Новая нижняя оценка нелинейности третьего и выше порядков через значение алгебраической иммунности

М. С. Лобанов

В ряде работ изучается взаимосвязь таких важных, с точки зрения теоретической криптографии, свойств булевых функций как нелинейности различных порядков (расстояние функции до полиномов степени не выше фиксированной) и алгебраическая иммунность. Одним из основных направлений исследований является вопрос получения нижних оценок на нелинейность фиксированного порядка через значение алгебраической иммунности функции. В частности, были получены точные оценки на нелинейности первого и второго порядков. В данной работе мы докажем новую оценку на нелинейность произвольного порядка через значение алгебраической иммунности, более сильную чем предыдущие аналогичные результаты разных авторов.

Ключевые слова: булева функция, алгебраическая иммунность, степень булевой функции, нелинейность, нелинейность высокого порядка, код Риде-Маллера.

1. Введение

Алгебраическая иммунность — это способность противостоять разного рода алгебраическим атакам на регистры сдвига с линейной обратной связью (linear feedback shift registers, LFSR). Эти атаки впервые были предложены в [14]. Они раскрывают секретный ключ путем решения системы уравнений, зависящих от многих переменных. Данные системы уравнений описывают соотношения между битами ключа/состояния и выходными битами f (комбинирующей функции для LFSR). Если найдено такое соотношение низкой степени, алгебраические атаки очень эффективны ([16]). В [14] показано, что указанные соотношения низкой степени и, соответственно, успешные алгебраические атаки существуют для некоторых хорошо

известных шифров, которые иммунны по отношению ко всем другим известным атакам. В [26] авторы сводят эти три вида к двум и вводят новый термин — алгебраическая иммунность. Авторы доказывают, что если алгебраическая иммунность достаточно высока, то алгебраическим атакам можно успешно противостоять.

Ранее важными критериями для комбинирующих функций в LFSR признавались высокая алгебраическая степень, высокий порядок корреляционной иммунности (устойчивости) и большое расстояние до множества аффинных функций (высокая нелинейность), чтобы успешно противостоять атакам Берлекэмпа-Мэсси и различным типам корреляционных и линейных атак [23, 9], а также [15, 21, 22, 24, 25, 29] достаточно большое расстояние до полиномов невысоких степеней (нелинейность r-ых порядков).

Разные критерии на булевы функции могут конфликтовать друг с другом. В то же время функция в LFSR, чтобы схема шифрования могла успешно противостоять существующим атакам, должна удовлетворять им всем. Из-за этого возникает необходимость изучения взаимосвязи этих свойств булевых функций.

Настоящая работа посвящена проблеме оценки снизу нелинейности r-го порядка функции через значение ее алгебраической иммунности.

Получение таких оценок дает не только информацию о взаимосвязи этих двух свойств, но важно еще и по следующей причине. Если вопросы, связанные с нелинейностью $nl(f) = nl_1(f)$, достаточно хорошо изучены и существует аппарат коэффициентов Уолша, который позволяет ее вычислять, то результатов, связанных с нелинейностью более высоких порядков ($nl_r(f)$ при $r \geqslant 2$), известно гораздо меньше. Стоит упомянуть верхнюю оценку из [12], которая имеет асимптотический вид. Доказана также достаточно сильная нижняя оценка [13] на максимально возможное значение нелинейности r-го порядка для булевых функций, которая, правда, тоже носит асимптотический характер и доказана мощностным методом, а поэтому ничего не дает для оценки нелинейности r-го порядка при $r > 1$ для конкретных функций.

В свете выше изложенного, получение как можно более сильных нижних оценок нелинейности r-го порядка через значение алгебраической иммунности приобретает особую важность. Отметим, что в [4, 5, 26, 18] был предложен целый ряд алгоритмов подсчета алгебраической иммунности, а в [7, 8, 10, 19] построено несколько се-

мейств функций, имеющих максимально возможную алгебраическую иммунность $\lceil \frac{n}{2} \rceil$.

В работе [1] была предложена точная нижняя оценка на нелинейность (первого порядка) через значение алгебраической иммунности функции. Нижние оценки нелинейности r-того порядка через алгебраическую иммунность были предложены в [3, 11, 20, 27]. Наиболее сильной из них является неравенство (4).

В данной работе нами будет доказана новая нижняя оценка на нелинейность r-го порядка через значение алгебраической иммунности. Оставшаяся часть работы организована следующим образом.

В части 2 мы приведем необходимые определения и некоторые ранее известные результаты. В части 3 докажем новую оценку на нелинейность r-го порядка.

