Математика и математическое моделирование.
2020. № 6. С. 1–12.

DOI: 10.24108/mathm.0620.0000246

Математика и Математическое моделирование

Сетевое научное издание

http://mathmelpub.ru ISSN 2412-5911

УДК 512.563

Булевы функции, имеющие аффинные аннигиляторы

Зеленецкий А. С.[1,*], **Ключарев П. Г.**[1]

[1]МГТУ им. Н.Э. Баумана, Москва, Россия

[*]Zelenetskiy_alexey@mail.ru

Булева функция g называется аннигилятором булевой функции f, если выполнено тождество $fg \equiv 0$. Аннигиляторы находят свое применение в алгебраическом криптоанализе, а также в некоторых задачах анализа конечных автоматов. В обоих случаях, как правило, требуется найти аннигилятор или аннигиляторы низкой степени для заданной булевой функции. Данная работа посвящена булевым функциям, имеющим аффинные аннигиляторы, а именно: оценке числа таких функций, связи спектра булевой функции с наличием у нее аффинного аннигилятора. Помимо этого, предложен способ анализа булева уравнения с помощью функций, имеющих аффинные аннигиляторы.

Ключевые слова: булева функция; аннигилятор; аффинная функция; линейная функция; преобразование Уолша — Адамара; бент-функция

Представлена в редакцию: 15.01.2021.

Введение

Рассмотрим произвольную систему булевых уравнений от нескольких переменных. При высоких алгебраических степенях исходных уравнений решение такой системы на практике, как правило, невозможно в связи с большой вычислительной сложностью. Однако существуют методы сведения исходной системы уравнений к более простой, которые в некоторых случаях могут помочь найти решение. К таким методам можно отнести линеаризацию, метод частичного опробования и другие.

В работе [1] были рассмотрены некоторые методы решения систем булевых уравнений. Мы остановимся на методе, обозначенном ее авторами как S3. Рассмотрим уравнение $f(x) = b$, где $b \in \{0, 1\}$, а f — булева функция. Пусть g является такой булевой функцией, что fg имеет низкую степень. Функция g называется множителем функции f. В этом случае предлагается заменить функцию f в уравнении на функцию fg, тем самым упростив исходную систему уравнений. В работе [2] были изложены модификации данного метода. В том числе было предложено использование аннигиляторов функции f низкой степени. Под

аннигилятором функции f понимается некоторая функция g такая, что $fg \equiv 0$. Аннигиляторы функции f, которые имеют низкую степень, предлагается применять для упрощения уравнений вида $f(x) = 1$. Домножив правую и левую части этого уравнения на некоторый аннигилятор g, можно свести исходное уравнение к уравнению вида $g(x) = 0$. Также предлагается использовать аннигиляторы инверсии функции f. Если найдутся такие аннигиляторы с низкой степенью, то удастся упростить уравнение вида $f(x) = 0$.

Для осуществления на практике предложенных сценариев необходим алгоритм поиска аннигиляторов или множителей малой степени для произвольной булевой функции. Исследованию таких алгоритмов посвящены такие работы как [3, 4, 5]. Уже в работе [2] появляется понятие порядка алгебраической иммунности булевой функции. Формальное определение данной величины будет дано в следующем разделе. Неформально, порядок алгебраической иммунности булевой функции равен минимальной возможной степени аннигилятора этой функции или ее инверсии. В этой же работе доказано, что порядок алгебраической иммунности любой булевой функции от n переменных ограничен сверху величиной $\lceil \frac{n}{2} \rceil$. В работе [6] была выведена оценка, связывающая минимальную возможную степень аннигилятора булевой функции и ее вес. Было доказано, что если для некоторой булевой функции f от n переменных и некоторого натурального $d \leq n$ выполнено, что $\sum\limits_{k=0}^{d} \binom{n}{k}$ больше веса f, то минимальная возможная степень аннигилятора функции f не превосходит числа d. Серьезные продвижения были сделаны в исследовании взаимосвязи нелинейности r-го порядка некоторой функции f и ее порядка алгебраической иммунности. Как правило, речь идет об ограничении нелинейности r-го порядка функции f снизу некоторой величиной, зависящей от ее порядка алгебраической иммунности. Этим исследованиям посвящены работы [7, 8, 9].

Настоящая работа посвящена исследованию булевых функций с аффинными аннигиляторами. Получены оценки количества таких функций, получена зависимость между спектром булевой функции и наличием у нее аффинного аннигилятора, а также предложена идея модернизации изложенных сценариев анализа систем булевых уравнений.

