

УДК 517.7, 519.1

ТОЧНЫЕ СООТНОШЕНИЯ МЕЖДУ НЕЛИНЕЙНОСТЬЮ И АЛГЕБРАИЧЕСКОЙ ИММУННОСТЬЮ*)

М. С. Лобанов

Аннотация. Усилены некоторые нижние оценки нелинейности высоких порядков булевой функции через значения её алгебраической иммунности и получены новые точные оценки. Доказана универсальная точная нижняя оценка, позволяющая сводить проблему оценки нелинейности высоких порядков к проблеме поиска размерности некоторых линейных подпространств в пространстве булевых функций. Как простое следствие этого результата получены все ранее известные оценки в этой области. Для бесповторных полиномов поиск размерности упомянутых выше линейных подпространств в пространстве булевых функций сведён к простому комбинаторному анализу. Для булевой функции доказана точная нижняя оценка её нелинейности второго порядка через значение алгебраической иммунности.

Ключевые слова: потоковый шифр, нелинейный фильтр, алгебраическая атака, булева функция, алгебраическая иммунность, степень булевой функции, нелинейность, нелинейность высокого порядка, аннигилятор.

Введение

Булевы функции нашли широкое применение в криптографии, в частности, в симметричной криптографии. Например, булевы функции используются в потоковых шифрах в качестве нелинейных фильтров. Также они применяются в блочных шифрах в S-блоках. Требование устойчивости схем шифрования к существующим атакам накладывает на различные элементы этих схем определённые условия, которым они должны удовлетворять. В случае с потоковыми шифрами речь обычно идёт о

*) Исследование выполнено при финансовой поддержке Российского фонда фундаментальных исследований (проект 08-01-00863), программы поддержки ведущих научных школ РФ (проект НШ-4470.2008.1), программы фундаментальных исследований Отделения математических наук РАН «Алгебраические и комбинаторные методы математической кибернетики» (проект «Синтез и сложность управляющих систем»).

том, чтобы булевы функции, используемые в качестве нелинейных фильтров, обладали целым набором криптографических свойств. Среди этих свойств наряду с другими можно выделить алгебраическую иммунность и нелинейность высоких порядков.

В последнее время появился ряд работ [1, 2, 4, 6, 8], в которых затрагиваются вопросы взаимосвязи этих двух свойств. Одной из самых интересных является проблема получения нижних оценок нелинейности различных порядков функции через значение её алгебраической иммунности. Это тем более важно, так как для нахождения значения алгебраической иммунности функции в последнее время предложено несколько алгоритмов, а для подсчёта нелинейности высоких порядков, насколько нам известно, эффективных алгоритмов не существует.

В работе [5] была предложена точная нижняя оценка нелинейности (первого порядка) через значение алгебраической иммунности функции. Нижние оценки нелинейности r -го порядка через алгебраическую иммунность были предложены в [2, 4, 6, 8]. Наиболее сильной из них является неравенство (4).

В данной работе предложен новый подход к получению для булевой функции как можно более сильных нижних оценок её нелинейности высоких порядков через значение алгебраической иммунности. По сути, проблема сведена к оценке размерности определённых линейных подпространств в пространстве всех булевых функций фиксированного числа переменных. Этот результат приведён в теореме 1. Эта теорема представляет собой новую универсальную оценку нелинейности r -го порядка через значение алгебраической иммунности функции. Эта оценка является точной в том смысле, что для любых допустимых значений параметров существует функция, достигающая оценки. Мы выведем все предложенные ранее оценки в этой области как простые следствия теоремы 1.

Далее, в теореме 2 для некоторого класса функций сведём проблему подсчёта размерности линейных подпространств из теоремы 1 к комбинаторному подсчёту. Используя теорему 2, докажем теорему 3, в которой будет предъявлена точная нижняя оценка нелинейности второго порядка функции через значение её алгебраической иммунности.

Оставшаяся часть работы организована следующим образом.

В разд. 1 приведены необходимые определения и некоторые ранее известные результаты. В разд. 2 доказана теорема 1, которая сводит проблему оценки нелинейности высоких порядков к оценке размерности определённых линейных подпространств в пространстве всех булевых

функций. Как простые следствия получены известные ранее оценки в этой области. В разд. 3 для определённого вида полиномов доказана теорема 2, позволяющая свести подсчёт размерности линейных подпространств из теоремы 1 к несложному комбинаторному анализу. И, наконец, в разд. 4 доказана теорема 3 — точная оценка нелинейности r -го порядка через алгебраическую иммунность.