Работа выполнена при поддержке РФФИ (проект 11–01–00508).

2. Основные определения и известные ранее 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 ее полиноме (количество переменных в этом слагаемом).

Определение 1. *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 [14, 26], что для любой f над F_2^n выполнено $AI(f) \leqslant \lceil \frac{n}{2} \rceil$.

В [17] доказано, что доля уравновешенных функций f от n переменных, для которых выполнены неравенства $\frac{n}{2} - \sqrt{\frac{n}{2} \ln n} \leqslant AI(f) \leqslant \frac{n+1}{2}$, стремится к единице при $n \to \infty$. То есть алгебраическая иммунность почти всех уравновешенных булевых функций от n переменных имеет асимптотический порядок $n/2$ — максимально возможный.

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

Определение 2. Нелинейностью r-го порядка $nl_r(f)$ булевой функции f над F_2^n называется $\min\limits_{\deg(l) \leqslant r} d(f, l)$.

Отметим, что на языке теории кодирования нелинейность r-го порядка функции — это расстояние функции до $RM(r,n)$ — кода Рида-Маллера r-го порядка.

Аффинным преобразованием назовем подстановку вида

$$g : (x^{(1)}, \ldots, x^{(n)})^\top \mapsto \left(\bigoplus_{j=1}^{n} a_{1j}x^{(j)} \oplus a^{(1)}, \ldots, \bigoplus_{j=1}^{n} a_{nj}x^{(j)} \oplus a^{(n)} \right)^\top,$$

где $\binom{1\ldots n}{j_1\ldots j_n}$ — подстановка на множестве $\{1,\ldots,n\}$, $A = (a_{ij})$ — обратимая $n \times n$-матрица, $a_{ij} \in F_2$, $i, j = 1, 2, \ldots, n$ и $a = (a^{(1)}, \ldots, a^{(n)})^\top \in F_2^n$.

Заметим, что при невырожденном аффинном преобразовании булевой функции такие ее свойства как степень, нелинейность r-го порядка, алгебраическая иммунность сохраняются.

В дальнейшем нам также понадобится аффинная классификация квадратичных (степень функции меньше или равна 2) булевых функций [6, 28]: *Пусть $f(x_1, \ldots, x_n)$ — квадратичная функция. Тогда существует такое аффинное преобразование, что f будет приведена к виду*

$$x_1x_2 + \ldots + x_{2i-1}x_{2i} + c,$$

где $c \in \{0, 1\}$, или к виду

$$x_1x_2 + \ldots + x_{2i-1}x_{2i} + x_{2i+1}.$$

В работе [20] был доказан результат, эквивалентный следующей оценке на нелинейность r-ого порядка:

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

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

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

И там же [1] для всех допустимых значений алгебраической иммунности автором были построены функции, на которых достигается равенство в приведенной оценке.

Еще позднее К. Карле в [11] обобщил доказанную автором оценку (2) на случай других r:

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

Отметим, что ни одна из двух приведенных выше оценок (1) и (3) для нелинейности r-ого порядка не влечет другую.

В работах [27] и [3] была доказана следующая оценка

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

более сильная, чем (1) и (3).

В [11] была доказана оценка, которая в некоторых случаях при значениях r, близких к $AI(f)$, дает оценку на $nl_r(f)$ более сильную, чем неравенство (4). Однако для остальных случаев оценка (4) долгое время оставалась лучшей из известных.

В работе [2] была доказана точная оценка для нелинейности второго порядка:

$$nl_2(f) \geqslant \sum_{i=0}^{AI(f)-1} \binom{n}{i} - \sum_{i=0}^{AI(f)-1} 2^i \binom{n-2i-1}{AI(f)-1-i},$$

которая достигается при всех допустимых значениях параметров.

В [2] проблема получения как можно более сильных нижних оценок нелинейности r-го порядка через значение алгебраической иммунности функции полностью сводится к задаче определения размерности некоторых подпространств $B_k(h) = \{g(x_1, \ldots, x_n) | \deg(g) \leqslant k, \deg(gh) \leqslant k\}$.

