Math-Net.Ru

Общероссийский математический портал

М. С. Лобанов, Об одном методе получения нижних оценок на нелинейность булевой функции, *Матем. заметки*, 2013, том 93, выпуск 5, 741–745

DOI: <https://doi.org/10.4213/mzm10233>

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: 18.234.197.8

26 апреля 2023 г., 17:49:15

Об одном методе получения нижних оценок на нелинейность булевой функции

М. С. Лобанов

Вычисление точного значения нелинейности r -го порядка для булевой функции (расстояние функции до множества функций степени не выше r) или получение нижней оценки на нее является сложной задачей (особенно для $r > 1$). В ряде работ были получены нижние оценки на нелинейность различных порядков через значение алгебраической иммунности. Эти оценки оказываются достаточно сильными, если значение алгебраической иммунности максимально или близко к максимальному. В данной статье мы докажем утверждение, которое позволяет получать довольно сильные нижние оценки на нелинейность различных порядков и для многих функций с низкой алгебраической иммунностью.

Библиография: 6 названий.

DOI: 10.4213/mzm10233

Булевой функцией называют отображение $f: F_2^n \rightarrow F_2$. *Вес набора* из F_2^n – количество единиц в этом наборе. *Вес* $wt(f)$ функции f на F_2^n – число наборов x из F_2^n , на которых $f(x) = 1$.

Каждая функция f на F_2^n может быть единственным образом представлена полиномом над F_2^n , степень которого по каждой переменной не превосходит 1. А именно,

$$f(x_1, \dots, x_n) = \bigoplus_{a_1, \dots, a_n \in F_2^n} g(a_1, \dots, a_n) x_1^{a_1} \cdots x_n^{a_n},$$

где g – это также функции на F_2^n . Такое полиномиальное представление называется *полиномом Жегалкина* функции f , а выражения $x_1^{a_1} \cdots x_n^{a_n}$ – *слагаемыми* АНФ. Далее, *алгебраическая степень* функции f , обозначаемая через $\deg(f)$ – это степень ее полинома Жегалкина.

Алгебраической иммунностью булевой функции называют величину

$$AI(f) = \min_{\substack{g \neq 0 \\ gf \equiv 0 \text{ или } g(f+1) \equiv 0}} \deg(g).$$

Известно [1], [2], что для любой f над F_2^n выполнено $AI(f) \leq \lceil n/2 \rceil$.

Нелинейностью r -го порядка $nl_r(f)$ булевой функции f над F_2^n называется

$$\min_{\deg(l) \leq r} d(f, l),$$

где $d(f, l)$ – это расстояние Хэмминга.

Ранее в [3], [4] были доказаны точные оценки на нелинейность первого и второго порядков через значение алгебраической иммунности, а в [5] оценка (неточная) для нелинейности r -го порядка:

$$\begin{aligned} nl_1(f) &\geq 2 \sum_{i=0}^{AI(f)-2} \binom{n-1}{i}, \\ nl_2(f) &\geq \sum_{i=0}^{AI(f)-1} \binom{n}{i} - \sum_{i=0}^{AI(f)-1} 2^i \binom{n-2i-1}{AI(f)-1-i}, \\ nl_r(f) &\geq \sum_{i=0}^{AI(f)-r-1} \binom{n}{i} + \sum_{i=AI(f)-2r}^{AI(f)-r-1} \binom{n-r}{i}. \end{aligned} \quad (1)$$

При значении $AI(f)$, близком к максимально возможному, оценки получаются довольно сильными, но для функций с низкой $AI(f)$ эти оценки дают не очень хорошие результаты. В статье [6] $nl_r(f)$ оценивается не через $AI(f)$, а через величины $\min_{g \neq 0, gf=0} \deg(g)$ и $\min_{g \neq 0, g(f+1)=0} \deg(g)$, что позволяет обобщить оценку (1) и для некоторых функций с низкой алгебраической иммунностью получить лучшие нижние оценки на $nl_r(f)$.