1. Основные определения и известные результаты

Пусть f является булевой функцией над F_2^n . Известно, что f единственным образом представляется полиномом. *Степенью* булевой функции называется длина самого длинного слагаемого в её полиноме (количество переменных в этом слагаемом). Булева функция g над F_2^n называется *аннигилятором* булевой функции f над F_2^n , если $fg = 0$. Очевидно, что аннигиляторы f образуют линейное подпространство в пространстве всех булевых функций от n переменных. *Алгебраической иммунностью* $AI(F)$ булевой функции f над F_2^n называется степень булевой функции g над F_2^n , где g — не равная тождественно нулю функция с минимальной степенью такая, что $fg = 0$ или $(f+1)g = 0$. Известно [5, 7], что для любой f над F_2^n выполнено $AI(f) \leq \lceil \frac{n}{2} \rceil$.

Весом $wt(x)$ набора x из F_2^n называется число единиц в x . *Расстояние* между булевыми функциями f_1 и f_2 определяется как

$$d(f_1, f_2) = |\{x \in F_2^n \mid f_1(x) \neq f_2(x)\}|.$$

Нелинейностью r -го порядка $nl_r(f)$ булевой функции f над F_2^n называется $\min_{l, \deg(l) \leq r} d(f, l)$. *Нелинейностью* $nl(f)$ функции f называется расстояние между f и множеством аффинных функций, т. е. нелинейность первого порядка.

В [3] доказан результат, эквивалентный следующей оценке на нелинейность r -го порядка:

$$nl_r(f) \geq \sum_{i=0}^{AI(f)-r-1} \binom{n}{i}. \quad (1)$$

Позже в [5] доказана нижняя оценка нелинейности ($r = 1$) функции через значение её алгебраической иммунности:

$$nl(f) \geq 2 \sum_{i=0}^{AI(f)-2} \binom{n-1}{i}. \quad (2)$$

Там же для всех допустимых значений алгебраической иммунности были построены функции, на которых достигается равенство в приведённой оценке. Затем Карле в [1] обобщил оценку (2) на случай $r \geq 1$:

$$nl_r(f) \geq 2 \sum_{i=0}^{AI(f)-r-1} \binom{n-r}{i}. \quad (3)$$

Отметим, что ни одна из двух приведённых выше оценок нелинейности r -го порядка не влечёт другую.

В [2] и [6] доказана оценка

$$nl_r(f) \geq \sum_{i=0}^{AI(f)-r-1} \binom{n}{i} + \sum_{i=AI(f)-2r}^{AI(f)-r-1} \binom{n-r}{i}, \quad (4)$$

более сильная, чем (1) и (3).

2. Сведение задачи к оценке размерности определённых линейных пространств булевых функций

Определение 1. Пусть h — булева функция от n переменных. Обозначим через $An_k(h)$ линейное пространство аннигиляторов степени не выше k и через $d_{k,h}$ его размерность.

Определение 2. Пусть $C = \{\bar{x}_1, \dots, \bar{x}_k\}$ — множество двоичных наборов длины n . Для любого $k \leq n$ произвольному набору $x = (x_1, \dots, x_n)$ можно сопоставить однородное линейное уравнение, получаемое подстановкой компонент набора в выражение

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

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

Ищем для функции f аннигиляторы степени не выше k методом неопределённых 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 функции f тогда и только тогда, когда $f(x) = 1$ влечёт $g(x) = 0$. Получаем систему линейных уравнений.

Несложно заметить, что

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

Утверждение 1. Пусть f и f_0 — функции от n переменных, $AI(f_0) \geq k$. Тогда $d(f, f_0) \geq \dim(An_{k-1}(f)) + \dim(An_{k-1}(f+1))$.

ДОКАЗАТЕЛЬСТВО. Так как $AI(f_0) \geq k$, то

$$r_{k-1}(\text{supp}(f_0)) = \sum_{i=0}^{k-1} \binom{n}{i}.$$

В то же время

$$r_{k-1}(\text{supp}(f)) = \sum_{i=0}^{k-1} \binom{n}{i} - d_{k-1,f}.$$

Следовательно, существует не меньше чем $d_{k-1,f}$ наборов, где f_0 равна единице, а f нулю.

Аналогично рассматриваем $f+1$ и f_0+1 , получаем оценку на число наборов, где f — единица, а f_0 — нуль. Утверждение 1 доказано.

