Math-Net.Ru

Общероссийский математический портал

С. С. Марченков, Равномерное id -разложение функций
многозначной логики над однородными функциями, *Дис-
крет. матем.*, 2010, том 22, выпуск 4, 55–63

DOI: <https://doi.org/10.4213/dm1119>

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

Параметры загрузки:

IP: 54.198.64.247

26 апреля 2023 г., 16:35:28

Равномерное *id*-разложение функций многозначной логики над однородными функциями

© 2010 г. С. С. Марченков

Рассматривается равномерное *id*-разложение класса P_k функций k -значной логики над классом H_k^* структурных однородных функций и классом D_k однородных функций, порождаемым дуальным дискриминатором d . Находятся степени равномерного *id*-разложения класса P_k над классами H_k^* и D_k . Указываются способы построения однородных функций, над которыми осуществляется равномерное *id*-разложение класса P_k .

Работа выполнена при поддержке Российского фонда фундаментальных исследований, проекты 09–01–00701 и 10–01–00768.

В теории функций многозначной логики важное место занимают разнообразные разложения (представления) функций. Они используются в доказательствах полноты конечных систем функций в различных замкнутых классах, при оценке сложности реализации функций формулами и схемами в полных и неполных базисах, в вопросах построения надежных схем из ненадежных элементов и в других направлениях исследований функций многозначной логики.

Один из распространенных типов разложения основан на идее восстановления разлагаемой функции по ее подфункциям, полученным всевозможными отождествлениями двух переменных. Некоторый вариант такого разложения был формализован в работе [2] в виде равномерного *id*-разложения. Дальнейшие исследования равномерного *id*-разложения проводились в работах [3, 4], где в основном рассматривались вопросы равномерного *id*-разложения одних замкнутых классов над другими.

В данной статье мы хотим рассмотреть равномерное *id*-разложение класса P_k функций k -значной логики над сравнительно небольшими замкнутыми классами: классом H_k^* структурных однородных функций и классом D_k однородных функций, который порождается дуальным дискриминатором d . Основанием для выбора классов H_k^* и D_k служит то, что эти классы представляют собой прямые обобщения важных в теории булевых функций классов S_{01} самодвойственных функций, сохраняющих 0, и SM самодвойственных монотонных функций [5, 7]. Кроме того, класс D_k весьма мал — он является атомом в решетке клонов из P_k [1]. Принципиальная возможность равномерного *id*-разложения класса P_k над классами H_k^* и D_k установлена в [4] (для классов S_{01} и SM — в работе [2]). Однако точное значение степеней равномерного *id*-разложения класса P_k над классами H_k^* и D_k устанавливается только с помощью доказываемых ниже теорем 1 и 2. Помимо этого, после теорем 1 и 2 указаны способы построения соответствующих однородных функций, над которыми можно осуществить равномерное *id*-разложение класса P_k .

Приведем необходимые определения. Пусть $k \geq 2$, $E_k = \{0, 1, \dots, k-1\}$, P_k — множество всех функций на E_k (множество функций k -значной логики). Для любой функции $f(x_1, x_2, \dots, x_n)$, $n \geq 2$, и любых неравных i, j , $1 \leq i, j \leq n$, через f_j^i обозначим функцию $f(x_1, \dots, x_{j-1}, x_i, x_{j+1}, \dots, x_n)$, получаемую из функции f подстановкой переменной x_i вместо переменной x_j . Пусть $2 \leq m \leq n$. Будем говорить, что функция $f(x_1, x_2, \dots, x_n)$ из P_k *id-разложима* над функцией

$$g(y_2^1, y_3^1, \dots, y_m^1, y_1^2, y_3^2, \dots, y_m^2, \dots, y_1^m, y_2^m, \dots, y_{m-1}^m) \quad (1)$$

по (первым) m переменным, если выполняется тождество

$$f(x_1, x_2, \dots, x_n) = g(f_2^1, \dots, f_m^1, \dots, f_1^m, \dots, f_{m-1}^m). \quad (2)$$

Пусть R — класс функций из P_k . Говорим, что класс R равномерно *id-разложим* над функцией (1), если для любого $n \geq m$ и любой функции f из R от n переменных имеет место разложение (2). Если для некоторой функции g от $m(m-1)$ переменных класс R является равномерно *id-разложимым* над функцией g , то говорим также, что класс R допускает равномерное *id-разложение* по m переменным или, короче, что класс R равномерно *m-разложим*. В случае, когда функция g принадлежит некоторому классу Q , используем термины класс R равномерно *id-разложим* по m переменным над классом Q или класс R равномерно *m-разложим* над классом Q .