В данной работе мы докажем теорему, которая обобщает как результат автора [4] о получении нижних оценок на $nl_r(f)$ через значение $AI(f)$, так и результат [6], и которая позволяет для многих функций получить более сильные оценки на $nl_r(f)$.

ОПРЕДЕЛЕНИЕ 1. Пусть $h(x_1, \dots, x_n)$ булева функция от n переменных. Обозначим

$$An_k(h) = \{g(x_1, \dots, x_n) \mid gh = 0, \deg(g) \leq k\}.$$

ОПРЕДЕЛЕНИЕ 2. Пусть $C = \{\bar{x}^1, \dots, \bar{x}^m\}$ множество двоичных наборов длины n . Для любого $k \leq n$ произвольному набору $x = (x_1, \dots, x_n)$ сопоставим однородное линейное уравнение, получаемое подстановкой компонент набора в

$$a_0 + \sum_{i=1}^n a_i x_i + \sum_{1 \leq i < j \leq n} a_{ij} x_i x_j + \dots + \sum_{1 \leq i_1 < \dots < i_k \leq n} a_{i_1 \dots i_k} x_{i_1} \dots x_{i_k}$$

и приравниванием полученного выражения к 0. Назовем k -рангом множества C ранг системы линейных уравнений, полученных таким образом из наборов множества C . Обозначим его через $r_k(C)$.

Найдем все функции из $An_k(f)$ методом неопределенных коэффициентов:

$$g = a_0 + \sum_{i=1}^n a_i x_i + \sum_{1 \leq i < j \leq n} a_{ij} x_i x_j + \dots + \sum_{1 \leq i_1 < \dots < i_k \leq n} a_{i_1 \dots i_k} x_{i_1} \dots x_{i_k}.$$

Функция g является аннигилятором f тогда и только тогда, когда $f(x) = 1$ влечет $g(x) = 0$. Таким образом, получим систему линейных уравнений на коэффициенты.

Размерность пространства решений однородной линейной системы уравнений равна числу переменных минус ранг системы, поэтому

$$\dim(An_k(f)) = \sum_{i=0}^k \binom{n}{i} - r_k(\text{supp}(f)). \quad (2)$$

УТВЕРЖДЕНИЕ 1. Пусть f и f_0 – функции от n переменных, $1 \leq k_1, k_2 \leq n$,

$$\dim(An_{k_1}(f)) \geq \dim(An_{k_1}(f_0)), \quad \dim(An_{k_2}(f+1)) \geq \dim(An_{k_2}(f_0+1)).$$

Тогда

$$d(f, f_0) \geq \dim(An_{k_1}(f)) - \dim(An_{k_1}(f_0)) + \dim(An_{k_2}(f+1)) - \dim(An_{k_2}(f_0+1)).$$

ДОКАЗАТЕЛЬСТВО. Из (2) следует

$$r_{k_1}(\text{supp}(f_0)) - r_{k_1}(\text{supp}(f)) = \dim(An_{k_1}(f)) - \dim(An_{k_1}(f_0)).$$

Следовательно, существует не меньше чем $\dim(An_{k_1}(f)) - \dim(An_{k_1}(f_0))$ наборов, где f_0 равна единице, а f нулю.

Аналогично получаем, что число наборов, где f единица, а f_0 ноль, не меньше чем $\dim(An_{k_2}(f+1)) - \dim(An_{k_2}(f_0+1))$.

ОПРЕДЕЛЕНИЕ 3. Пусть h – булева функция от n переменных. Определим

$$B_{k_1, k_2}(h) = \{g(x_1, \dots, x_n) \mid \deg(g) \leq k_1, \deg(gh) \leq k_2\}.$$

В [4] фактически была доказана оценка

$$\dim(B_{k, k}(h)) \geq \sum_{i=0}^{k-r} \binom{n}{i} + \sum_{i=k-2r+1}^{k-r} \binom{n-r}{i}. \quad (3)$$

УТВЕРЖДЕНИЕ 2. Пусть $k_1 \geq k_2$; тогда верно равенство

$$\dim(An_{k_1}(f)) + \dim(An_{k_2}(f+1)) = \dim(B_{k_1, k_2}(f)).$$

ДОКАЗАТЕЛЬСТВО. Для доказательства утверждения достаточно показать, что пространство $B_{k_1, k_2}(f)$ является прямой суммой пространств $An_{k_1}(f)$ и $An_{k_2}(f+1)$.