Теорема 1. *[2] Пусть $f(x_1, \ldots, x_n)$ имеет $AI(f) = k$, тогда*

$$nl_r(f) \geqslant \min_{deg(g) \leqslant r} dim(B_{k-1}(g)). \tag{5}$$

Кроме того, при $k \leqslant \lceil \frac{n}{2} \rceil$ и $\min\limits_{deg(g) \leqslant r} dim(B_{k-1}(g)) > 0$ существует функция f_0, $AI(f_0) = k$, для которой

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

3. Новая нижняя оценка нелинейности третьего и выше порядка через значение алгебраической иммунности

Утверждение 1. *Пусть $f(x_1, \ldots, x_n)$ булева функция, $deg(f) = k > 1$. Тогда аффинными преобразованиями ее можно привести к многочлену, который будет содержать моном $x_1 x_2 \ldots x_k$ и любой другой моном которого будет содержать не более чем $k-2$ из переменных $x_1, x_2, \ldots, x_k$.*

Доказательство. Доказательство проведем по индукции. Для $k = 2$ утверждение следует из аффинной классификации квадратичных булевых функций. Предположим, что для $deg(f) = k$ утверждение доказано, докажем его для $deg(f) = k+1$.

В силу предположения индукции можем считать, что функция f аффинными преобразованиями может быть приведена к виду:

$$x_{k+1}(x_1 \ldots x_k + g_1(x_1, \ldots, x_k, x_{k+2}, \ldots, x_n)) + \\ + g_2(x_1, \ldots, x_k, x_{k+2}, \ldots, x_n),$$

где $deg(g_1) \leqslant k, deg(g_2) \leqslant k+1$, и любой моном функции g_1 содержит не более $k-2$ из переменных $x_1, x_2, \ldots, x_k$.

Выберем среди мономов функции g_2 те, которые содержат одновременно переменные $x_1, x_2, \ldots, x_k$ и перегруппируем слагаемые:

$$x_1 \ldots x_k(x_{k+1} + x_{j_1} + \ldots + x_{j_m} + a_0) + \\ + x_{k+1}\tilde{g}_1(x_1, \ldots, x_k, x_{k+2}, \ldots, x_n) + \tilde{g}_2(x_1, \ldots, x_k, x_{k+2}, \ldots, x_n),$$

где $k+1 < j_i \leqslant n$ для $i = 1, \ldots, m$, а $deg(\tilde{g}_1) \leqslant k, deg(\tilde{g}_2) \leqslant k+1$ и любой моном функции $\tilde{g}_1$ содержит не более $k-2$, а любой моном функции $\tilde{g}_2$ не более $k-1$ из переменных $x_1, x_2, \ldots, x_k$.

Следовательно, аффинными преобразованиями функция f приводима к виду:

$$x_1 \ldots x_{k+1} + (x_{k+1} + x_{j_1} + \ldots + x_{j_m} + a_0)\hat{g}_1(x_1, \ldots, x_k, x_{k+2}, \ldots, x_n) + \\ + \hat{g}_2(x_1, \ldots, x_k, x_{k+2}, \ldots, x_n),$$

где $k+1 < j_i \leqslant n$ для $i = 1, \ldots, m$, а $deg(\hat{g}_1) \leqslant k, deg(\hat{g}_2) \leqslant k+1$ и любой моном функции $\hat{g}_1$ содержит не более $k-2$, а любой моном функции $\hat{g}_2$ не более $k-1$ из переменных $x_1, x_2, \ldots, x_k$.

Несложно убедится, что из этого следует утверждение.

Утверждение 2. *Пусть* $deg(f) = r \geqslant 2$ *и* $k \leqslant \lceil \frac{n}{2} \rceil$, *тогда*

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

Доказательство. Можно считать, что в полином функции f входит моном $x_1 \dots x_r$. С учетом утверждения 1 функция f может быть приведена к виду:

$$x_1 \dots x_r + g(x_1, \dots, x_n),$$

где любой моном функции g содержит не более чем $r-2$ из переменных $x_1, \dots, x_r$.

Отдельно рассмотрим случай, когда функция g равна тождественно константе. В этом случае

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

Действительно, в этом случае функция f удовлетворяет условию теоремы 2 и имеет место равенство:

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

Для функции f множество $S_r(k-1)$ имеет вид $S_r(k-1) = \{x = (x_1, \dots, x_n) | k - r \leqslant wt(x) \leqslant k-1, x_i = 0 \,\text{при}\, i = 1, \dots, r\}$ и имеет мощность $\sum_{i=k-r}^{k-1} \binom{n-r}{i}$. При рассмотрении случая $g = const$ осталось убедиться, что имеет место следующее неравенство:

$$\sum_{i=0}^{k-1} \binom{n}{i} - \sum_{i=k-r}^{k-1} \binom{n-r}{i} \geqslant$$
$$\geqslant \sum_{i=0}^{k-r-1} \binom{n}{i} + \sum_{i=k-2r}^{k-r-1} \binom{n-r}{i} + 2 \sum_{i=k-2r-1}^{k-r-2} \binom{n-r-2}{i}.$$