Пусть класс R равномерно *id-разложим* над классом Q . Степенью равномерного *id-разложения* класса R над классом Q , обозначаемой $\deg(R/Q)$, называется такое наименьшее число m , что класс R равномерно *m-разложим* над классом Q . Если $Q = P_k$, то говорим о степени равномерного *id-разложения* класса R и применяем обозначение $\deg(R)$.

Пусть E — непустое подмножество множества E_k . Говорят, что функция f сохраняет множество E , если для любых элементов $e_1, \dots, e_n$ из E имеет место включение $f(e_1, \dots, e_n) \in E$.

Пусть π — перестановка на множестве E_k и $f \in P_k$. Говорят, что функция f самодвойственна относительно перестановки π , если выполняется тождество

$$f(\pi(x_1), \dots, \pi(x_n)) = \pi(f(x_1, \dots, x_n)).$$

Функция f называется однородной [8], если она самодвойственна относительно любых перестановок на E_k . Множество всех однородных функций из P_k обозначим через H_k , а через H_k^* обозначим множество всех функций из H_k , сохраняющих множество E_{k-1} (множество структурных однородных функций). Отметим [1, 8], что каждая функция из класса H_k^* сохраняет любое непустое подмножество множества E_k . Кроме того, класс H_2 совпадает с классом S самодвойственных булевых функций, а класс H_2^* совпадает с классом S_{01} самодвойственных булевых функций, сохраняющих 0 (а также 1).

Пусть $\tilde{a} = (a_1, \dots, a_n)$ — набор из E_k^n . Обозначим через $\ker(\tilde{a})$ эквивалентность на множестве $\{1, 2, \dots, n\}$, которая определяется соотношением

$$(i, j) \in \ker(\tilde{a}) \iff (a_i = a_j).$$

Назовем наборы $\tilde{a}$ и $\tilde{b} = (b_1, \dots, b_n)$ однотипными, если $\ker(\tilde{a}) = \ker(\tilde{b})$. Известно [1], что если $f \in H_k^*$ и значение $f(\tilde{a})$ совпадает со значением a_i , то для любого набора $\tilde{b}$, однотипного с набором $\tilde{a}$, значение $f(\tilde{b})$ совпадает со значением b_i .

Теорема 1. Пусть $k \geq 2$ и класс P_k допускает равномерное *id-разложение* по m переменным. Тогда класс P_k равномерно *m-разложим* над классом H_k^* .

Доказательство. Предположим, что класс P_k равномерно id -разложим над функцией (1) по m переменным. Вследствие леммы 1 из [3] справедливо неравенство $m \geq 2k$. Возьмем произвольную функцию $f(x_1, \dots, x_m)$ из P_k и произвольный набор $\tilde{a} = (a_1, \dots, a_m)$ из E_k^m . По выбору функции g ее значением на наборе

$$(f_2^1(\tilde{a}), \dots, f_m^1(\tilde{a}), \dots, f_1^m(\tilde{a}), \dots, f_{m-1}^m(\tilde{a})) \quad (3)$$

будет $f(\tilde{a})$. В силу неравенства $m \geq 2k$ и в соответствии с определением функций $f_2^1, \dots, f_{m-1}^m$ значение $f(\tilde{a})$ входит в набор (3).

Рассмотрим далее произвольную перестановку π на множестве E_k . Проведенные выше рассуждения будут справедливы и для функции $\pi(f)$. Поэтому, в частности, значением функции g на наборе

$$((\pi(f))_2^1(\tilde{a}), \dots, (\pi(f))_m^1(\tilde{a}), \dots, (\pi(f))_1^m(\tilde{a}), \dots, (\pi(f))_{m-1}^m(\tilde{a})) \quad (4)$$

будет $\pi(f(\tilde{a}))$. Однако набор (4), как легко видеть, совпадает с набором

$$(\pi(f_2^1(\tilde{a})), \dots, \pi(f_m^1(\tilde{a})), \dots, \pi(f_1^m(\tilde{a})), \dots, \pi(f_{m-1}^m(\tilde{a}))). \quad (5)$$