Определение 3. Пусть h — булева функция от n переменных. Обозначим через $B_k(h)$ линейное пространство функций от n переменных степени не выше k , которые при умножении на h снова дают функции степени не выше k .

Утверждение 2. Имеет место равенство

$$\dim(An_k(f)) + \dim(An_k(f+1)) = \dim(B_k(f)).$$

ДОКАЗАТЕЛЬСТВО. Рассмотрим пару (g_1, g_2) , где $g_1 \in An_k(f)$, $g_2 \in An_k(f+1)$. Тогда $fg_1 + (f+1)g_2 = 0$, отсюда $f(g_1 + g_2) = g_2$. Получим соответствие между парами функций из $An_k(f) \times An_k(f+1)$ и функциями из $B_k(f)$. Несложно проверить, что соответствие взаимно однозначное. Утверждение 2 доказано.

Лемма 1. Пусть $r_k(\text{supp}(f)) = wt(f)$, где $k < \lceil \frac{n}{2} \rceil$. Тогда

$$\dim(An_k(f+1)) = 0.$$

ДОКАЗАТЕЛЬСТВО. Из условия следует, что для любого набора x такого, что $f(x) = 1$, существует функция g степени не выше k , что произведение fg равно 1 только на одном наборе x . В противном случае существовала бы функция, отличная от f лишь на наборе x с k -рангом $r_k(\text{supp}(f)) = wt(f)$ и весом, равным $wt(f) - 1$, что невозможно.

Пусть существует такая функция f' , $\deg(f') \leq k$ и $f \neq 0$, что $(f+1)f' = 0$. Возьмём набор x такой, что $f'(x) = 1$. Из того, что $\text{supp}(f') \subseteq \text{supp}(f)$, следует, что существует функция g' степени не выше k такая, что произведение $f'g'$ равно 1 только на одном наборе x . Но степень произведения двух булевых функций не превосходит суммы степеней этих функций, поэтому $\deg(f'g') < n$, что противоречит тому, что $f'g'$ равно 1 ровно на одном наборе. Лемма 1 доказана.

Следствие 1. Пусть $\dim(An_k(f)) = \sum_{i=0}^k \binom{n}{i} - wt(f)$, где $k < \lceil \frac{n}{2} \rceil$. Тогда $\dim(An_{\lceil \frac{n}{2} \rceil - 1}(f+1)) = 0$.

Следствие 2. Пусть $n = 2k + 1$ и $An_k(f) = 0$. Тогда $AI(f) = k + 1$.

Следствие 2 получено в [3].

Утверждение 3. Пусть $\deg(f) \leq \lceil \frac{n}{2} \rceil$, $k \leq \lceil \frac{n}{2} \rceil$. Тогда существует функция g такая, что $AI(g) = k$ и $d(f, g) = \dim(B_{k-1}(f))$.

ДОКАЗАТЕЛЬСТВО. Среди наборов, на которых f равна 1, найдётся $r_{k-1}(\text{supp}(f))$ таких, что их $(k-1)$ -ранг тоже будет равен $r_{k-1}(\text{supp}(f))$, обозначим это множество наборов через C_1 . Аналогично, рассмотрев $f+1$, получим множество C_0 из $r_{k-1}(\text{supp}(f+1))$ наборов. Из леммы 1 следует, что мы можем дополнить C_1 за счёт $\sum_{i=0}^{k-1} \binom{n}{i} - r_{k-1}(\text{supp}(f))$ наборов, которые не входят в C_0 и на которых f равна 0, так, чтобы k -ранг нового множества был в точности равен $\sum_{i=0}^{k-1} \binom{n}{i}$. Аналогично мы можем дополнить и множество C_0 за счёт $\sum_{i=0}^{k-1} \binom{n}{i} - r_{k-1}(\text{supp}(f+1))$ наборов, которые не входят в C_1 и на которых f равна 1, так, чтобы k -ранг нового множества был в точности равен $\sum_{i=0}^{k-1} \binom{n}{i}$.

Из вышесказанного следует, что можно изменить значение f на

$$\begin{aligned} & \sum_{i=0}^{k-1} \binom{n}{i} - r_{k-1}(\text{supp}(f)) + \sum_{i=0}^{k-1} \binom{n}{i} - r_{k-1}(\text{supp}(f+1)) \\ &= \dim(An_{k-1}(f)) + \dim(An_{k-1}(f+1)) = \dim(B_{k-1}(f)) \end{aligned}$$

наборах и получить функцию g такую, что

$$\dim(An_{k-1}(g)) = \dim(An_{k-1}(g+1)) = 0.$$

Следовательно, $AI(g) = k$. Утверждение 3 доказано.