Или:

$$\sum_{i=k-r}^{k-1} \binom{n}{i} \geqslant \sum_{i=k-2r}^{k-1} \binom{n-r}{i} + 2 \sum_{i=k-2r-1}^{k-r-2} \binom{n-r-2}{i}.$$

Применяя известные тождества $\binom{n}{k} = \sum_{j=0}^{k} \binom{r}{k-j}\binom{n-r}{j}$ и $\binom{n}{k} = \binom{n-1}{k} + \binom{n-1}{k-1}$ и учитывая $r \geqslant 3$, получаем требуемое неравенство:

$$\sum_{i=k-r}^{k-1} \binom{n}{i} = \sum_{i=k-r}^{k-1} \sum_{j=i-r}^{i} \binom{r}{i-j}\binom{n-r}{j} =$$

$$= \sum_{j=k-2r}^{k-1} \sum_{i=k-r-j}^{k-j-1} \binom{r}{i}\binom{n-r}{j} \geqslant$$

$$\geqslant \sum_{i=k-2r}^{k-1} \binom{n-r}{i} + 2 \sum_{i=k-2r+1}^{k-r-2} \binom{n-r}{i} \geqslant$$

$$\geqslant \sum_{i=k-2r}^{k-1} \binom{n-r}{i} + 2 \sum_{i=k-2r-1}^{k-r-2} \binom{n-r-2}{i}.$$

Далее считаем, что функция g не равна тождественно константе.

Среди мономов функции g выберем мономы, которые содержат максимальное число переменных из $x_1, \ldots, x_r$. Среди них выберем какой-нибудь моном максимальной длины. Можем считать, что функция f имеет вид:

$$x_1 \ldots x_r + x_{r-m+1} \ldots x_{r+t} + \tilde{g}(x_1, \ldots, x_n),$$

где $r - m \geqslant 2$, $m + t \leqslant r$, а для функции $\tilde{g}$ верно следующее:

1) $deg(\tilde{g}) \leqslant r$,
2) многочлен $\tilde{g}$ не содержит мономов $x_1 \ldots x_r$ и $x_{r-m+1} \ldots x_{r+t}$,
3) любой моном функции $\tilde{g}$ содержит не более чем m из переменных $x_1, \ldots, x_r$,
4) длина монома функции $\tilde{g}$ не превосходит $m+t$, если он содержит ровно m из переменных $x_1, \ldots, x_r$.

Определим два множества мономов:

$$H_1 = \{x_{j_1} \ldots x_{j_q} | k - 2r \leqslant q \leqslant k - r - 1 \text{ и } r + 1 \leqslant j_i \leqslant n\},$$
$$H_2 = \{x_{c_1} \ldots x_{c_l} x_{j_1} \ldots x_{j_q} | 1 \leqslant l \leqslant r - m - 1,$$
$$k - r - (m + t) - l \leqslant q \leqslant k - r - l - 1,$$
$$1 \leqslant c_i \leqslant r - m, r + t + 1 \leqslant j_i \leqslant n\}.$$

Рассмотрим функции вида:

$$h(x_1, \ldots, x_n) = h_1(x_1, \ldots, x_n) + h_2(x_1, \ldots, x_n) f(x_1, \ldots, x_n),$$

где $deg(h_1) \leqslant k - r - 1$, а h_2 содержит только мономы из множеств H_1 и H_2.

Лемма 1. *Если h_2 не равна тождественно нулю, тогда $deg(h_2 f) \geqslant k - r$.*

Доказательство. Пусть среди мономов h_2 есть мономы из H_2. Тогда выберем среди них какой-нибудь $x_{c_1} \ldots x_{c_l} x_{j_1} \ldots x_{j_q} \in H_2$ с максимальным числом переменных. Тогда в полином функции $h_2 f$ входит моном $x_{c_1} \ldots x_{c_l} x_{r-m+1} \ldots x_{r+t} x_{j_1} \ldots x_{j_q}$. Докажем это, рассмотрев все случаи, как этот моном может возникнуть в произведении функций h_2 и f. Функция h_2 содержит только мономы из H_1 и H_2, а функция f мономы $x_1 \ldots x_r$, $x_{r-m+1} \ldots x_{r+t}$ и мономы функции $\tilde{g}$, значит, возможны только следующие 5 вариантов:

случай 1) Моном $x_{c_1} \ldots x_{c_l} x_{r-m+1} \ldots x_{r+t} x_{j_1} \ldots x_{j_q}$ появляется как произведение монома из H_1 или H_2 на $x_1 \ldots x_r$. Такого быть не может, так как произведение этих мономов содержит все переменные $x_1, \ldots, x_{r-m}$, а моном $x_{c_1} \ldots x_{c_l} x_{r-m+1} \ldots x_{r+t} x_{j_1} \ldots x_{j_q}$ какую-то из них не содержит в силу определения множества H_2.