Таким образом, перестановка π переводит набор (3) в набор (5) и, кроме того, значение $f(\tilde{a})$ функции g на наборе (3) преобразуется в значение $\pi(f(\tilde{a}))$ функции g на наборе (5). Поскольку π — произвольная перестановка на E_k , отсюда следует, что на всех наборах из $E_k^{m(m-1)}$, однотипных с набором (3), значение функции g определяется ее значением на одном из наборов (3). Более точно, если значение функции g на наборе (3) равно i -й компоненте этого набора, то на всяком наборе $\tilde{b}$ из $E_k^{m(m-1)}$, однотипном с набором (3), значение $g(\tilde{b})$ также совпадает с i -й компонентой набора $\tilde{b}$. Это позволяет определить в классе H_k^* искомую функцию g' от $m(m-1)$ переменных. Именно, если $\tilde{b} \in E_k^{m(m-1)}$ и для некоторого набора $\tilde{a}$ из E_k^m и некоторой функции $f(x_1, \dots, x_m)$ из P_k набор $\tilde{b}$ совпадает с набором (3), то полагаем $g'(\tilde{b}) = f(\tilde{a})$. В противном случае значение $g'(\tilde{b})$ полагаем равным, например, первой компоненте набора $\tilde{b}$. Легко видеть, что эти условия обеспечивают вхождение функции g' в класс H_k^* . Теорема доказана.

Следствие 1. Для любого $k \geq 2$ имеет место равенство

$$\deg(P_k/H_k^*) = 2k.$$

Доказательство. Достаточно воспользоваться теоремой 3 из [3], согласно которой $\deg(P_k) = 2k$.

Отметим, что равенство $\deg(P_2/S_{01}) = 4$ доказано в [2] (см. леммы 3 и 9, где класс S_{01} имеет обозначение D_1).

Для любых неравных a, b из E_k обозначим через P_k^{ab} множество всех функций из P_k , которые принимают лишь значения a, b .

Следствие 2. Для любого $k \geq 2$ и любых неравных a, b из E_k имеет место равенство

$$\deg(P_k^{ab}/H_k^*) = 2k.$$

Доказательство. Для доказательства достаточно воспользоваться теоремами 2 и 3 из [3], из которых вытекает соотношение $\deg(P_k^{ab}) = 2k$.

Пусть класс P_k равномерно id -разложим над функцией (1) из класса H_k^* . Тогда над этой функцией g равномерно id -разложим и класс P_k^{01} . При этом из всей функции g используется только ее часть g^{01} — ограничение функции g на множество E_2 . Ввиду включения $g \in H_k^*$ функция g^{01} является самодвойственной булевой функцией, сохраняющей 0, то есть принадлежит классу S_{01} . Таким образом, равномерное id -разложение класса P_k^{01} можно рассматривать над классом S_{01} , а в силу следствия 2 справедливо равенство $\deg(P_k^{01}/S_{01}) = 2k$.

Мы бы хотели при равномерном id -разложении всего класса P_k использовать вместо класса H_k^* более простой класс S_{01} . Это можно сделать, например, следующим образом.

Пусть g — функция от $2k(2k-1)$ переменных из класса S_{01} , над которой равномерно id -разложим класс P_k^{01} . Пусть далее $n \geq 2k$ и $f(x_1, \dots, x_n)$ — функция из P_k . Для любого i , $1 \leq i \leq [\log_2 k]$, обозначим через $h_i(x)$ функцию из P_k , которая для любого $x \in E_k$ выдает i -й двоичный разряд числа x . Понятно, что по значениям функций $h_1(f), \dots, h_l(f)$ на наборе $(x_1, \dots, x_n)$ (здесь $l = [\log_2 k]$) значение $f(x_1, \dots, x_n)$ восстанавливается однозначно. Следовательно, id -разложение функции f над функцией g можно получить в виде

$$f(x_1, \dots, x_n) = e(g((h_1(f))_2^1, \dots, (h_1(f))_{2k}^1, \dots, (h_1(f))_1^{2k}, \dots, (h_1(f))_{2k-1}^{2k}), \\ \dots, g((h_l(f))_2^1, \dots, (h_l(f))_{2k}^1, \dots, (h_l(f))_1^{2k}, \dots, (h_l(f))_{2k-1}^{2k})),$$

где

$$e(z_1, \dots, z_l) = z_1 + 2z_2 + \dots + 2^{l-1}z_l.$$

Однако следует заметить, что для получения данного id -разложения над функцией g необходимо предварительно образовать все функции $h_1(f), \dots, h_l(f)$.