Таким образом, с учётом утверждений 1–3 доказано, что задача нахождения наиболее сильной оценки нелинейности r -го порядка функции через значение её алгебраической иммунности k полностью сводится к нахождению $\min_{\deg(g) \leq r} \dim(B_{k-1}(g))$. Сформулируем это в качестве теоремы.

Теорема 1. Пусть $f(x_1, \dots, x_n)$ имеет $AI(f) = k$. Тогда

$$nl_r(f) \geq \min_{\deg(g) \leq r} \dim(B_{k-1}(g)).$$

Кроме того, при $k \leq \lceil \frac{n}{2} \rceil$ существует функция f_0 , $AI(f_0) = k$, для которой

$$nl_r(f_0) = \min_{\deg(g) \leq r} \dim(B_{k-1}(g)).$$

Теперь посмотрим, какие конкретные оценки можно получить из теоремы 1.

Утверждение 4. Пусть $\deg(f) = r$. Тогда

$$\dim(B_{k-1}(f)) \geq \sum_{i=0}^{k-r-1} \binom{n}{i}.$$

ДОКАЗАТЕЛЬСТВО вытекает из рассмотрения всех функций степени не больше $(k - r - 1)$.

Следствие 3. Пусть $AI(g) = k$. Тогда

$$nl_r(g) \geq \sum_{i=0}^{k-r-1} \binom{n}{i}.$$

Мы получили оценку (1) из [3].

Утверждение 5. Пусть $\deg(f) = r$. Тогда

$$\dim(B_{k-1}(f)) \geq 2 \sum_{i=0}^{k-r-1} \binom{n-r}{i}.$$

ДОКАЗАТЕЛЬСТВО. Можно считать, что полином f содержит слагаемое $x_1 x_2 \dots x_r$. Рассмотрим функции вида $f g_1 + (f + 1) g_2$, где g_1 и g_2 — любые функции от x_{m+1}, \dots, x_n степени не более $(k - r - 1)$. Несложно проверить, что все такие функции различны и принадлежат $B_{k-1}(f)$. Утверждение 5 доказано.

Следствие 4. Пусть $AI(g) = k$. Тогда

$$nl_r(g) \geq 2 \sum_{i=0}^{k-r-1} \binom{n-r}{i}.$$

Мы получили оценку (3) из [1].

Утверждение 6. Пусть $\deg(f) = r$. Тогда

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

ДОКАЗАТЕЛЬСТВО. Можно считать, что полином f содержит слагаемое $x_1 x_2 \dots x_r$. Рассмотрим функции вида $g_1 + f g_2$, где g_1 — любая функция степени не более $(k-r-1)$, а g_2 — любая функция от x_{r+1}, \dots, x_n степени не более $(k-r-1)$, содержащая лишь мономы длины не менее $k-2r$.

Несложно проверить, что все такие функции принадлежат $B_{k-1}(f)$. Проверка того, что все функции различны, сводится к проверке того, что из $g_1 + f g_2 = 0$ следует $g_1 = 0$ и $g_2 = 0$. Равенство $g_2 = 0$ следует из того, что в противном случае функция $f g_2$ содержала бы моном длины не менее $(k-r)$, который был бы и в полиноме f (так как $\deg(f_1) \leq (k-r-1)$). Равенство $g_1 = 0$ следует непосредственно из $g_1 + f g_2 = 0$ и $g_2 = 0$. Утверждение 6 доказано.

Следствие 5. Пусть $AI(g) = k$. Тогда

$$nl_r(g) \geq \sum_{i=0}^{k-r-1} \binom{n}{i} + \sum_{i=k-2r}^{k-r-1} \binom{n-r}{i}.$$

Мы получили оценку (4) из [2, 8].

Теорема 1 даёт возможность получения и более сильных следствий. О некоторых из них речь пойдёт ниже.

3. Точное значение $\dim(B_k(f))$ для бесповторных полиномов

Определение 4. Пусть $a_1 \geq a_2 \geq \dots \geq a_q > 0$ — набор целых чисел таких, что $\sum_{i=1}^q a_i \leq n$. Тогда двоичному набору $x = (x_1, \dots, x_n)$ длины n можно сопоставить набор $s_{a_1, \dots, a_q}(x)$ из целых чисел:

$$(s_1(x), \dots, s_q(x)) = \left(\sum_{i=1}^{a_1} x_i, \sum_{i=a_1+1}^{a_1+a_2} x_i, \dots, \sum_{i=a_1+\dots+a_{q-1}+1}^{a_1+\dots+a_q} x_i \right).$$

Обозначим через $S_{a_1, \dots, a_q}(k)$ множество двоичных наборов x длины n таких, что $s_t(x) = 0$ при некотором $t \leq q$, $0 < s_i(x) < a_i$ при $i < t$ и $k - a_t < wt(x) \leq k$.