случай 2) Моном $x_{c_1} \ldots x_{c_l} x_{r-m+1} \ldots x_{r+t} x_{j_1} \ldots x_{j_q}$ появляется как произведение монома из H_1 на $x_{r-m+1} \ldots x_{r+t}$. Такого быть не может, так как произведение этих мономов не содержит ни одной переменной из $x_1, \ldots, x_{r-m}$, моном $x_{c_1} \ldots x_{c_l} x_{r-m+1} \ldots x_{r+t} x_{j_1} \ldots x_{j_q}$ хотя бы одну из них содержит в силу определения множества H_2.

случай 3) Моном $x_{c_1} \ldots x_{c_l} x_{r-m+1} \ldots x_{r+t} x_{j_1} \ldots x_{j_q}$ появляется как произведение монома из H_2 на $x_{r-m+1} \ldots x_{r+t}$. Действительно, моном $x_{c_1} \ldots x_{c_l} x_{r-m+1} \ldots x_{r+t} x_{j_1} \ldots x_{j_q}$ появляется только единственный раз как произведение $x_{r-m+1} \ldots x_{r+t}$ на $x_{c_1} \ldots x_{c_l} x_{j_1} \ldots x_{j_q}$, который, как мы предположили, является моном функции h_2.

случай 4) Моном $x_{c_1} \ldots x_{c_l} x_{r-m+1} \ldots x_{r+t} x_{j_1} \ldots x_{j_q}$ появляется как произведение монома из H_1 на какой-то моном функции $\tilde{g}$. Этот моном функции $\tilde{g}$ должен содержать тогда переменные $x_{c_1}, \ldots, x_{c_l}$ и переменные $x_{r-m+1}, \ldots, x_r$. Значит, он содержит более чем m из первых r переменных, что противоречит пункту 3 описания функции $\tilde{g}$, то есть этот случай тоже невозможен.

случай 5) Моном $x_{c_1} \ldots x_{c_l} x_{r-m+1} \ldots x_{r+t} x_{j_1} \ldots x_{j_q}$ появляется как произведение монома из H_2 на какой-то моном функции $\tilde{g}$.

Этот моном функции $\tilde{g}$ должен содержать тогда переменные монома $x_{r-m+1}\dots x_{r+t}$, но этого быть не может, так как в силу пунктов 2 и 4 описания функции $\tilde{g}$ ее многочлен не содержит монома, в который одновременно входят $x_{r-m+1},\dots,x_{r+t}$. Значит, этот случай тоже невозможен.

Получается, что моном $x_{c_1}\dots x_{c_l}x_{r-m+1}\dots x_{r+t}x_{j_1}\dots x_{j_q}$ возникает единственный раз в случае 4, а значит он действительно входит в произведение h_2f и поэтому $\deg(h_2f)\geqslant l+q+m+t\geqslant k-r$, когда h_2 содержит хоть один моном из H_2.

Теперь пусть функция h_2 содержит только мономы из H_1. Выберем среди них один максимальной длины, пусть это будет $x_{i_1}\dots x_{i_d}$, где $i_j>r$ в силу определения H_1. Тогда в полином функции h_2f входит моном $x_1\dots x_rx_{i_1}\dots x_{i_d}$. Докажем это, рассмотрев все случаи как этот моном может возникнуть в произведении функций h_2 и f. Функция h_2 содержит в нашем предположении только мономы из H_1, а функция f мономы $x_1\dots x_r$, $x_{r-m+1}\dots x_{r+t}$ и мономы функции $\tilde{g}$, значит, возможны только следующие 3 варианта:

случай 1) Моном $x_1\dots x_rx_{i_1}\dots x_{i_d}$ появляется как произведение монома из H_1 на $x_1\dots x_r$. Это происходит в единственном случае, когда $x_{i_1}\dots x_{i_d}$ умножается на $x_1\dots x_r$.