Теорема 1 не дает способа построения в классе H_k^* функции g от $2k(2k-1)$ переменных, над которой равномерно id -разложим класс P_k . Вместе с тем довольно близкая функция определена в работе [3] (функция h после доказательства теоремы 3). Мы воспроизведем основную часть определения этой функции, заменив в нем пункт об остальных случаях, который фактически не работает при id -разложении функций из класса P_k .

Итак, определим искомую функцию $g(y_2^1, y_3^1, \dots, y_{2k}^1, y_2^{2k}, y_3^{2k}, \dots, y_{2k-1}^{2k})$ из класса H_k^* . При этом будем опираться на то (см. [1, 8]), что при задании функций из класса H_k^* можно пользоваться отношением равенства/неравенства между значениями переменных, а значения определяемой функции в каждом конкретном случае должны совпадать со значениями одной из переменных.

Пусть $(K_1, \dots, K_l)$ — разбиение множества $\{1, 2, \dots, 2k\}$ на непустые попарно непересекающиеся подмножества, i, j — элементы множества $\{1, 2, \dots, 2k\}$. Будем говорить, что элементы i, j эквивалентны относительно разбиения $(K_1, \dots, K_l)$, если они принадлежат одному и тому же множеству разбиения $(K_1, \dots, K_l)$.

Пусть $\tilde{a} = (a_2^1, a_3^1, \dots, a_{2k-1}^{2k})$ — произвольный набор из множества $E_k^{2k(2k-1)}$. Для определения значения $g(\tilde{a})$ разыскиваем такое разбиение $(K_1, \dots, K_l)$, $2 \leq l \leq k$, множества $\{1, 2, \dots, 2k\}$ на непустые попарно непересекающиеся подмножества, что выполняется следующее условие: для любых пар (i, j) , (s, t) неравных элементов, эквивалентных относительно разбиения $(K_1, \dots, K_l)$, и любого $v \in \{1, 2, \dots, 2k\}$, $v \notin \{i, j\}$, справедливы равенства

$$a_j^i = a_t^s, \quad a_v^i = a_v^j.$$

Если такое разбиение $(K_1, \dots, K_l)$ существует, то полагаем $g(\tilde{a})$ равным значению a_j^i для какой-либо пары элементов (i, j) , эквивалентных относительно разбиения $(K_1, \dots, K_l)$. В противном случае полагаем $g(\tilde{a}) = a_2^1$.

Отметим, что разыскиваемое разбиение $(K_1, \dots, K_l)$ может быть не единственным. Для определенности можно выбрать, например, наименьшее из таких разбиений (при каком-либо упорядочении всех разбиений, когда сначала рассматриваются разбиения с наибольшим возможным l , равным k , и так далее). Корректность такого задания функции g следует из результатов работы [3].

В качестве примера рассмотрим построение функции $g(y_2^1, \dots, y_6^1, \dots, y_1^6, \dots, y_5^6)$ от 30 переменных для случая $k = 3$. Определение функции g состоит из четырех блоков. Первые три блока отвечают разбиениям множества $\{1, 2, 3, 4, 5, 6\}$ на три непустых подмножества с распределениями числа элементов в подмножествах соответственно $(4, 1, 1)$, $(3, 2, 1)$, $(2, 2, 2)$. Разбиения множества $\{1, 2, 3, 4, 5, 6\}$ на два непустых подмножества при определении функции g можно не использовать. Четвертый блок заключает в себе все остальные случаи.

Из 15 разбиений типа $(4, 1, 1)$ рассмотрим только разбиение $(\{1, 2, 3, 4\}, \{5\}, \{6\})$. Для него соответствующий пункт определения функции g выглядит так: если

$$y_2^1 = y_3^1 = y_4^1 = y_1^2 = y_3^2 = y_4^2 = y_1^3 = y_2^3 = y_4^3 = y_1^4 = y_2^4 = y_3^4, \\ y_5^1 = y_5^2 = y_5^3 = y_5^4, \quad y_6^1 = y_6^2 = y_6^3 = y_6^4,$$

то $g(y_2^1, \dots, y_6^1, \dots, y_1^6, \dots, y_5^6) = y_2^1$; в качестве значения функции g здесь можно выбрать также любую переменную y_j^i , где $i, j \in \{1, 2, 3, 4\}$ и $i \neq j$.

