+\sum_{\substack{f,l,l+k\neq 2^n-1\\ h=2^n-1}} \frac{c_kc_lc_hc_f\theta^{2l}\theta^k}{(\theta^f-1)(\theta^l-1)^2(\theta^{l+k}-1)^2}\,\frac{1-\theta^{3(l+k)}}{\theta^{3(l+k)}} +$$
$$+\sum_{\substack{f,l,k\neq 2^n-1\\ h=2^n-1}} \frac{c_kc_lc_hc_f}{(\theta^f-1)(\theta^l-1)^2(\theta^k-1)\theta^l}\,\frac{1-\theta^{3k}}{\theta^{3k}} + \sum_{\substack{f,k\neq 2^n-1\\ h,l=2^n-1}} \frac{c_kc_lc_hc_f}{(\theta^f-1)(\theta^k-1)^3\theta^k}(1-\theta^{3k}).$$

Сравнивая суммы A и B, можно заметить, что B получается из A заменой $h\mapsto h+f$ и умножением на θ^f. Поэтому сразу выпишем B:

$$B = \sum_{\substack{f,l,k\neq 2^n-1\\ h+f\neq 2^n-1}} \frac{c_kc_lc_hc_f(1-\theta^{3k})}{(\theta^f-1)(\theta^{h+f}-1)(\theta^l-1)(\theta^k-1)\theta^h\theta^{2l}\theta^{3k}} +$$
$$+\sum_{\substack{f,l,k+l\neq 2^n-1\\ h+f\neq 2^n-1}} \frac{c_kc_lc_hc_f\theta^l(1-\theta^{3(k+l)})}{(\theta^f-1)(\theta^{h+f}-1)(\theta^l-1)(\theta^{k+l}-1)\theta^h\theta^{3(k+l)}} + \sum_{\substack{f,h+f,k\neq 2^n-1\\ l=2^n-1}} \frac{c_kc_lc_hc_f\theta^k(1-\theta^{3k})}{(\theta^f-1)(\theta^{h+f}-1)(\theta^k-1)^2\theta^h\theta^{3k}} +$$
$$+\sum_{\substack{f,h+f,k\neq 2^n-1\\ l+h+f\neq 2^n-1}} \frac{c_kc_lc_hc_f(1-\theta^{3k})}{(\theta^f-1)(\theta^{h+f}-1)(\theta^{l+h+f}-1)(\theta^k-1)\theta^h\theta^{2l}\theta^{3k}} +$$
$$+\sum_{\substack{f,k+l+h+f\neq 2^n-1\\ h+f,l+h+f\neq 2^n-1}} \frac{c_kc_lc_hc_f(1-\theta^{3(l+h+f+k)})}{(\theta^f-1)(\theta^{h+f}-1)(\theta^{l+h+f}-1)(\theta^{l+h+f+k}-1)\theta^h\theta^{2l}\theta^{3k}} +$$
$$+\sum_{\substack{f,h+f,k\neq 2^n-1\\ l+h+f=2^n-1}} \frac{c_kc_lc_hc_f\theta^{h+k}\theta^{2f}(1-\theta^{3k})}{(\theta^f-1)(\theta^{h+f}-1)(\theta^k-1)^2\theta^{3k}} + \sum_{\substack{f,l,l+k\neq 2^n-1\\ h+f=2^n-1}} \frac{c_kc_lc_hc_f\theta^f(1-\theta^{3(k+l)})}{(\theta^f-1)(\theta^l-1)^2(\theta^{k+l}-1)^2\theta^l\theta^{3k}} +$$
$$+\sum_{\substack{f,l,l+k\neq 2^n-1\\ h+f=2^n-1}} \frac{c_kc_lc_hc_f\theta^f\theta^{2l}\theta^k}{(\theta^f-1)(\theta^l-1)^2(\theta^{l+k}-1)^2}\,\frac{1-\theta^{3(l+k)}}{\theta^{3(l+k)}} + \sum_{\substack{f,l,k\neq 2^n-1\\ h+f=2^n-1}} \frac{c_kc_lc_hc_f\theta^f}{(\theta^f-1)(\theta^l-1)^2(\theta^k-1)\theta^l}\,\frac{1-\theta^{3k}}{\theta^{3k}} +$$
$$+\sum_{\substack{f,k\neq 2^n-1\\ h+f,l=2^n-1}} \frac{c_kc_lc_hc_f\theta^f}{(\theta^f-1)(\theta^k-1)^3\theta^k}(1-\theta^{3k}).$$