случай 2) Моном $x_1\dots x_rx_{i_1}\dots x_{i_d}$ появляется как произведение монома из H_1 на $x_{r-m+1}\dots x_{r+t}$. Это невозможно, так как произведение этих мономов не содержало бы переменных $x_1,\dots,x_{r-m}$.

случай 3) Моном $x_1\dots x_rx_{i_1}\dots x_{i_d}$ появляется как произведение монома из H_1 на какой-то моном функции $\tilde{g}$. Но в силу описания $\tilde{g}$ ее моном содержит не более m из переменных $x_1,\dots,x_r$, моном из H_1 вообще не содержит $x_1,\dots,x_r$, поэтому их произведение никак не может содержать все эти переменные. Значит, этот случай тоже невозможен.

Получается, что моном $x_1\dots x_rx_{i_1}\dots x_{i_d}$ возникает единственный раз в случае 1, а, значит, он действительно входит в произведение h_2f и, следовательно, $\deg(h_2f)\geqslant r+(k-2r)=k-r$. Это завершает доказательство леммы.

Убедимся, что все определенные выше функции $h(x_1,\dots,x_n)$ будут различными. Для этого достаточно показать, что из $h\equiv 0$ следует $h_1\equiv 0$ и $h_2\equiv 0$. Пусть h_2 не равна тождественно нулю, тогда из леммы следует $deg(h_2f)\geqslant k-r$. Но $deg(h_1)<k-r$ и тогда функция h не равна тождественно нулю. Значит, $h\equiv 0$ влечет $h_2\equiv 0$, а это влечет $h_1\equiv 0$.

Теперь проверим, что $h(x_1,\dots,x_n)\in B_{k-1}(f)$. Так как $deg(h_1)\leqslant k-r-1$, то $deg(h_1f)\leqslant k-1$. В силу определения множеств H_1 и H_2, имеем $deg(h_2)\leqslant k-r-1$, поэтому $deg(h_2f)\leqslant k-1$. Из всего этого и того, что $hf=h_1f+h_2f$, получается $deg(h)\leqslant k-1$ и $deg(hf)\leqslant k-1$. Следовательно, $h\in B_{k-1}(f)$.

Заметим, что функции h образуют линейное подпространство в пространстве всех функций. Размерность этого подпространства равна:

$$\sum_{i=0}^{k-r-1}\binom{n}{i}+|H_1|+|H_2|.$$

Вклад $\sum_{i=0}^{k-r-1}\binom{n}{i}$ дают функции h_1, а $|H_1|+|H_2|$ функции h_2. Из определений множеств H_1 и H_2 непосредственно следует:

$$|H_1|=\sum_{i=k-2r}^{k-r-1}\binom{n-r}{i},$$

$$|H_2|=\sum_{i=k-r-(m+t)}^{k-r-1}\left(\binom{n-(m+t)}{i}-\binom{n-r-t}{i}-\binom{n-r-t}{i-r+m}\right).$$

Второе равенство получается из того, что количество мономов длины i, входящих в H_2, равно $\binom{n-(m+t)}{i}-\binom{n-r-t}{i}-\binom{n-r-t}{i-r+m}$.

При $t\geqslant 2$ с учетом $k\leqslant\lceil\frac{n}{2}\rceil$ и $r\geqslant m+t$, получаем:

$$\sum_{i=k-r-(m+t)}^{k-r-1}\left(\binom{n-(m+t)}{i}-\binom{n-r-t}{i}-\binom{n-r-t}{i-r+m}\right)\geqslant$$

$$\geqslant\sum_{i=k-r-(m+t)}^{k-r-1}\left(\binom{n-r-2}{i}+2\sum_{j=i-r+(m+t)-1}^{i-1}\binom{n-r-2}{j}+\right.$$

$$\left.+\binom{n-r-2}{i-r+(m+t)-2}-\binom{n-r-t}{i}-\binom{n-r-t}{i-r+m}\right)\geqslant$$

$$\geqslant\sum_{i=k-r-(m+t)}^{k-r-1}\left(2\sum_{j=i-r+(m+t)-1}^{i-1}\binom{n-r-2}{j}\right)=$$

$$= 2 \sum_{i=k-r-(m+t)}^{k-r-1} \sum_{j=i-r+(m+t)-1}^{i-1} \binom{n-r-2}{j} \geqslant 2 \sum_{i=k-2r-1}^{k-r-2} \binom{n-r-2}{i} \geqslant$$

$$\geqslant 2 \sum_{i=k-2r-1}^{k-r-2} \binom{n-r-2}{i}.$$

При $t = 0$ и $t = 1$, учитывая $m \leqslant r-2$:

$$\sum_{i=k-r-(m+t)}^{k-r-1} \left(\binom{n-(m+t)}{i} - \binom{n-r-t}{i} - \binom{n-r-t}{i-r+m} \right) \geqslant$$

$$\geqslant \sum_{i=k-r-(m+t)}^{k-r-1} \left(\binom{n-r-t}{i} + 2 \sum_{j=i-r+m+1}^{i-1} \binom{n-r-t}{j} + \binom{n-r-t}{i-r+m} - \right.$$

$$\left. - \binom{n-r-t}{i} - \binom{n-r-t}{i-r+m} \right) = 2 \sum_{i=k-r-(m+t)}^{k-r-1} \sum_{j=i-r+m+1}^{i-1} \binom{n-r-t}{j} \geqslant$$

$$\geqslant 2 \sum_{i=k-2r-t+1}^{k-r-2} \binom{n-r-t}{i} \geqslant 2 \sum_{i=k-2r-1}^{k-r-2} \binom{n-r-2}{i}.$$

Заметим, что при $m = r-2$, $t = 2$ достигается равенство:

$$\sum_{i=k-2r}^{k-r-1} \binom{n-r}{i} - \sum_{i=k-2r}^{k-r-1} \binom{n-r-2}{i} - \sum_{i=k-2r}^{k-r-1} \binom{n-r-2}{i-2} =$$

$$= 2 \sum_{i=k-2r-1}^{k-r-2} \binom{n-r-2}{i}.$$

Из того, что функции типа h являются подпространством в $B_{k-1}(f)$, и оценки, полученной на размерность этого подпространства, будет следовать утверждение.

Как простое следствие утверждения 2 и неравенства (5) из теоремы 1 получаем новую оценку для нелинейности третьего и выше порядков.

Теорема 2. *Пусть $AI(g) = k$, тогда*

$$nl_r(g) \geqslant \sum_{i=0}^{k-r-1} \binom{n}{i} + \sum_{i=k-2r}^{k-r-1} \binom{n-r}{i} + 2 \sum_{i=k-2r-1}^{k-r-2} \binom{n-r-2}{i}. \quad (6)$$

Легко увидеть, что оценка (6) из теоремы 2 сильнее чем оценка (4).

Приведем таблицу сравнения оценок (6) и (4) для функций с относительно небольшим числом переменных при $r = 3$ и $r = 4$. Мы будем рассматривать случай, когда функция имеет нечетное количество слагаемых и максимально возможную алгебраическую имунность.

r	n	$AI(f)$	оценка(4)	оценка (6)
3	9	5	17	19
3	11	6	104	118
3	13	7	553	627
3	15	8	2722	3072
3	17	9	12769	14331
3	19	10	57992	64726
3	21	11	257396	285788
3	23	12	1123220	1241132
3	25	13	4838490	5322990
3	27	14	20633040	22608508
3	29	15	87279291	95287753
3	31	16	366785074	399109964
3	33	17	1533077041	1663115131
4	11	6	20	22
4	13	7	138	154
4	15	8	808	900
4	17	9	4306	4770
4	19	10	21592	23776
4	21	11	1037846	113640
4	23	12	483680	526928
4	25	13	2202164	2388212
4	27	14	9846132	10634898
4	29	15	43393566	46700782
4	31	16	189026584	202774604
4	33	17	815568466	872330626

Список литературы

[1] Лобанов М. С. Точное соотношение между нелинейностью и алгебраической иммунностью // Дискретная математика. — 2006. — Т. 18, вып. 3. — С. 152–159.

[2] Лобанов М. С. Точные соотношения между нелинейностью и алгебраической иммунностью // Дискретный анализ и исследование операций. — 2008. — Т. 15, вып. 5. — С. 47–60.

[3] Лобанов М. С. Оценка нелинейности высоких порядков булевой функции через значение ее алгебраической иммунности // Материалы VI молодежной научной школы по дискретной математике и ее приложениям (Москва, 16–21 апреля, 2007). Часть 2. — М.: Институт прикладной математики РАН, 2007. — С. 11–16.

[4] Баев В. В. Некоторые нижние оценки на алгебраическую иммунность функций, заданных своими след-формами // Пробл. передачи информ. — 2008. — Т. 44, вып. 3. — С. 81–104.

[5] Баев В. В. Усовершенствованный алгоритм поиска аннигиляторов низкой степени для многочлена Жегалкина // Дискретная математика. — 2007. — Т. 19, вып. 4. — С. 132–138.