Из 60 разбиений типа $(3, 2, 1)$ рассмотрим разбиение $(\{1, 2, 3\}, \{4, 5\}, \{6\})$. Соответствующая часть определения функции g для него будет такой: если

$$y_2^1 = y_3^1 = y_1^2 = y_3^2 = y_1^3 = y_2^3 = y_5^4 = y_5^5, \quad y_4^1 = y_4^2 = y_4^3, \quad y_5^1 = y_5^2 = y_5^3, \\ y_6^1 = y_6^2 = y_6^3, \quad y_1^4 = y_1^5, \quad y_2^4 = y_2^5, \quad y_3^4 = y_3^5, \quad y_4^4 = y_4^5,$$

то $g(y_2^1, \dots, y_6^1, \dots, y_1^6, \dots, y_5^6) = y_2^1$; в качестве значения функции g можно выбрать любую переменную y_j^i , где $\{i, j\} \subset \{1, 2, 3\}$ и $i \neq j$ или $\{i, j\} = \{4, 5\}$.

Из 90 разбиений типа $(2, 2, 2)$ рассмотрим разбиение $(\{1, 2\}, \{3, 4\}, \{5, 6\})$. Для него, если

$$y_2^1 = y_1^2 = y_4^3 = y_3^4 = y_6^5 = y_5^6, \quad y_3^1 = y_3^2, \quad y_4^1 = y_4^2, \quad y_5^1 = y_5^2, \\ y_6^1 = y_6^2, \quad y_1^3 = y_1^4, \quad y_2^3 = y_2^4, \quad y_3^5 = y_3^6, \quad y_4^5 = y_4^6, \\ y_5^5 = y_5^6, \quad y_6^5 = y_6^6,$$

то $g(y_2^1, \dots, y_6^1, \dots, y_1^6, \dots, y_5^6) = y_2^1$, но можно также взять любую из переменных $y_1^2, y_3^4, y_5^6, y_6^5$.

Во всех остальных случаях полагаем, например,

$$g(y_2^1, \dots, y_6^1, \dots, y_1^6, \dots, y_5^6) = y_2^1.$$

Покажем корректность определения функции g . Пусть выполняются два пункта определения функции g , например, второй и третий пункты. И пусть соответствующие разбиения множества $\{1, 2, 3, 4, 5, 6\}$ суть (X_1, X_2, X_3) и (Y_1, Y_2, Y_3) , где

$$|X_1| = 3, \quad |X_2| = 2, \quad |X_3| = 1, \quad |Y_1| = |Y_2| = |Y_3| = 2.$$

Тогда либо одно из множеств Y_1, Y_2, Y_3 целиком входит в одно из множеств X_1, X_2 , либо каждое из множеств Y_1, Y_2, Y_3 пересекается с каждым из множеств X_1, X_2, X_3 не более

чем по одному элементу. Если, например, в первом случае $Y_1 = \{i, j\}$ целиком входит в одно из множеств X_1 или X_2 , то согласно второму и третьему пунктам определения функции g значения функции g будет совпадать со значениями переменной y_j^i .

Во втором случае пусть, например,

$$X_1 \cap Y_1 = \{i\}, \quad X_1 \cap Y_2 = \{j\}, \quad X_2 \cap Y_1 = \{l\}, \quad X_2 \cap Y_2 = \{m\}.$$

Из того, что $Y_1 = \{i, l\}$, следует, что $y_j^i = y_j^l$, а из $Y_2 = \{j, m\}$ следует, что $y_j^l = y_j^m$. Поэтому $y_j^i = y_j^m$. Однако y_j^i есть значение функции g согласно пункту 2 определения, а y_j^m — ее значение согласно пункту 3 определения. Таким образом, оба значения оказываются равными.