Утверждение 7. Пусть любые два монома, входящие в полиномиальную запись функции $f(x_1, \dots, x_n)$, не содержат общих переменных. Пусть q — число мономов в полиноме функции, а $a_1 \geq a_2 \geq \dots \geq a_q$ — длины этих мономов. Тогда

$$\dim(B_k(f)) \leq \sum_{i=0}^k \binom{n}{i} - |S_{a_1, \dots, a_q}(k)|.$$

ДОКАЗАТЕЛЬСТВО. Можно считать, что функция имеет вид

$$f = x_1 x_2 \cdot \dots \cdot x_{a_1} + x_{a_1+1} \cdot \dots \cdot x_{a_1+a_2} + \dots \\ + x_{a_1+\dots+a_{q-1}+1} \cdot \dots \cdot x_{a_1+\dots+a_q}.$$

Любому двоичному набору длины n можно сопоставить моном, состоящий из тех переменных x_1, \dots, x_n , которым соответствуют единицы в исходном наборе.

Рассмотрим линейное подпространство $C_{f,k}$ в пространстве булевых функций от n переменных, натянутое на мономы, соответствующие наборам, входящим в $S_{a_1, \dots, a_q}(k)$. Это пространство является также подпространством и в пространстве функций степени не выше k . Любая не равная тождественно нулю функция из $C_{f,k}$ не принадлежит $B_k(f)$. Действительно, пусть $g \in C_{f,k}$, тогда каждому моному из g и соответствующему ему набору $x = (x_1, \dots, x_n)$ можно сопоставить своё $t \leq q$ из определения 4 такое, что $s_t(x) = 0$ и $0 < s_i(x) < a_i$ при $i < t$. Выберем из мономов функции g мономы с наибольшей длиной, а среди них возьмём какой-нибудь моном $x_{i_1} \cdot \dots \cdot x_{i_h}$, которому соответствует наименьшее t , тогда в запись функции gf входит моном

$$x_{i_1} \cdot \dots \cdot x_{i_h} x_{a_1+\dots+a_{t-1}+1} \cdot \dots \cdot x_{a_1+\dots+a_t},$$

который ни с чем сократиться не может. Значит, $\deg(fg) > k$ и g не принадлежит $B_k(f)$.

Размерность $C_{f,k}$ равна $|S_{a_1, \dots, a_q}(k)|$, из чего и следует утверждение 7.

Теперь докажем обратное неравенство.

Утверждение 8. Пусть любые два монома, входящие в полиномиальную запись функции $f(x_1, \dots, x_n)$, не содержат общих переменных.

Пусть q — число мономов в полиноме функции, а $a_1 \geq a_2 \geq \dots \geq a_q$ — длины этих мономов. Тогда

$$\dim(B_k(f)) \geq \sum_{i=0}^k \binom{n}{i} - |S_{a_1, \dots, a_q}(k)|.$$

ДОКАЗАТЕЛЬСТВО. Можно считать, что функция имеет вид

$$f = x_1 x_2 \cdot \dots \cdot x_{a_1} + x_{a_1+1} \cdot \dots \cdot x_{a_1+a_2} + \dots \\ + x_{a_1+\dots+a_{q-1}+1} \cdot \dots \cdot x_{a_1+\dots+a_q}.$$

Обозначим через $\overline{S_{a_1, \dots, a_q}(k)}$ множество наборов $x = (x_1, \dots, x_n)$, $wt(x) \leq k$ и $x \notin S_{a_1, \dots, a_q}(k)$.

Пусть $x = (x_1, \dots, x_n) \in \overline{S_{a_1, \dots, a_q}(k)}$. Поставим в соответствие набору x функцию f_x по следующим правилам.

1. Если $\deg(x_{i_1} x_{i_2} \cdot \dots \cdot x_{i_{wt(x)}} f) \leq k$, где $i_1, \dots, i_{wt(x)}$ — номера мест, на которых стоят единицы в x , то $f_x = x_{i_1} x_{i_2} \cdot \dots \cdot x_{i_{wt(x)}}$.