[6] Логачев О. А., Сальников А. А., Ященко В. В. Булевы функции в теории кодирования и криптологии. — М.: МЦНМО, 2004.

[7] Armknecht F., Krause M. Constructing single- and multi-output boolean functions with maximal algebraic immunity // International conference on automata, language and programing 2006. — LNCS 4052. Springer, 2006. — Part II. — P. 180–191.

[8] Braeken A., Preneel B. On the algebraic immunity of symmetric boolean functions // Indocrypt 2005. — LNCS 3797. Springer, 2005. — P. 35–48.

[9] Canteaut A., Trabbia M. Improved fast correlation attacks using Parity-check equations of weight 4 and 5 // Eurocrypt 2000 (Bruges, Belgium, May 14–18, 2000). — Springer-Verlag, 2000. — P. 573–588. (Lecture Notes in Computer Science. Vol. 1807).

[10] Carlet C. A method of construction of balanced functions with optimum algebraic immunity // Cryptology ePrint archive. [http://eprint.iacr.org/2006/149]

[11] Carlet C. On the higher order nonlinearities of algebraic immune functions // CRYPTO 2006. — Berlin/Heidelberg: Springer, 2006. — P. 584–601. (Lecture Notes in Computer Science. Vol. 4117).

[12] Carlet C., Mesnager S. Improving the upper bounds on the covering radii of binary Reed-Muller codes // IEEE Transactions on Information Theory. — 2006.

[13] Cohen G., Honkala I., Litsyn S., Lobstein A. Covering codes. — North-Holland, 1997.

[14] 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. (Lecture Notes in Computer Science. Vol. 2656).

[15] Courtois N. Higher order corralation attacks, XL algorithm and cryptanalysis of Toyocrypt // Proceedings of ICISC 2002. — LNCS 2587. — P. 182–199.

[16] Courtois N. Fast algebraic attacks on stream ciphers with linear feedback // Advanced in Cryptology: Crypto 2003 (Santa Barbara, California, USA, August 17–21, 2003). — Springer-Verlag, 2003. — P. 176–194. (Lecture Notes in Computer Science. Vol. 2729).

[17] Didier F. A new bound on the block error probability after decoding over the erasure channel // IEEE Trans. on Information Theory. — Vol. IT–52. N 10. — 2006.

[18] Didier F., Tillich J. P. Computing the algebraic immunity efficiently // Fast softwware encryption. LNCS 4047. — 2006. — P. 359–374.

[19] Dalai D. K., Maitra S. Balanced Boolean functions with (more than) maximum algebraic immunity // Cryptology ePrint archive. [http://eprint.iacr.org/2006/434]

[20] 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.

[21] Golic J. Fast low order approximation of cryptographic funtions // Proceedings of EUROCRYPT'96. — LNCS 1070. — 1996. — P. 268–282.

[22] Iwata T., Kurosawa K. Probabilistic higher order differential attack and higher order bent function // Proceedings of ASIACRYPT'99. — LNCS 1716. — 1999. — P. 62–74.

[23] Johansson T., Jönsson F. Fast correlation attacks through reconstruction of linear polynomials // Advanced in Cryptology: Crypto 2000 (Santa Barbara, California, USA, August 20–24, 2000). — Springer-Verlag, 2000. — P. 300–315. (Lecture Notes in Computer Science. Vol. 1880)

[24] Knudsen L. R., Robshaw M. J. B. Non-linear approximations in linear cryptanalysis // Proceedings of EUROCRYPT'96. — LNCS 1070. — 1996. — P. 224–236.

[25] Maurer U. M. New approaches to the design of self-synchronizing stream ciphers // Proceedings of EUROCRYPT'91. — LNCS 547. — 1991. — P. 458–471.

[26] Meier W., Pasalic E., Carlet C. Algebraic attacks and decomposition of Boolean functions // Advances in Cryptology — EUROCRYPT 2004. — Berlin/Heidelberg: Springer Verl., 2004. — P. 474–491. (Lecture Notes in Computer Science. Vol. 3027).

[27] Mesnager S. Improving the lower bound on the higher order nonlinearity of Boolean functions with prescribed algebraic immunity. Cryptology ePrint archive. Report 2007/117. [http://eprint.iacr.org/]

[28] McWilliams F. J., Sloane N. J. A. The Theory of Error Correcring Codes. New York: North-Holland, 1977.

[29] W.Millan. Low order approximation of cipher functions // Cryptographic Policy and Algorithms. — LNCS 1029. —1996. — P. 144–155.