Рассмотрим еще один случай разбиений (X_1, X_2, X_3) , (Y_1, Y_2, Y_3) , когда

$$|X_1| = |X_2| = |X_3| = |Y_1| = |Y_2| = |Y_3| = 2.$$

Если одно из множеств X_1, X_2, X_3 совпадает с одним из множеств Y_1, Y_2, Y_3 , то рассуждаем так же, как и выше. Предположим далее, что каждое из множеств X_1, X_2, X_3 пересекается с каждым из множеств Y_1, Y_2, Y_3 не более чем по одному элементу. Пусть, например,

$$\begin{aligned} X_1 &= \{i, j\}, & X_2 &= \{l, m\}, & X_3 &= \{n, p\}, \\ Y_1 &= \{j, l\}, & Y_2 &= \{m, n\}, & Y_3 &= \{i, p\}. \end{aligned}$$

Рассматривая множества X_1, Y_1, X_2, Y_2 , приходим к цепочке равенств

$$y_p^i = y_p^j, \quad y_p^j = y_p^l, \quad y_p^l = y_p^m, \quad y_p^m = y_p^n,$$

откуда следует, что $y_p^i = y_p^n$. Однако y_p^i есть значение функции g согласно разбиению (Y_1, Y_2, Y_3) , а y_p^n — согласно разбиению (X_1, X_2, X_3) . Таким образом, оба значения вновь оказываются равными.

Наконец, включение $g \in H_3^*$ следует из того, что значения функции g определяются с помощью отношения равенства/неравенства между переменными, а в каждом отдельном случае соответствующие значения функции g совпадают со значениями некоторой из ее переменных.

При любом $k \geq 2$ рассмотрим в классе P_k дуальный дискриминатор $d(x, y, z)$, который определяется следующими соотношениями:

$$d(x, y, z) = \begin{cases} x, & \text{если } x = y, \\ z & \text{в противном случае.} \end{cases}$$

Дискриминатор d представляет собой однородную функцию из H_k^* , которая порождает (относительно операции суперпозиции) замкнутый класс, обозначаемый далее через D_k . Класс D_k является атомом в решетке клонов из P_k [1]. Отметим еще, что ограничение функции $d(x, y, z)$ на множество E_2 (а также сама функция $d(x, y, z)$ при $k = 2$) является медианой — самодвойственной монотонной функцией $xy \vee xz \vee yz$.

Теорема 2. При любом $k \geq 2$ справедливо равенство

$$\deg(P_k/D_k) = k^2 + 1.$$

Доказательство. Дискриминатор d является мажоритарной функцией от трех переменных, то есть удовлетворяет тождествам

$$d(x, x, y) = d(x, y, x) = d(y, x, x) = x.$$

Поэтому на основании теоремы 1 из [4] получаем, что

$$\deg(P_k/D_k) \leq k^2 + 1.$$

Далее мы установим, что $\deg(P_k/D_k) > k^2$. На самом деле будет показано, что даже

$$\deg(P_k^{01}/D_k) > k^2.$$

Предположим, что для некоторой функции $g(y_2^1, \dots, y_{k^2}^1, y_1^2, \dots, y_{k^2}^2, \dots, y_1^{k^2}, \dots, y_{k^2-1}^{k^2})$ из класса P_k , зависящей от $k^2(k^2-1)$ переменных, класс P_k^{01} равномерно id -разложим над функцией g . Иными словами, пусть для любого $n \geq k^2$ и любой функции $f(x_1, \dots, x_n)$ из P_k^{01} имеет место тождество

$$f(x_1, \dots, x_n) = g(f_2^1, \dots, f_{k^2}^1, f_1^2, f_3^2, \dots, f_{k^2}^2, \dots, f_1^{k^2}, \dots, f_{k^2-1}^{k^2}). \quad (6)$$

Поскольку функция f и все функции f_j^i принимают лишь значения 0, 1, функцию g можно считать булевой функцией. Предположим еще, что функция g монотонна, и выведем отсюда некоторые ограничения на строение функции g .