Осталось посчитать последнюю сумму:

$$D = \sum_{f=2^n-1} c_kc_lc_hc_f \sum_{s=0}^{2^n-5}\left(\theta^{sk}\sum_{t=s+1}^{2^n-4}\left[\theta^{tl}\sum_{p=t+1}^{2^n-3} p\theta^{ph}\right]\right) = \sum_{\substack{h\neq 2^n-1\\ f=2^n-1}} c_kc_lc_hc_f \sum_{s=0}^{2^n-5}\theta^{sk}\sum_{t=s+1}^{2^n-4}\theta^{tl}\sum_{p=t+1}^{2^n-3} p(\theta^h)^{p-1}\theta^h +$$

$$+\sum_{f,h=2^n-1} c_k c_l c_h c_f \sum_{s=0}^{2^n-5} \theta^{sk} \sum_{t=s+1}^{2^n-4} \theta^{tl} \sum_{p=t+1}^{2^n-3} p = \sum_{\substack{h\neq 2^n-1\\ f=2^n-1}} c_k c_l c_h c_f \sum_{s=0}^{2^n-5} \theta^{sk} \sum_{t=s+1}^{2^n-4} \theta^{tl}\theta^h \left(\sum_{p=t+1}^{2^n-3} x^p\right)'_{x=\theta^h} +$$

$$+\sum_{f,h=2^n-1} c_k c_l c_h c_f \sum_{s=0}^{2^n-5} \theta^{sk} \sum_{t=s+1}^{2^n-4} \theta^{tl} \sum_{p=t+1}^{2^n-3} p.$$

Обозначим последние две суммы D_1 и D_2 соответственно. Для вычисления D_1 сначала посчитаем следующую сумму:

$$\left(\sum_{p=t+1}^{2^n-3} x^p\right)'_{x=\theta^h} = \frac{t\theta^{h(t+1)} - (t+1)\theta^{th} - \theta^{-h}}{(\theta^h-1)^2}.$$

Вернёмся к D_1:

$$D_1 = \sum_{\substack{h\neq 2^n-1\\ f=2^n-1}} c_k c_l c_h c_f \theta^h \sum_{s=0}^{2^n-5} \theta^{sk} \sum_{t=s+1}^{2^n-4} \theta^{tl} \frac{t\theta^{h(t+1)} - (t+1)\theta^{th} - \theta^{-h}}{(\theta^h-1)^2} =$$

$$= \sum_{\substack{h\neq 2^n-1\\ f=2^n-1}} \frac{c_k c_l c_h c_f \theta^h}{(\theta^h-1)^2} \sum_{s=0}^{2^n-5} \theta^{sk} \sum_{t=s+1}^{2^n-4} \left(t\theta^{t(l+h)}\theta^h - (t+1)\theta^{t(h+l)} - \theta^{tl}\theta^{-h}\right) =$$

$$= \sum_{\substack{h\neq 2^n-1\\ f=2^n-1}} \frac{c_k c_l c_h c_f \theta^{2h}}{(\theta^h-1)^2} \sum_{s=0}^{2^n-5} \theta^{sk} \sum_{t=s+1}^{2^n-4} t\theta^{t(l+h)} + \sum_{\substack{h\neq 2^n-1\\ f=2^n-1}} \frac{c_k c_l c_h c_f \theta^{h}}{(\theta^h-1)^2} \sum_{s=0}^{2^n-5} \theta^{sk} \sum_{t=s+1}^{2^n-4} (t+1)\theta^{t(h+l)} +$$

$$+ \sum_{\substack{h\neq 2^n-1\\ f=2^n-1}} \frac{c_k c_l c_h c_f}{(\theta^h-1)^2} \sum_{s=0}^{2^n-5} \theta^{sk} \sum_{t=s+1}^{2^n-4} \theta^{tl}.$$

Обозначим получившиеся суммы $D_{1.1}$, $D_{1.2}$ и $D_{1.3}$ соответственно. Тогда

$$D_{1.1} = \sum_{\substack{h\neq 2^n-1\\ f=2^n-1}} \frac{c_k c_l c_h c_f \theta^{2h}}{(\theta^h-1)^2} \sum_{s=0}^{2^n-5} \theta^{sk} \sum_{t=s+1}^{2^n-4} t\theta^{(t-1)(l+h)}\theta^{l+h} =$$

$$= \sum_{\substack{h,l+h\neq 2^n-1\\ f=2^n-1}} \frac{c_k c_l c_h c_f \theta^{2h}}{(\theta^h-1)^2} \sum_{s=0}^{2^n-5} \theta^{sk}\theta^{l+h} \left(\sum_{t=s+1}^{2^n-4} x^t\right)'_{x=\theta^{l+h}} + \sum_{\substack{h\neq 2^n-1\\ f,l+h=2^n-1}} \frac{c_k c_l c_h c_f \theta^{2h}}{(\theta^h-1)^2} \sum_{s=0}^{2^n-5} \theta^{sk} \sum_{t=s+1}^{2^n-4} t.$$

С использованием леммы 4 выпишем значение

$$\left(\sum_{t=s+1}^{2^n-4} x^t\right)'_{x=\theta^{l+h}} = \frac{\theta^{-3(l+h)} - s\theta^{(l+h)(s+1)} - (s+1)\theta^{(l+h)s}}{(\theta^{l+h}-1)^2}.$$

