Math-Net.Ru

Общероссийский математический портал

С. Н. Селезнева, О сложности поляризованных полиномов функций многозначных логик, зависящих от одной переменной, *Дискрет. матем.*, 2004, том 16, выпуск 2, 117–120

DOI: <https://doi.org/10.4213/dm157>

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

Параметры загрузки:

IP: 54.89.56.158

26 апреля 2023 г., 10:27:38

О сложности поляризованных полиномов функций многозначных логик, зависящих от одной переменной

© 2004 г. С. Н. Селезнева

Рассматривается задание функций многозначных логик поляризованными полиномами. Поляризованным называется полином, в котором каждая переменная может быть поляризована смещением на определенную величину. Вводится функция Шеннона, характеризующая сложность задания функций многозначных логик поляризованными полиномами. Получена точная оценка функции Шеннона для функций, зависящих от одной переменной.

Работа выполнена при поддержке Российского фонда фундаментальных исследований, проект 00-01-00351.

В настоящей заметке рассматриваются полиномы, в которых каждая переменная может быть поляризована смещением на определенную величину. Такие полиномы называются поляризованными. Доказываются некоторые оценки сложности задания функций многозначных логик поляризованными полиномами.

Пусть $k \geq 2$, $E_k = \{0, 1, \dots, k-1\}$. Функцией k -значной логики называется отображение $f^n: E_k^n \rightarrow E_k$, $n = 0, 1, \dots$. Множество всех функций k -значной логики обозначим через P_k .

Пусть k — простое число. Тогда множество E_k с операциями сложения и умножения по модулю k образуют простое поле вычетов по модулю k . Каждая функция k -значной логики может быть записана (причем однозначно) полиномом относительно операций сложения и умножения по модулю k (см., например, [1]). Обозначим полином, задающий функцию $f(x_1, \dots, x_n)$, через $P(f)$.

Пусть $\delta = (d_1, \dots, d_n)$, где $d_1, \dots, d_n \in E_k$. Поляризованным полиномом функции $f(x_1, \dots, x_n)$ по вектору поляризации δ назовем полином по модулю k функции $f(x_1 - d_1, \dots, x_n - d_n)$ и обозначим его $P^\delta(f)$. Из существования и однозначности полинома, задающего функцию k -значной логики при простом k , следует, что для каждой функции k -значной логики поляризованный полином по каждому вектору поляризации δ существует и однозначен.

Будем полагать, что в рассматриваемых полиномах приведены все подобные слагаемые. Назовем длиной полинома P число его слагаемых с ненулевыми коэффициентами и обозначим ее $l(P)$. Введем понятие сложности функции $f(x_1, \dots, x_n)$ при задании ее поляризованными полиномами:

$$l(f) = \min l(P^\delta(f)),$$

где минимум берется по всем возможным векторам поляризации δ .

Для каждого простого k и всех n , $n \geq 1$, рассмотрим функцию Шеннона $L_k(n)$ сложности представления функций k -значной логики, зависящих от n переменных, поляризованными полиномами:

$$L_k(n) = \max l(f),$$

где максимум берется по всем функциям f , зависящим от n переменных.

В [2] была получена точная оценка функции Шеннона для булевых функций:

$$L_2(n) = \left\lceil \frac{2}{3} 2^n \right\rceil,$$

где выражение $[a]$ обозначает целую часть числа a . В [3] была получена верхняя оценка функции Шеннона:

$$L_k(n) \leq \frac{k(k-1)}{k(k-1)+1} k^n.$$

В настоящей заметке доказывается точная оценка функции Шеннона для функций, зависящих от одной переменной.

Теорема 1. Если k — простое число, то $L_k(1) = k - 1$.

Доказательство. Получим верхнюю оценку. Рассмотрим произвольную функцию $f(x)$. Пусть ее полином по модулю k есть $c_{k-1}x^{k-1} + \dots + c_1x + c_0$, где $c_{k-1}, \dots, c_1, c_0 \in E_k$. Если $c_{k-1} = 0$, то в качестве поляризованного полинома функции $f(x)$ оставим ее полином по модулю k . Его длина не больше $k - 1$. В противном случае выполним следующие преобразования:

(1) вынесем за скобки множитель c_{k-1} :

$$f(x) = c_{k-1} \left(x^{k-1} + \frac{c_{k-2}}{c_{k-1}} x^{k-2} + \dots + \frac{c_1}{c_{k-1}} x + \frac{c_0}{c_{k-1}} \right);$$

(2) в выражении, оставшемся в скобках, выделим слагаемые, образующие разложение степени $(x + d)^{k-1}$, где элемент d выбирается так, чтобы поглотить слагаемое $c_{k-2}x^{k-2}$:

$$\begin{aligned} f(x) &= c_{k-1} \left(x^{k-1} + (k-1) \frac{c_{k-2}}{c_{k-1}(k-1)} x^{k-2} + \dots \right) \\ &= c_{k-1} (x + d)^{k-1} + c'_{k-3} x^{k-3} + \dots + c'_1 x + c'_0 \end{aligned}$$

при

$$d = \frac{c_{k-2}}{c_{k-1}(k-1)}.$$

Представим функцию $f(x)$ полиномом, поляризованным по вектору $\delta = (-d)$. Его длина будет не больше $k - 1$.