Пусть $(X_1, \dots, X_k)$ — какое-либо разбиение множества $\{1, 2, \dots, k^2\}$ на попарно непересекающиеся подмножества, содержащие каждое по k элементов. Рассмотрим такую функцию $f \in P_k^{01}$ от k^2 переменных, которая принимает значение 1 только на одном наборе $\tilde{a} = (a_1, \dots, a_{k^2})$, где $a_j = i - 1$ при $j \in X_i$. Пусть $y_{j_1}^{i_1} \dots y_{j_s}^{i_s}$ — конъюнкция из сокращенной дизъюнктивной нормальной формы (ДНФ) [6, 7] функции g , для которой

$$f_{j_1}^{i_1}(\tilde{a}) \dots f_{j_s}^{i_s}(\tilde{a}) = 1.$$

Из определения функции f следует, что при любом t , $1 \leq t \leq s$, числа i_t, j_t эквивалентны относительно разбиения $(X_1, \dots, X_k)$.

Рассмотрим теперь булево отрицание функции f функцию $\bar{f}$. Чтобы для функции $\bar{f}$ выполнялось тождество (6), каждая конъюнкция из сокращенной ДНФ функции g должна содержать хотя бы одну переменную вида $y_{j_t}^{i_t}$, где числа i_t, j_t эквивалентны относительно разбиения $(X_1, \dots, X_k)$. Однако, как мы установили, в сокращенную ДНФ функции g входит конъюнкция K , которая отвечает такому разбиению $(X'_1, \dots, X'_k)$ множества $\{1, 2, \dots, k^2\}$, в котором каждое множество X'_l пересекается с каждым множеством X_m ровно по одному элементу. Понятно, что данная конъюнкция K не содержит ни одной переменной вида $y_{j_t}^{i_t}$, где числа i_t, j_t эквивалентны относительно разбиения $(X_1, \dots, X_k)$.

Итак, при сделанных выше предположениях функция g не может быть монотонной. Этот факт символически можно было бы записать в виде $\deg(P_k^{01}/M) > k^2$, где через M обозначен класс монотонных булевых функций.

Вернемся к функции d и классу D_k . Предположим, что класс P_k^{01} равномерно id -разложим над классом D_k по k^2 переменным. Поскольку ограничение функции d на множество E_2 есть монотонная булева функция медиана, вместо соответствующей функции g от $k^2(k^2-1)$ переменных, принадлежащей классу D_k , можно рассматривать ее ограничение на множество E_2 , которое представляет собой монотонную булеву функцию. Однако, как установлено выше, подобная монотонная булева функция от $k^2(k^2-1)$ переменных участвовать в равномерном id -разложении класса P_k^{01} не может. Теорема доказана.

Отметим, что равенство

$$\deg(P_2/D_2) = 5$$

установлено в работе [2].

Как уже говорилось, при равномерном id -разложении класса P_k^{01} над функцией g последнюю можно считать булевой функцией. Ограничение функции d на множество E_2 есть медиана (которая является базисом по суперпозиции в классе самодвойственных монотонных функций [5, 7]), поэтому, в частности, при равномерном id -разложении класса P_k^{01} над классом D_k соответствующие функции g можно считать самодвойственными монотонными функциями. Доказательство теоремы 1 из [4] дает некоторый индуктивный способ получения функций g из функции d . Однако этот метод по существу является переборным (объем перебора порядка k^{k^2+1}) и потому вряд ли может быть применим на практике.

Пользуясь некоторыми идеями, высказанными в [2] для равномерного id -разложения класса P_2 над классами монотонных функций, мы хотим предложить другой, менее трудоемкий путь построения самодвойственных монотонных функций g . Мы продемонстрируем его для случая $k = 3$, ограничившись по понятным техническим причинам получением только монотонной функции g .

Итак, рассматриваем класс P_3^{01} . Согласно доказанной выше теореме 2

$$\deg(P_3^{01}/SM) = 3^2 + 1 = 10.$$

Построим монотонную функцию $g(y_2^1, \dots, y_{10}^9)$ от 45 переменных, над которой равномерно id -разложим класс P_3^{01} (из двух переменных y_j^i , y_i^j для функции g здесь достаточно взять одну переменную y_j^i , $i < j$). Функция g будет представлена в виде сокращенной ДНФ, каждая (монотонная) конъюнкция которой определяется разбиением (X_1, X_2, X_3) множества $\{1, 2, \dots, 10\}$ на непустые попарно непересекающиеся подмножества. Именно разбиению (X_1, X_2, X_3) указанного вида отвечает конъюнкция, которая состоит из всех переменных y_j^i , где $i < j$ и числа i, j эквивалентны относительно разбиения X_1, X_2, X_3 .