Подставляя это выражение в $D_{1.1}$, получаем

$$D_{1.1} = \sum_{\substack{h,l+h\neq 2^n-1\\ f=2^n-1}} \frac{c_k c_l c_h c_f \theta^{2h}\theta^{l+h}}{(\theta^h-1)^2} \sum_{s=0}^{2^n-5} \theta^{sk} \frac{\theta^{-3(l+h)} - s\theta^{(l+h)(s+1)} - (s+1)\theta^{(l+h)s}}{(\theta^{l+h}-1)^2} +$$

$$+ \sum_{\substack{h\neq 2^n-1\\ f,l+h=2^n-1}} \frac{c_k c_l c_h c_f \theta^{2h}}{(\theta^h-1)^2} \sum_{t=1}^{2^n-4} t \sum_{s=0}^{t-1} \theta^{sk} = \sum_{\substack{h,l+h\neq 2^n-1\\ f=2^n-1}} \frac{c_k c_l c_h c_f \theta^{2h}}{(\theta^h-1)^2(\theta^{l+h}-1)^2\theta^{2(l+h)}} \sum_{s=0}^{2^n-5} \theta^{sk} +$$

$$+ \sum_{\substack{h,l+h\neq 2^n-1\\ f=2^n-1}} \frac{c_k c_l c_h c_f \theta^{3h}\theta^l}{(\theta^h-1)^2(\theta^{l+h}-1)^2} \sum_{s=0}^{2^n-5} s\theta^{(l+h+k)s}\theta^{l+h} + \sum_{\substack{h,l+h\neq 2^n-1\\ f=2^n-1}} \frac{c_k c_l c_h c_f \theta^{3h}\theta^l}{(\theta^h-1)^2(\theta^{l+h}-1)^2} \sum_{s=0}^{2^n-5} (s+1)\theta^{(l+h+k)s} +$$

$$+ \sum_{\substack{h,k\neq 2^n-1\\ f,l+h=2^n-1}} \frac{c_k c_l c_h c_f \theta^{2h}}{(\theta^h-1)^2} \sum_{t=1}^{2^n-4} t\frac{\theta^{kt}-1}{\theta^k-1} + \sum_{\substack{h\neq 2^n-1\\ f,l+h,k=2^n-1}} \frac{c_k c_l c_h c_f \theta^{2h}}{(\theta^h-1)^2} \underbrace{\sum_{t=1}^{2^n-4} t\cdot t}_{=0} =$$

$$= \sum_{\substack{h,l+h,k\neq 2^n-1\\ f=2^n-1}} \frac{c_k c_l c_h c_f}{(\theta^h-1)^2(\theta^{l+h}-1)^2\theta^{2l}} \frac{1-\theta^{3k}}{\theta^{3k}(\theta^k-1)} +$$

$$+ \sum_{\substack{h,l+h,l+h+k\neq 2^n-1\\ f=2^n-1}} \frac{c_k c_l c_h c_f \theta^{4h}\theta^{2l}}{(\theta^h-1)^2(\theta^{l+h}-1)^2} \sum_{s=0}^{2^n-5} s\theta^{(l+h+k)(s-1)}\theta^{l+h+k} +$$

$$+ \sum_{\substack{h,l+h,l+h+k\neq 2^n-1\\ f=2^n-1}} \frac{c_k c_l c_h c_f \theta^{3h}\theta^l}{(\theta^h-1)^2(\theta^{l+h}-1)^2} \left(\sum_{s=0}^{2^n-5} x^{s+1}\right)'_{x=\theta^{l+h+k}} + \sum_{\substack{h,k\neq 2^n-1\\ f,l+h=2^n-1}} \frac{c_k c_l c_h c_f \theta^{2h}}{(\theta^h-1)^2(\theta^k-1)} \sum_{t=1}^{2^n-4} t\theta^{k(t-1)}\theta^k =$$

$$= \sum_{\substack{h,l+h,k\neq 2^n-1\\ f=2^n-1}} \frac{c_kc_lc_hc_f(1-\theta^{3k})}{(\theta^h-1)^2(\theta^{l+h}-1)^2(\theta^k-1)\theta^{2l}\theta^{3k}} + \sum_{\substack{h,l+h,l+h+k\neq 2^n-1\\ f=2^n-1}} \frac{c_kc_lc_hc_f\theta^{2h}\theta^k(1-\theta^{3(l+h+k)})}{(\theta^h-1)^2(\theta^{l+h}-1)^2(\theta^{l+h+k}-1)^2\theta^{3k}} +$$

$$+ \sum_{\substack{h,l+h,l+h+k\neq 2^n-1\\ f=2^n-1}} \frac{c_kc_lc_hc_f(1-\theta^{3(l+h+k)})}{(\theta^h-1)^2(\theta^{l+h}-1)^2(\theta^{l+h+k}-1)^2\theta^{2l}\theta^{3k}} + \sum_{\substack{h,k\neq 2^n-1\\ f,l+h=2^n-1}} \frac{c_kc_lc_hc_f\theta^{2h}(1-\theta^{3k})}{(\theta^h-1)^2(\theta^k-1)^3\theta^{2k}}.$$