2. Если x не подпадает под первый случай и $0 < s_t(x) \leq a_i$ при любом $t \leq q$, то

$$f_x = (x_{i_1} \cdot \dots \cdot x_{i_{s_1(k)}} + 1) \cdot \dots \cdot (x_{i_{s_1(k)+\dots+s_{q-1}(k)+1}} \cdot \dots \cdot x_{i_{s_1(k)+\dots+s_q(k)}} + 1),$$

где $i_1, \dots, i_{s_1(k)+\dots+s_q(k)}$ — номера мест, на которых стоят единицы в x .

3. Если x не подпадает ни под один из предыдущих двух случаев и $s_t(x) = 0$, $0 < s_i(x) < a_i$ при $i < t$, то

$$f_x = (x_{i_1} \cdot \dots \cdot x_{i_{s_1(k)}} + 1) \cdot \dots \cdot (x_{i_{s_1(k)+\dots+s_{q-1}(k)+1}} \cdot \dots \cdot x_{i_{s_1(k)+\dots+s_q(k)}} + 1),$$

где $i_1, \dots, i_{s_1(k)+\dots+s_q(k)}$ — номера мест, на которых стоят единицы в x .

4. Если x не подпадает ни под один из предыдущих трёх случаев, то $s_t(x) = 1$ при некотором $t \leq q$ и $s_i(k) = 0$ при $i = b_1, \dots, b_u$, где $b_h > t$ ($0 < s_i(x) < a_i$ при $i < t$ и $0 < s_i(x)$ при $i \neq t, b_1, \dots, b_u$) Тогда

$$f_x = (x_{i_1} \cdot \dots \cdot x_{i_{s_1(k)}} + 1) (x_{i_{s_1(k)+1}} \cdot \dots \cdot x_{i_{s_1(k)+s_2(k)}} + 1) \times \dots \\ \times (x_{i_{s_1(k)+\dots+s_{t-2}(k)+1}} \cdot \dots \cdot x_{i_{s_1(k)+\dots+s_{t-1}(k)}} + 1) \\ \times (x_{i_{s_1(k)+\dots+s_t(k)+1}} \cdot \dots \cdot x_{i_{s_1(k)+\dots+s_{t+1}(k)}} + 1) \\ \times (x_{i_{s_1(k)+\dots+s_{q-1}(k)+1}} \cdot \dots \cdot x_{i_{s_1(k)+\dots+s_q(k)}} + 1) \times \dots \\ \times (x_{a_1+\dots+a_{t-1}+1} \cdot \dots \cdot x_{a_1+\dots+a_t} + x_{a_1+\dots+a_{b_1-1}+1} \cdot \dots \cdot x_{a_1+\dots+a_{b_1}} + \\ \dots + x_{a_1+\dots+a_{b_u-1}+1} \cdot \dots \cdot x_{a_1+\dots+a_{b_u}}),$$

где $i_1, \dots, i_{s_1(k)+\dots+s_q(k)}$ — номера мест, на которых стоят единицы в x .

Как можно убедиться, по приведённому выше правилу каждому набору $x = (x_1, \dots, x_n) \in \overline{S_{a_1, \dots, a_q}(k)}$ сопоставляется единственная функция f_x .

В запись f_x для любого описанного выше набора x входит моном, содержащий все переменные, которые соответствуют единицам в наборе x , все остальные мономы имеют меньшую длину или меньший лексикографический порядок. Отсюда следует линейная независимость всех f_x , соответствующих наборам $x = (x_1, \dots, x_n) \in \overline{S_{a_1, \dots, a_q}(k)}$. Действительно, пусть есть наборы $x^1, \dots, x^h \in \overline{S_{a_1, \dots, a_q}(k)}$, выберем среди них наборы с наибольшим весом, а среди них набор, старший с точки зрения лексикографического порядка. Соответствующий этому набору моном будет входить в $f_{x^1} + \dots + f_{x^h}$, а все остальные мономы будут иметь меньшую длину или меньший лексикографический порядок, значит, сумма $f_{x^1} + \dots + f_{x^h}$ не равна тождественно нулю.