Разбиениям (X_1, X_2, X_3) с распределением числа элементов в множествах $(8, 1, 1)$ соответствуют 45 конъюнкций длины 28, разбиениям с распределением $(7, 2, 1)$ — 360 конъюнкций длины 22. Дальнейшие выкладки таковы: распределение $(6, 3, 1)$ — 840 конъюнкций длины 18; распределение $(6, 2, 2)$ — 1260 конъюнкций длины 17; распределение $(5, 4, 1)$ — 1260 конъюнкций длины 16; распределение $(5, 3, 2)$ — 2520 конъюнкций длины 14; распределение $(4, 4, 2)$ — 3150 конъюнкций длины 13; распределение $(4, 3, 3)$ — 4200 конъюнкций длины 12.

Таким образом, сокращенная ДНФ функции g состоит из 13635 конъюнкций указанного выше вида.

Покажем, что построенную функцию g можно использовать при равномерном id -разложении класса P_3^{01} . Возьмем в классе P_3^{01} произвольную функцию f , зависящую от 10 переменных. Пусть далее $\tilde{a}$ — произвольный набор из E_3^{10} . Рассмотрим сначала случай, когда в наборе $\tilde{a}$ присутствуют все три числа 0, 1, 2. Пусть (X_1, X_2, X_3) — разбиение множества $\{1, 2, \dots, 10\}$, отвечающее эквивалентности $\ker(\tilde{a})$, в котором $|X_1| \geq |X_2| \geq |X_3|$. Тогда в сокращенную ДНФ функции g входит конъюнкция K , построенная выше для данного разбиения (X_1, X_2, X_3) . Если $f(\tilde{a}) = 1$, то, очевидно, конъюнкция K обратится в 1, если каждую из ее переменных y_j^i заменить соответствующим значением $f_j^i(\tilde{a})$. Если же $f(\tilde{a}) = 0$, то следует заметить, что конъюнкция K имеет непустое пересечение с любой другой конъюнкцией из сокращенной ДНФ функции g . Это обеспечивает равенство

$$g(f_2^1(\tilde{a}), \dots, f_{10}^9(\tilde{a})) = 0.$$

Пусть теперь в наборе $\tilde{a}$ присутствуют только два числа из E_3 , и пусть в этом случае эквивалентности $\ker(\tilde{a})$ отвечает разбиение (X'_1, X'_2) множества $\{1, 2, \dots, 10\}$. Разделим какое-либо неоднородное множество из X'_1, X'_2 на два непустых непересекающихся подмножества и обозначим полученное разбиение множества $\{1, 2, \dots, 10\}$ через (X_1, X_2, X_3) . Особенностью этого разбиения является то, что для любой пары неравных чисел i, j , эквивалентных относительно разбиения (X_1, X_2, X_3) , значение $f_j^i(\tilde{a})$ совпадает со значением $f(\tilde{a})$. Дальнейшие рассуждения повторяют соответствующие рассуждения для случая трех чисел в наборе $\tilde{a}$.

Случай, когда набор $\tilde{a}$ состоит только из одного элемента, очевиден.

Искомую самодвойственную монотонную функцию можно получить из данной монотонной функции g добавлением к сокращенной ДНФ функции g некоторого (довольно большого) числа монотонных конъюнкций.

Список литературы

1. Марченков С. С., Однородные алгебры. *Проблемы кибернетики* (1982) **39**, 85–106.
2. Марченков С. С., О равномерном id -разложении булевых функций. *Дискретная математика* (1990) **2**, №3, 29–41.
3. Марченков С. С., О степени равномерного id -разложения замкнутых классов в P_k . *Дискретная математика* (1991) **3**, №4, 128–142.
4. Марченков С. С., Об id -разложениях класса P_k над предполными классами. *Дискретная математика* (1993) **5**, №2, 98–110.
5. Марченков С. С., *Замкнутые классы булевых функций*. Физматлит, Москва, 2000.
6. Яблонский С. В., *Введение в дискретную математику*. Наука, Москва, 1986.
7. Яблонский С. В., Гаврилов Г. П., Кудрявцев В. Б., *Функции алгебры логики и классы Поста*. Наука, Москва, 1966.
8. Marczewski E., Homogeneous operations and homogeneous algebras. *Fundam. Math.* (1964) **56**, 81–103.

Статья поступила 15.01.2010.