Теперь посчитаем $D_{1.2}$:

$$D_{1.2} = \sum_{\substack{h,h+l\neq 2^n-1\\ f=2^n-1}} \frac{c_kc_lc_hc_f\theta^h}{(\theta^h-1)^2}\sum_{s=0}^{2^n-5}\theta^{sk}\left(\sum_{t=s+2}^{2^n-3}x^t\right)'_{x=\theta^{h+l}} + \sum_{\substack{h\neq 2^n-1\\ f,h+l=2^n-1}} \frac{c_kc_lc_hc_f\theta^h}{(\theta^h-1)^2}\sum_{s=0}^{2^n-5}\theta^{sk}\sum_{t=s+2}^{2^n-3}t.$$

По лемме 4 имеем $\left(\sum_{t=s+2}^{2^n-3}x^t\right)'_{x=\theta^{h+l}} = \dfrac{(s+1)\theta^{(h+l)(s+2)}-s\theta^{(h+l)(s+1)}-\theta^{-(h+l)}}{(\theta^{h+l}-1)^2}$. Вернёмся к вычислению $D_{1.2}$:

$$D_{1.2} = \sum_{\substack{h,h+l\neq 2^n-1\\ f=2^n-1}} \frac{c_kc_lc_hc_f\theta^h}{(\theta^h-1)^2}\sum_{s=0}^{2^n-5}\theta^{sk}\frac{(s+1)\theta^{(h+l)(s+2)}-s\theta^{(h+l)(s+1)}-\theta^{-(h+l)}}{(\theta^{h+l}-1)^2} +$$

$$+ \sum_{\substack{h\neq 2^n-1\\ f,h+l=2^n-1}} \frac{c_kc_lc_hc_f\theta^h}{(\theta^h-1)^2}\sum_{t=2}^{2^n-3}t\sum_{s=0}^{t-2}\theta^{sk}.$$

Заметим, что вторая сумма была посчитана в $A_{3.4}$. Продолжим преобразования:

$$D_{1.2} = \sum_{\substack{h,h+l\neq 2^n-1\\ f=2^n-1}} \frac{c_kc_lc_hc_f\theta^h}{(\theta^h-1)^2(\theta^{h+l}-1)^2}\sum_{s=0}^{2^n-5}(s+1)\theta^{(h+l+k)s}\theta^{2(h+l)} +$$

$$+ \sum_{\substack{h,h+l\neq 2^n-1\\ f=2^n-1}} \frac{c_kc_lc_hc_f\theta^h}{(\theta^h-1)^2(\theta^{h+l}-1)^2}\sum_{s=0}^{2^n-5}s\theta^{(h+l+k)s}\theta^{(h+l)} +$$

$$+ \sum_{\substack{h,h+l\neq 2^n-1\\ f=2^n-1}} \frac{c_kc_lc_hc_f\theta^h}{(\theta^h-1)^2(\theta^{h+l}-1)^2}\sum_{s=0}^{2^n-5}\theta^{sk}\theta^{-(h+l)} + \sum_{\substack{h,k\neq 2^n-1\\ f,h+l=2^n-1}} \frac{c_kc_lc_hc_f\theta^h(1-\theta^{3k})}{(\theta^h-1)^2(\theta^k-1)^3\theta^k} =$$

$$= \sum_{\substack{h,h+l,h+l+k\neq 2^n-1\\ f=2^n-1}} \frac{c_kc_lc_hc_f\theta^{3h}\theta^{2l}}{(\theta^h-1)^2(\theta^{h+l}-1)^2}\left(\sum_{s=1}^{2^n-4}x^s\right)'_{x=\theta^{h+l+k}} +$$

$$+ \sum_{\substack{h,h+l,h+l+k\neq 2^n-1\\ f=2^n-1}} \frac{c_kc_lc_hc_f\theta^{2h}\theta^l}{(\theta^h-1)^2(\theta^{h+l}-1)^2}\left(\sum_{s=1}^{2^n-5}x^s\right)'_{x=\theta^{h+l+k}}\theta^{h+l+k} +$$

$$+ \sum_{\substack{h,h+l,k\neq 2^n-1\\ f=2^n-1}} \frac{c_kc_lc_hc_f(1-\theta^{3k})}{(\theta^h-1)^2(\theta^{h+l}-1)^2(\theta^k-1)\theta^l\theta^{3k}} + \sum_{\substack{h,k\neq 2^n-1\\ f,h+l=2^n-1}} \frac{c_kc_lc_hc_f\theta^h(1-\theta^{3k})}{(\theta^h-1)^2(\theta^k-1)^3\theta^k} =$$

$$= \sum_{\substack{h,h+l,h+l+k\neq 2^n-1\\ f=2^n-1}} \frac{c_kc_lc_hc_f\theta^{3h}\theta^{2l}}{(\theta^h-1)^2(\theta^{h+l}-1)^2}\,\frac{1-\theta^{3(l+h+k)}}{\theta^{3(l+h+k)}(\theta^{l+h+k}-1)^2} +$$