Получим нижнюю оценку. Рассмотрим функцию $f(x) = ax^{k-1} + (x + 1)^{k-1}$, где $a \in E_k$. Докажем, что коэффициент a можно так подобрать, что при любой поляризации переменной x получаемый полином будет иметь не менее $k - 1$ слагаемых.

Запишем полином функции $f(x)$, поляризованный по вектору $\delta = (-d)$:

$$\begin{aligned} f(x+d) &= a(x+d)^{k-1} + (x+d+1)^{k-1} \\ &= c_{k-1}x^{k-1} + c_{k-2}x^{k-2} + \dots + c_1x + c_0, \end{aligned} \quad (1)$$

где $c_{k-1} = a + 1, c_{k-2}, \dots, c_1, c_0 \in E_k$.

Каждый коэффициент $c_{(k-1)-i}$ равен

$$C_{k-1}^{(k-1)-i}(ad^i + (d+1)^i), \quad i = 2, \dots, k-1.$$

Проведем доказательство от противного. Предположим, что среди коэффициентов $c_{k-1}, c_{k-2}, \dots, c_1, c_0$ по меньшей мере два нулевых. Пусть их номера равны $k-i$ и $k-j$, где $i \leq j$. Тогда

$$C_{k-1}^{(k-1)-i}(ad^i + (d+1)^i) = 0,$$

$$C_{k-1}^{(k-1)-j}(ad^j + (d+1)^j) = 0.$$

Или, так как $C_{k-1}^{(k-1)-i} \neq 0$ и $C_{k-1}^{(k-1)-j} \neq 0$,

$$ad^i + (d+1)^i = 0, \quad (2)$$

$$ad^j + (d+1)^j = 0. \quad (3)$$

Выразим $(d+1)^i$ из равенства (2) и подставим в равенство (3). Получим равенство

$$ad^j - ad^i(d+1)^{j-i} = 0,$$

откуда

$$ad^i(d^{j-i} - (d+1)^{j-i}) = 0.$$

Так как $ad^i \neq 0$, получаем, что

$$d^{j-i} = (d+1)^{j-i}. \quad (4)$$

Обозначим разность $j-i$ через m . Тогда, поделив левую и правую части равенства (4) на d^m (заметим, что $d^m \neq 0$), получим, что

$$(1 + 1/d)^m = 1,$$

или

$$(1 + b)^m = 1, \quad (5)$$

где $b = 1/d$. Следовательно, число m есть делитель числа $k-1$.

Рассмотрим элемент $1 + b$. Пусть e — примитивный элемент поля E_k . Тогда

$$1 + b = e^t,$$

где $1 \leq t \leq k-1$. Рассмотрим элементы поля E_k $(1+b), (1+b)^2, \dots, (1+b)^{m-1}, (1+b)^m$. Перепишем их в виде

$$e^t, e^{2t}, \dots, e^{(m-1)t}, e^{mt}. \quad (6)$$

По равенству (5) $e^{mt} = 1$. Отсюда

$$mt = (k - 1)l_1,$$

где l_1 — некоторое натуральное число. Сократим левую и правую части на m ($m \neq 0$). Получим равенство $t = sl_1$, причем $s, s \neq 1$, — делитель числа $k - 1$.

Теперь докажем, что в ряду (6) примитивный элемент e встретиться не может. Предположим противное. Пусть

$$e = (1 + b)^r = e^{rt}, \quad 1 \leq r \leq t.$$

Тогда

$$rt = (k - 1)l_2 + 1.$$

Получаем противоречие, так как левая часть последнего равенства делится на s , а правая часть при делении на s дает в остатке 1.

Следовательно, все степени элемента $1 + b$ не равны примитивному элементу e . Предположим, что $a = -e$. Из равенства (2) получаем, что

$$a = -(1 + 1/d)^i = -(1 + b)^i. \quad (7)$$

Но по доказанному равенство (7) при $a = -e$ не может выполняться, если среди коэффициентов $c_{k-1}, \dots, c_1, c_0$ в выражении (1) по меньшей мере два нулевые.

Таким образом, доказано, что

$$l_k(f) \geq k - 1.$$

Сопоставляя верхнюю и нижнюю оценку получаем, что

$$L_k(1) = k - 1.$$

Теорема 1 доказана.

Следствие 1. Если k — простое число, то $L_k(n) \geq (k - 1)^n$.

Доказательство. Достаточно рассмотреть функцию

$$g(x_1, \dots, x_n) = f(x_1)f(x_2)\dots f(x_n),$$

где $f(x)$ — функция, построенная при доказательстве справедливости нижней оценки в теореме 1.

Список литературы

1. Лидл Р., Нидеррайтер Г., *Конечные поля*. Мир, Москва, 1988.
2. Перязев Н. А., Сложность булевых функций в классе полиномиальных поляризованных форм. *Алгебра и логика* (1995) **34**, 323–326.
3. Селезнева С. Н., О сложности представления функций многозначных логик поляризованными полиномами. *Дискретная математика* (2002) **14**, №2, 48–53.

Статья поступила 20.09.2003.