Покажем, что для любого $x = (x_1, \dots, x_n) \in \overline{S_{a_1, \dots, a_q}(k)}$ соответствующая f_x принадлежит $B_k(f)$. Если набор x соответствует п. 1, то это следует из определения f_x для таких наборов. В случае, когда x соответствует п. 2, произведение f на f_x тождественно равно нулю. В случае, когда x соответствует п. 3, произведение f на f_x имеет степень не больше k , так как в противном случае $x \in S_{a_1, \dots, a_q}(k)$. Пусть x соответствует п. 4, тогда представим f как сумму двух функций: $f = f_1 + f_2$, где в f_1 входят мономы с номерами t, b_1, \dots, b_u из записи f , а в f_2 — все остальные. Несложно проверить, что произведение f_2 на f_x тождественно равно нулю, а произведение f_1 на f_x равно f_x , так как f_1 входит как один из сомножителей (последний) в f_x . С учётом того, что $\deg(f_x) = wt(x)$, из вышесказанного следует, что для любого $x = (x_1, \dots, x_n) \in \overline{S_{a_1, \dots, a_q}(k)}$ соответствующая f_x принадлежит $B_k(f)$.

Значит,

$$\dim(B_k(f)) \geq |\overline{S_{a_1, \dots, a_q}(k)}| = \sum_{i=0}^k \binom{n}{i} - |S_{a_1, \dots, a_q}(k)|.$$

Утверждение 8 доказано.

Утверждения 7 и 8 можно объединить в теорему.

Теорема 2. Пусть любые два монома, входящие в полиномиальную запись функции $f(x_1, \dots, x_n)$, не содержат общих переменных. Пусть q — число мономов в полиноме функции, а $a_1 \geq a_2 \geq \dots \geq a_q$ — длины этих

мономов. Тогда

$$\dim(B_k(f)) = \sum_{i=0}^k \binom{n}{i} - |S_{a_1, \dots, a_q}(k)|.$$

Для довольно широкого класса функций мы свели проблему вычисления размерности пространства $B_k(f)$ к несложному комбинаторному подсчёту.

4. Точное соотношение между алгебраической иммунностью и нелинейностью второго порядка

Замечание. Везде ниже биномиальный коэффициент $\binom{n}{m}$ равен нулю, если n или m меньше нуля.

Утверждение 9. Пусть $f(x_1, \dots, x_n) = x_1x_2 + x_3x_4 + \dots + x_{2q-1}x_{2q}$. Тогда

$$\dim(B_k(f)) = \sum_{i=0}^k \binom{n}{i} - \sum_{i=0}^{q-1} 2^i \binom{n-2i-1}{k-i}.$$

ДОКАЗАТЕЛЬСТВО. Множество $S_{a_1, \dots, a_q}(k)$ содержит $\binom{n-2}{k}$ наборов веса k и $\binom{n-2}{k-1}$ — веса $k-1$, равных нулю в первых двух компонентах. В сумме получаем $\binom{n-1}{k}$ наборов.

Множество $S_{a_1, \dots, a_q}(k)$ содержит $2\binom{n-4}{k-1}$ наборов веса k и $2\binom{n-4}{k-2}$ — веса $k-1$, равных нулю во второй паре компонент и единице в одной из первых двух компонент. В сумме получаем $2\binom{n-3}{k-1}$ наборов.

Множество $S_{a_1, \dots, a_q}(k)$ содержит $2^{t-1}\binom{n-2t}{k-t+1}$ наборов веса k и $2^{t-1}\binom{n-2t}{k-t}$ — веса $k-1$, равных нулю в t -й паре компонент и единице в одной из двух компонент каждой предыдущей пары переменных. В сумме получаем $2^{t-1}\binom{n-2t+1}{k-t+1}$ наборов.

Таким образом, мы исчерпываем все наборы из $S_{a_1, \dots, a_q}(k)$ и получаем, что их общее число равно

$$\begin{aligned} \binom{n-1}{k} + 2\binom{n-3}{k-1} + 4\binom{n-5}{k-2} + \dots + 2^{q-1}\binom{n-2q+1}{k-q+1} \\ = \sum_{i=0}^{q-1} 2^i \binom{n-2i-1}{k-i}. \end{aligned}$$

Из теоремы 2 получаем требуемое утверждение.