$$+ \sum_{\substack{h,h+l,h+l+k\neq 2^n-1\\ f=2^n-1}} \frac{c_kc_lc_hc_f\theta^{2h}\theta^l}{(\theta^h-1)^2(\theta^{h+l}-1)^2}\,\frac{1-\theta^{3(l+h+k)}}{\theta^{2(l+h+k)}(\theta^{l+h+k}-1)^2} +$$

$$+ \sum_{\substack{h,h+l,k\neq 2^n-1\\ f=2^n-1}} \frac{c_kc_lc_hc_f(1-\theta^{3k})}{(\theta^h-1)^2(\theta^{h+l}-1)^2(\theta^k-1)\theta^l\theta^{3k}} + \sum_{\substack{h,k\neq 2^n-1\\ f,h+l=2^n-1}} \frac{c_kc_lc_hc_f\theta^h(1-\theta^{3k})}{(\theta^h-1)^2(\theta^k-1)^3\theta^k}.$$

Далее вычислим сумму $D_{1.3}$:

$$D_{1.3} = \sum_{\substack{h\neq 2^n-1\\ f=2^n-1}} \frac{c_kc_lc_hc_f}{(\theta^h-1)^2}\sum_{s=0}^{2^n-5}\theta^{sk}\sum_{t=s+1}^{2^n-4}\theta^{tl} = \sum_{\substack{h,l\neq 2^n-1\\ f=2^n-1}} \frac{c_kc_lc_hc_f}{(\theta^h-1)^2}\sum_{s=0}^{2^n-5}\theta^{sk}\frac{\theta^{(2^n-3)l}-\theta^{l(s+1)}}{\theta^l-1} +$$

$$+ \sum_{\substack{h\neq 2^n-1\\ f,l=2^n-1}} \frac{c_kc_lc_hc_f}{(\theta^h-1)^2}\sum_{s=0}^{2^n-5}\theta^{sk}\sum_{t=s+1}^{2^n-4}1 = \sum_{\substack{h,l\neq 2^n-1\\ f=2^n-1}} \frac{c_kc_lc_hc_f}{(\theta^h-1)^2(\theta^l-1)\theta^{2l}}\sum_{s=0}^{2^n-5}\theta^{sk} +$$

$$+ \sum_{\substack{h,l\neq 2^n-1\\ f=2^n-1}} \frac{c_kc_lc_hc_f\theta^l}{(\theta^h-1)^2(\theta^l-1)}\sum_{s=0}^{2^n-5}\theta^{s(l+k)} + \sum_{\substack{h\neq 2^n-1\\ f,l=2^n-1}} \frac{c_kc_lc_hc_f}{(\theta^h-1)^2}\sum_{s=0}^{2^n-5}s\theta^{(s-1)k}\theta^k =$$

$$= \sum_{\substack{k,h,l\neq 2^n-1\\ f=2^n-1}} \frac{c_kc_lc_hc_f}{(\theta^h-1)^2(\theta^l-1)\theta^{2l}}\,\frac{1-\theta^{3k}}{(\theta^k-1)\theta^{3k}} + \sum_{\substack{h,l,l+k\neq 2^n-1\\ f=2^n-1}} \frac{c_kc_lc_hc_f\theta^l}{(\theta^h-1)^2(\theta^l-1)}\,\frac{1-\theta^{3(l+k)}}{(\theta^{l+k}-1)\theta^{3(l+k)}} +$$

$$+ \sum_{\substack{h,k\neq 2^n-1\\ f,l=2^n-1}} \frac{c_kc_lc_hc_f\theta^k}{(\theta^h-1)^2}\left(\sum_{s=1}^{2^n-5} x^s\right)'_{x=\theta^k} = \sum_{\substack{k,h,l\neq 2^n-1\\ f=2^n-1}} \frac{c_kc_lc_hc_f}{(\theta^h-1)^2(\theta^l-1)\theta^{2l}}\,\frac{1-\theta^{3k}}{(\theta^k-1)\theta^{3k}} +$$

$$+ \sum_{\substack{h,l,l+k\neq 2^n-1\\ f=2^n-1}} \frac{c_kc_lc_hc_f\theta^l}{(\theta^h-1)^2(\theta^l-1)}\,\frac{1-\theta^{3(l+k)}}{(\theta^{l+k}-1)\theta^{3(l+k)}} + \sum_{\substack{h,k\neq 2^n-1\\ f,l=2^n-1}} \frac{c_kc_lc_hc_f\theta^k}{(\theta^h-1)^2}\,\frac{1-\theta^{3k}}{(\theta^k-1)^2\theta^{3k}}.$$