Так как $An_{k_1}(f) \cap An_{k_2}(f+1) = 0$, остается проверить, что любая функция из $B_{k_1, k_2}(f)$ представима как сумма каких-то функций из $An_{k_1}(f)$ и $An_{k_2}(f+1)$, а сумма любых функций из $An_{k_1}(f)$ и $An_{k_2}(f+1)$ дает функцию из $B_{k_1, k_2}(f)$.

Пусть $g_1 \in An_{k_1}(f)$, а $g_2 \in An_{k_2}(f+1)$. Тогда $g_1 + g_2 \in B_{k_1, k_2}(f)$. Действительно,

$$\begin{aligned} \deg(g_1 + g_2) &\leq \max(\deg(g_1), \deg(g_2)) \leq k_1, \\ \deg((g_1 + g_2)f) &= \deg(g_1f + g_2(f+1) + g_2) = \deg(g_2) \leq k_2. \end{aligned}$$

Обратно, пусть $g \in B_{k_1, k_2}(f)$. Тогда $g(f+1) \in An_{k_1}(f)$, а $gf \in An_{k_2}(f+1)$. Это следует из определения пространства $B_{k_1, k_2}(f)$ и того, что

$$\begin{aligned} gf(f+1) &\equiv 0, \\ \deg(g(f+1)) &= \deg(gf + g) \leq \max(\deg(gf), \deg(g)) \leq k_1. \end{aligned}$$

Так как $g = gf + g(f+1)$, любая функция $g \in B_{k_1, k_2}(f)$ может быть представлена как сумма $g = g_1 + g_2$, где

$$g_1 = g(f+1) \in An_{k_1}(f), \quad g_2 = gf \in An_{k_2}(f+1).$$

Как простое следствие утверждений 1 и 2 получаем

СЛЕДСТВИЕ 1. Пусть f и f_0 – функции от n переменных, $1 \leq k_2 \leq k_1 \leq n$,

$$\dim(An_{k_1}(f)) \geq \dim(An_{k_1}(f_0)), \quad \dim(An_{k_2}(f+1)) \geq \dim(An_{k_2}(f_0+1)).$$

Тогда

$$d(f, f_0) \geq \dim(B_{k_1, k_2}(f)) - \dim(B_{k_1, k_2}(f_0)).$$

Отдельно рассмотрев случай приближения константами, из следствия 1 получаем следующую оценку на нелинейность r -го порядка.

ТЕОРЕМА 1. Пусть для $f(x_1, \dots, x_n)$ выполнено

$$\begin{aligned} \min_{1 \leq \deg(g) \leq r} \dim(An_{k_1}(g)) &\geq \dim(An_{k_1}(f)), \\ \min_{1 \leq \deg(g) \leq r} \dim(An_{k_1}(g)) &\geq \dim(An_{k_1}(f+1)). \end{aligned}$$

Тогда

$$nl_r(f) \geq \min \left(\min_{\deg(g) \leq r} \dim(B_{k_1, k_2}(g)) - \dim(B_{k_1, k_2}(f)), wt(f), wt(f+1) \right),$$

если $k_1 \geq k_2$, и

$$nl_r(f) \geq \min \left(\min_{\deg(g) \leq r} \dim(B_{k_2, k_1}(g)) - \dim(B_{k_2, k_1}(f+1)), wt(f), wt(f+1) \right),$$

если $k_1 < k_2$.

Докажем утверждение, которое может быть полезным для проверки условий теоремы 1.