Аналогично доказывается следующее

Утверждение 10. Пусть

$$f(x_1, \dots, x_n) = x_1x_2 + x_3x_4 + \dots + x_{2q-1}x_{2q} + x_{2q+1}.$$

Тогда

$$\dim(B_k(f)) = \sum_{i=0}^k \binom{n}{i} - \sum_{i=0}^q 2^i \binom{n-2i-1}{k-i}.$$

Теорема 3. Пусть $f(x_1, \dots, x_n)$ имеет $AI(f) = k$. Тогда

$$nl_2(f) \geq \sum_{i=0}^{k-1} \binom{n}{i} - \sum_{i=0}^{k-1} 2^i \binom{n-2i-1}{k-1-i}.$$

Кроме того, при $k \leq \lceil \frac{n}{2} \rceil$ существует функция f_0 , $AI(f_0) = k$, для которой

$$nl_2(f_0) = \sum_{i=0}^{k-1} \binom{n}{i} - \sum_{i=0}^{k-1} 2^i \binom{n-2i-1}{k-1-i}.$$

ДОКАЗАТЕЛЬСТВО. Известно (см., например, [7]), что функция степени не выше 2 приводится аффинными преобразованиями либо к виду из утверждения 9, либо к виду из утверждения 10. Тогда из этих утверждений и теоремы 1 получаем утверждение теоремы 3.

Т а б л и ц а

Нижняя оценка на $nl_2(f)$ из теоремы 3 и неравенства (4) [2, 8].

n	5,6	7	8	9	9	10	10	11	11	11
$AI(f)$	3	4	4	4	5	4	5	4	5	6
Оценка из теоремы 3	2	16	18	20	90	22	110	24	132	440
Оценка (4)	2	14	16	18	74	20	92	22	112	352

12	12	12	13	13	13	13	14	14	14	14	15	15
4	5	6	4	5	6	7	4	5	6	7	4	5
26	156	572	28	182	728	2004	30	210	910	2732	32	240
24	134	464	26	158	598	1588	28	184	756	2186	30	212

15	15	15	16	16	16	16	16	17	17	17	17
6	7	8	4	5	6	7	8	4	5	6	7
1120	3642	8768	34	272	1360	4762	12410	36	306	1632	6122
940	2942	6996	32	242	1152	3882	9888	32	274	1394	5034

17	17	18	18	18	18	18	18
8	9	4	5	6	7	8	9
17172	37434	38	342	1938	7754	23294	54606
13770	29786	36	308	1668	64282	18804	43556

Автор выражает глубокую благодарность Ю. В. Таранникову за внимание к работе и ценные советы.

ЛИТЕРАТУРА

1. **Лобанов М. С.** Точное соотношение между нелинейностью и алгебраической иммунностью // Дискрет. математика. — 2006. — Т. 18, вып. 3. — С. 152–159.
2. **Лобанов М. С.** Оценка нелинейности высоких порядков булевой функции через значение её алгебраической иммунности // Материалы VI молодежной научной школы по дискретной математике и её приложениям (Москва, апрель 2007). Часть 2. — М.: Ин-т прикладной математики РАН, 2007. — С. 11–16.
3. **Canteaut A.** Open problems related to algebraic attacks on stream ciphers // International workshop on coding and cryptography (WCC 2005) (Bergen, March 2005). — Berlin: Springer, 2006. — P. 1–11. (Lect. Notes in Comp. Sci.; Vol. 3969).
4. **Carlet C.** On the higher order nonlinearities of algebraic immune functions // CRYPTO 2006. — Berlin, Heidelberg: Springer, 2006. — P. 584–601. (Lect. Notes in Comp. Sci.; Vol. 4117).
5. **Courtois N., Meier W.** Algebraic attacks on stream ciphers with linear feedback // Advances in cryptology, EUROCRYPT 2003. — Berlin, Heidelberg: Springer Verl., 2003. — P. 345–359. — (Lect. Notes in Comp. Sci.; Vol. 2656).
6. **Dalai D. K., Gupta K. C., Maitra S.** Results on algebraic immunity for cryptographically significant boolean functions // Indocrypt 2004 (Chennai, India, December 20–22, 2004). — Berlin, Heidelberg: Springer Verl., 2004. — P. 92–106. (Lect. Notes in Comp. Sci.; Vol. 3348).
7. **Meier W., Pasalic E., Carlet C.** Algebraic attacks and decomposition of Boolean functions // In Advances in Cryptology, EUROCRYPT 2004. — Berlin, Heidelberg: Springer Verl., 2004. — P. 474–491. (Lect. Notes in Comp. Sci.; Vol. 3027).
8. **Mesnager S.** Improving the lower bound on the higher order nonlinearity of Boolean functions with prescribed algebraic immunity // Cryptology ePrint archive(<http://eprint.iacr.org/>), Report 2007/117.
9. **McWilliams F. J., Sloane N. J. A.** The theory of error correcting codes. — New York: North-Holland, 1977. — 760 p.

Лобанов Михаил Сергеевич,
e-mail: misha_msu@mail.ru

Статья поступила
7 апреля 2008 г.