Осталось вычислить D_2:

$$D_2 = \sum_{f,h=2^n-1} c_kc_lc_hc_f \sum_{s=0}^{2^n-5}\theta^{sk}\sum_{t=s+1}^{2^n-4}\theta^{tl}\sum_{p=t+1}^{2^n-3} p = \sum_{f,h=2^n-1} c_kc_lc_hc_f \sum_{s=0}^{2^n-5}\theta^{sk}\sum_{p=s+2}^{2^n-3} p\sum_{t=s+1}^{p-1}\theta^{tl} =$$

$$= \sum_{\substack{l\neq 2^n-1\\ f,h=2^n-1}} c_kc_lc_hc_f \sum_{s=0}^{2^n-5}\theta^{sk}\sum_{p=s+2}^{2^n-3} p\theta^{(s+1)l}\,\frac{\theta^{(p-1-s)l}-1}{\theta^l-1} + \sum_{f,h,l=2^n-1} c_kc_lc_hc_f \sum_{s=0}^{2^n-5}\theta^{sk}\sum_{p=s+2}^{2^n-3} p(p-1-s) =$$

$$= \sum_{\substack{l\neq 2^n-1\\ f,h=2^n-1}} \frac{c_kc_lc_hc_f}{\theta^l-1} \sum_{s=0}^{2^n-5}\theta^{sk}\sum_{p=s+2}^{2^n-3} p\theta^{(p-1)l}\theta^l + \sum_{\substack{l\neq 2^n-1\\ f,h=2^n-1}} \frac{c_kc_lc_hc_f}{\theta^l-1} \sum_{s=0}^{2^n-5}\theta^{sk}\sum_{p=s+2}^{2^n-3} p\theta^{ls}\theta^l +$$

$$+ \sum_{f,h,l=2^n-1} c_kc_lc_hc_f \sum_{s=0}^{2^n-5}\theta^{sk}\sum_{p=s+2}^{2^n-3} (p(p-1)+ps) = \sum_{\substack{l\neq 2^n-1\\ f,h=2^n-1}} \frac{c_kc_lc_hc_f\theta^l}{\theta^l-1} \sum_{s=0}^{2^n-5}\theta^{sk}\left(\sum_{p=s+2}^{2^n-3} x^p\right)'_{x=\theta^l} +$$

$$+ \sum_{\substack{l\neq 2^n-1\\ f,h=2^n-1}} \frac{c_kc_lc_hc_f\theta^l}{\theta^l-1} \sum_{s=0}^{2^n-5}\theta^{s(l+k)}\sum_{p=s+2}^{2^n-3} p + \sum_{f,h,l=2^n-1} c_kc_lc_hc_f \sum_{s=0}^{2^n-5} s\theta^{sk}\sum_{p=s+2}^{2^n-3} p.$$

Обозначим три последние суммы $D_{2.1}$, $D_{2.2.}$ и $D_{2.3}$. Заметим, что $D_{2.1}$ вычисляется аналогично $D_{1.2}$:

$$D_{2.1} = \sum_{\substack{l\neq 2^n-1\\ f,h=2^n-1}} \frac{c_kc_lc_hc_f\theta^l}{\theta^l-1} \sum_{s=0}^{2^n-5}\theta^{sk}\left(\sum_{p=s+2}^{2^n-3} x^p\right)'_{x=\theta^l} =$$

$$= \sum_{\substack{l\neq 2^n-1\\ f,h=2^n-1}} \frac{c_kc_lc_hc_f\theta^l}{\theta^l-1} \sum_{s=0}^{2^n-5}\theta^{sk}\,\frac{(s+1)\theta^{l(s+2)}-s\theta^{l(s+1)}-\theta^{-l}}{(\theta^l-1)^2} =$$

$$= \sum_{\substack{l\neq 2^n-1\\ f,h=2^n-1}} \frac{c_kc_lc_hc_f\theta^{3l}}{(\theta^l-1)^3} \sum_{s=0}^{2^n-5}(s+1)\theta^{s(k+l)} + \sum_{\substack{l\neq 2^n-1\\ f,h=2^n-1}} \frac{c_kc_lc_hc_f\theta^{2l}}{(\theta^l-1)^3} \sum_{s=0}^{2^n-5} s\theta^{(s-1)(k+l)}\theta^{l+k} +$$

$$+ \sum_{\substack{l\neq 2^n-1\\ f,h=2^n-1}} \frac{c_kc_lc_hc_f\theta^l}{(\theta^l-1)^3} \sum_{s=0}^{2^n-5}\theta^{sk}\theta^{-l} = \sum_{\substack{l,k+l\neq 2^n-1\\ f,h=2^n-1}} \frac{c_kc_lc_hc_f\theta^{3l}}{(\theta^l-1)^3}\,\frac{1-\theta^{3(k+l)}}{\theta^{3(k+l)}(\theta^{k+l}-1)^2} +$$

$$+ \sum_{\substack{l,k+l\neq 2^n-1\\ f,h=2^n-1}} \frac{c_kc_lc_hc_f\theta^{3l}\theta^k}{(\theta^l-1)^3}\,\frac{1-\theta^{3(k+l)}}{\theta^{3(k+l)}(\theta^{k+l}-1)^2} + \sum_{\substack{l,k\neq 2^n-1\\ f,h=2^n-1}} \frac{c_kc_lc_hc_f}{(\theta^l-1)^3}\,\frac{1-\theta^{3k}}{\theta^{3k}(\theta^k-1)}.$$