УТВЕРЖДЕНИЕ 3. Верно неравенство

$$\min_{1 \leq \deg(g) \leq r} \dim(An_k(g)) \geq \sum_{i=0}^{k-r} \binom{n-r}{i}.$$

ДОКАЗАТЕЛЬСТВО. Для произвольной функции g степени не больше r выберем один из ее главных мономов. Тогда все функции, получающиеся умножением $g+1$ на произвольную функцию степени не выше $k-r$, не зависящую от переменных в этом мономе, будут различными и при этом лежать в $An_k(g)$.

Теорема 1 обобщает соответствующие результаты из работ [4]–[6], поэтому оценки, получаемые с ее помощью, заведомо не хуже. Ниже мы покажем, что на самом деле для конкретных функций эта теорема дает более сильные оценки на $nl_r(f)$, чем результаты из работ [4]–[6].

Определим для $n = 4k + 1$ функцию $f_n(x_1, \dots, x_n)$ следующим образом:

$$f_n(x_1, \dots, x_n) = \begin{cases} 0, & \text{если } wt(x_1, \dots, x_n) \leq 2k, \\ 1, & \text{если } wt(x_1, \dots, x_n) > 2k. \end{cases}$$

Рассмотрим функцию $f = f_n \cdot (x_1 \vee x_2 \vee \dots \vee x_k) \vee x_1 x_2 \dots x_k$. Несложно доказать, что $AI(f) = k$. Из [4], [5] и из [6] с учетом (3) следует одна и та же оценка:

$$nl_r(f) \geq \min_{\deg(g) \leq r} \dim(B_{k-1, k-1}(g)) \geq \sum_{i=0}^{k-r-1} \binom{n}{i} + \sum_{i=k-2r}^{k-r-1} \binom{n-r}{i}.$$

В то же время из теоремы 1 и утверждения 3 можно получить заметно более сильную оценку

$$\begin{aligned} nl_r(f) &\geq \min_{\deg(g) \leq r} \dim(B_{2k, 2k}(g)) - 2 \sum_{i=0}^k \binom{n-k}{i} \\ &\geq \sum_{i=0}^{2k-r} \binom{n}{i} + \sum_{i=2k-2r+1}^{2k-r} \binom{n-r}{i} - 2 \sum_{i=0}^k \binom{n-k}{i}. \end{aligned}$$

СПИСОК ЦИТИРОВАННОЙ ЛИТЕРАТУРЫ

- [1] N. T. Courtois, W. Meier, “Algebraic attacks on stream ciphers with linear feedback”, *Advances in cryptology – EUROCRYPT 2003*, Lecture Notes in Comput. Sci., **2656**, Springer-Verlag, Heidelberg, 2003, 345–359.
- [2] W. Meier, E. Pasalic, C. Carlet, “Algebraic attacks and decomposition of Boolean functions”, *Advances in Cryptology – EUROCRYPT 2004*, Lecture Notes in Comput. Sci., **3027**, Springer-Verlag, Heidelberg, 2004, 474–491.
- [3] М. С. Лобанов, “Точное соотношение между нелинейностью и алгебраической иммунностью”, *Дискрет. матем.*, **18**:3 (2006), 152–159.
- [4] М. С. Лобанов, “Точные соотношения между нелинейностью и алгебраической иммунностью”, *Дискретн. анализ и исслед. опер.*, **15**:6 (2008), 34–47.
- [5] S. Mesnager, “Improving the lower bound on the higher order nonlinearity of Boolean functions with prescribed algebraic immunity”, *IEEE Trans. Inform. Theory*, **54**:8 (2008), 3656–3662.
- [6] P. Rizomiliotis, “Improving the high order nonlinearity lower bound for Boolean functions with given algebraic immunity”, *Discrete Appl. Math.*, **158**:18 (2010), 2049–2055.

М. С. Лобанов

Московский государственный университет

им. М. В. Ломоносова

E-mail: misha-msu@mail.ru

Поступило

24.05.2012