Вычислим $D_{2.2}$:

$$D_{2.2} = \sum_{\substack{l\neq 2^n-1\\ f,h=2^n-1}} \frac{c_kc_lc_hc_f\theta^l}{\theta^l-1} \sum_{s=0}^{2^n-5}\theta^{s(l+k)}\sum_{p=s+2}^{2^n-3} p = \sum_{\substack{l\neq 2^n-1\\ f,h=2^n-1}} \frac{c_kc_lc_hc_f\theta^l}{\theta^l-1} \sum_{p=2}^{2^n-3} p\sum_{s=0}^{p-2}\theta^{s(l+k)} =$$

$$= \sum_{\substack{l,l+k\neq 2^n-1\\ f,h=2^n-1}} \frac{c_kc_lc_hc_f\theta^l}{\theta^l-1} \sum_{p=2}^{2^n-3} p\frac{\theta^{(l+k)(p-1)}-1}{\theta^{l+k}-1} + \sum_{\substack{l\neq 2^n-1\\ f,h,l+k=2^n-1}} \frac{c_kc_lc_hc_f\theta^l}{\theta^l-1} \sum_{p=2}^{2^n-3} \underbrace{p(p-1)}_{=0} =$$

$$= \sum_{\substack{l,l+k\neq 2^n-1\\ f,h=2^n-1}} \frac{c_kc_lc_hc_f\theta^l}{(\theta^l-1)(\theta^{l+k}-1)} \sum_{p=2}^{2^n-3} p\theta^{(p-1)(l+k)} = \sum_{\substack{l,l+k\neq 2^n-1\\ f,h=2^n-1}} \frac{c_kc_lc_hc_f\theta^l}{(\theta^l-1)(\theta^{l+k}-1)}\left(\sum_{p=2}^{2^n-3} x^p\right)'_{x=\theta^{l+k}} =$$

$$= \sum_{\substack{l,l+k\neq 2^n-1\\ f,h=2^n-1}} \frac{c_kc_lc_hc_f\theta^l}{(\theta^l-1)(\theta^{l+k}-1)}\,\frac{1-\theta^{3(l+k)}}{\theta^{l+k}(\theta^{l+k}-1)^2}.$$

Осталось вычислить $D_{2.3}$:

$$D_{2.3} = \sum_{f,h,l=2^n-1} c_kc_lc_hc_f \sum_{s=1}^{2^n-5} s\theta^{sk}\sum_{p=s+2}^{2^n-3} p = \sum_{f,h,l=2^n-1} c_kc_lc_hc_f\theta^k \sum_{p=3}^{2^n-3} p\sum_{s=1}^{p-2} s\theta^{(s-1)k} =$$

$$= \sum_{\substack{f,h,l=2^n-1\\ k\neq 2^n-1}} c_k c_l c_h c_f \theta^k \sum_{p=3}^{2^n-3} p \left(\sum_{s=1}^{p-2} x^s\right)'_{x=\theta^k} + \sum_{f,h,l,k=2^n-1} c_k c_l c_h c_f \theta^k \underbrace{\sum_{p=3}^{2^n-3} p \sum_{s=1}^{p-2} s}_{=1}.$$

Заметим, что $\left(\sum\limits_{s=1}^{p-2} x^s\right)'_{x=\theta^k} = \dfrac{px^{p-1}-(p-1)x^{p-2}-1}{(x-1)^2}$. Тогда

$$D_{2.3} = \sum_{\substack{f,h,l=2^n-1\\ k\neq 2^n-1}} c_k c_l c_h c_f \theta^k \sum_{p=3}^{2^n-3} p\frac{p\theta^{k(p-1)}-(p-1)\theta^{k(p-2)}-1}{(\theta^k-1)^2} + (c_{2^n-1})^4 =$$

$$= \sum_{\substack{f,h,l=2^n-1\\ k\neq 2^n-1}} \frac{c_k c_l c_h c_f \theta^k}{(\theta^k-1)^2} \sum_{p=3}^{2^n-3} p^2\theta^{k(p-1)} + (c_{2^n-1})^4 = \sum_{\substack{f,h,l=2^n-1\\ k\neq 2^n-1}} \frac{c_k c_l c_h c_f \theta^k}{(\theta^k-1)^2} \left(\sum_{p=3}^{2^n-3} x^p\right)'_{x=\theta^k} + (c_{2^n-1})^4 =$$

$$= \sum_{\substack{f,h,l=2^n-1\\ k\neq 2^n-1}} \frac{c_k c_l c_h c_f \theta^k}{(\theta^k-1)^2} \frac{1-\theta^{3k}}{\theta^k(\theta^k-1)^2} + (c_{2^n-1})^4 = \sum_{\substack{f,h,l=2^n-1\\ k\neq 2^n-1}} \frac{c_k c_l c_h c_f}{(\theta^k-1)^4}(1-\theta^{3k}) + (c_{2^n-1})^4.$$

В итоге получаем

$$D = \sum_{\substack{h,l+h,k\neq 2^n-1\\ f=2^n-1}} \frac{c_k c_l c_h c_f (1-\theta^{3k})}{(\theta^h-1)^2(\theta^{l+h}-1)^2(\theta^k-1)\theta^{2l}\theta^{3k}} + \sum_{\substack{h,l+h,l+h+k\neq 2^n-1\\ f=2^n-1}} \frac{c_k c_l c_h c_f \theta^{2h}\theta^k(1-\theta^{3(l+h+k)})}{(\theta^h-1)^2(\theta^{l+h}-1)^2(\theta^{l+h+k}-1)^2\theta^{3k}} +$$

$$+ \sum_{\substack{h,l+h,l+h+k\neq 2^n-1\\ f=2^n-1}} \frac{c_k c_l c_h c_f (1-\theta^{3(l+h+k)})}{(\theta^h-1)^2(\theta^{l+h}-1)^2(\theta^{l+h+k}-1)^2\theta^{2l}\theta^{3k}} + \sum_{\substack{h,k\neq 2^n-1\\ f,l+h=2^n-1}} \frac{c_k c_l c_h c_f \theta^{2h}(1-\theta^{3k})}{(\theta^h-1)^2(\theta^k-1)^3\theta^{2k}} +$$

$$+ \sum_{\substack{h,h+l,h+l+k\neq 2^n-1\\ f=2^n-1}} \frac{c_k c_l c_h c_f \theta^{2l}}{(\theta^h-1)^2(\theta^{h+l}-1)^2} \frac{1-\theta^{3(l+h+k)}}{\theta^{3(l+k)}(\theta^{l+h+k}-1)^2} +$$

$$+ \sum_{\substack{h,h+l,h+l+k\neq 2^n-1\\ f=2^n-1}} \frac{c_k c_l c_h c_f \theta^{l}}{(\theta^h-1)^2(\theta^{h+l}-1)^2} \frac{1-\theta^{3(l+h+k)}}{\theta^{2(l+k)}(\theta^{l+h+k}-1)^2} +$$

$$+ \sum_{\substack{h,h+l,k\neq 2^n-1\\ f=2^n-1}} \frac{c_k c_l c_h c_f (1-\theta^{3k})}{(\theta^h-1)^2(\theta^{h+l}-1)^2(\theta^k-1)\theta^l\theta^{3k}} + \sum_{\substack{h,k\neq 2^n-1\\ f,h+l=2^n-1}} \frac{c_k c_l c_h c_f \theta^h(1-\theta^{3k})}{(\theta^h-1)^2(\theta^k-1)^3\theta^k} +$$

$$+ \sum_{\substack{k,h,l\neq 2^n-1\\ f=2^n-1}} \frac{c_k c_l c_h c_f}{(\theta^h-1)^2(\theta^l-1)\theta^{2l}} \frac{1-\theta^{3k}}{(\theta^k-1)\theta^{3k}} + \sum_{\substack{h,l,l+k\neq 2^n-1\\ f=2^n-1}} \frac{c_k c_l c_h c_f \theta^l}{(\theta^h-1)^2(\theta^l-1)} \frac{1-\theta^{3(l+k)}}{(\theta^{l+k}-1)\theta^{3(l+k)}} +$$

$$+ \sum_{\substack{h,k\neq 2^n-1\\ f,l=2^n-1}} \frac{c_k c_l c_h c_f \theta^k}{(\theta^h-1)^2} \frac{1-\theta^{3k}}{(\theta^k-1)^2\theta^{3k}} + \sum_{\substack{l,k+l\neq 2^n-1\\ f,h=2^n-1}} \frac{c_k c_l c_h c_f}{(\theta^l-1)^3} \frac{1-\theta^{3(k+l)}}{\theta^{3k}(\theta^{k+l}-1)^2} +$$

$$+ \sum_{\substack{l,k+l\neq 2^n-1\\ f,h=2^n-1}} \frac{c_k c_l c_h c_f \theta^k}{(\theta^l-1)^3} \frac{1-\theta^{3(k+l)}}{\theta^{3k}(\theta^{k+l}-1)^2} + \sum_{\substack{l,k\neq 2^n-1\\ f,h=2^n-1}} \frac{c_k c_l c_h c_f}{(\theta^l-1)^3} \frac{1-\theta^{3k}}{\theta^{3k}(\theta^k-1)} +$$

$$+ \sum_{\substack{l,l+k\neq 2^n-1\\ f,h=2^n-1}} \frac{c_k c_l c_h c_f}{(\theta^l-1)(\theta^{l+k}-1)} \frac{1-\theta^{3(l+k)}}{\theta^k(\theta^{l+k}-1)^2} + \sum_{\substack{f,h,l=2^n-1\\ k\neq 2^n-1}} \frac{c_k c_l c_h c_f}{(\theta^k-1)^4}(1-\theta^{3k}) + (c_{2^n-1})^4.$$

Выражение $A+B+D$ даёт требуемый результат. ■