Данная работа имеет следующую структуру. В разделе 1 представлены основные понятия и определения, необходимые для понимания работы. Раздел 2 посвящен оценке количества булевых функций с аффинными аннигиляторами. В разделе 3 речь идет о связи спектра булевой функции с ее расстоянием до множества функций с аффинными аннигиляторами.

1. Основные понятия и определения

В этом разделе изложены основные определения и известные утверждения [10], которые будут использоваться нами в следующих разделах. Для начала введем следующие обозначения:

- V_n — линейное пространство размерности n над полем $\mathbb{F}_2$;
- $\mathcal{F}_n$ — множество булевых функций от n переменных;
- $\mathcal{A}_n$ — множество аффинных булевых функций от n переменных;

- $\mathcal{L}_n$ — множество линейных булевых функций от n переменных;
- $\mathcal{B}_n$ — множество бент-функций от n переменных;
- $\mathcal{AA}_n$ — множество функций от n переменных, имеющих аффинные аннигиляторы;
- $\mathrm{Ann}(f)$ — пространство аннигиляторов функции f;
- $\|f\|$ — вес булевой функции f(число единиц в ее векторе значений);
- $d(f,g)$ — расстояние по Хеммингу между двоичными векторами f, g;
- (x,y) — скалярное произведение векторов $x,\ y \in V_n$;

Определение 1. Пусть $f \in \mathcal{F}_n$. Функция $g \in \mathcal{F}_n$, такая, что $fg \equiv 0$, называется *аннигилятором* функции f.

Множество всех аннигиляторов функции f будем обозначать $\mathrm{Ann}(f)$, т.е.

$$\mathrm{Ann}(f) = \{g \in \mathcal{F}_n \colon fg \equiv 0\}.$$

Легко видеть, что на всех двоичных наборах, где функция f принимает ненулевое значение, любой ее аннигилятор принимает нулевое значение. Однако на тех наборах, где f обращается в нуль, ее аннигилятор может принимать произвольные значения, поэтому справедливо следующее утверждение:

Утверждение 1. $|\mathrm{Ann}(f)| = 2^{2^n - \|f\|}$.

Более того, нулевая функция, очевидно, аннигилирует любую функцию и, если $g_1,\ g_2 \in \mathrm{Ann}(f)$, то $f(g_1+g_2) \equiv 0$, поэтому $\mathrm{Ann}(f)$ — линейное подпространство в V_{2^n}. Из предыдущего утверждения легко установить, что $\dim \mathrm{Ann}(f) = 2^n - \|f\|$. Для произвольного k в $\mathrm{Ann}(f)$ можно выделить линейное подпространство $\mathrm{Ann}_k(f) = \{g \in \mathrm{Ann}(f) \colon \deg g \le k\}$.

Определение 2. *Порядком алгебраической иммунности* функции $f \in \mathcal{F}_n$ называется следующая величина: $AI(f) = \min\{\deg g, g \in \mathcal{F}_n, g \neq 0 : fg \equiv 0 \vee (f+1)g \equiv 0\}$.

Перечислим также некоторые факты о преобразовании Уолша — Адамара, которые будут нами использоваться в дальнейшем. Под преобразованием Уолша — Адамара мы понимаем целочисленную функцию на пространстве V_n, а именно:

$$W_f(u) = \sum_{x \in V_n} (-1)^{f(x)+(u,x)}.$$

Утверждение 2. *Пусть $f \in \mathcal{F}_n$, $l \in \mathcal{L}_n$ и $l(x) = (u,x)$. Тогда расстояние по Хеммингу между функциями f и l можно выразить следующим образом:* $d(f,l) = 2^{n-1} - W_f(u)/2$.

Заметим, что функция $l+1 \in \mathcal{A}_n \setminus \mathcal{L}_n$ находится от f на расстоянии $d(f,l+1) = 2^{n-1} + W_f(u)/2$.

Определение 3. Пусть $f \in \mathcal{F}_n$. Нелинейностью функции f называется величина, равная расстоянию между этой функцией и множеством аффинных функций. Нелинейность f будем обозначать как $nl(f)$.

Утверждение 3. *Пусть $f \in \mathcal{F}_n$. Тогда* $nl(f) = 2^{n-1} - \max\limits_{u \in V_n} |W_f(u)|/2$.

Определение 4. Функция $f \in \mathcal{F}_n$ называется максимально-нелинейной, если ее нелинейность $nl(f)$ достигает максимально возможного для функции из $\mathcal{F}_n$ значения.

Определение 5. Пусть n — четное число. Функция $f \in \mathcal{F}_n$ называется бент-функцией, если все ее коэффициенты Уолша — Адамара равны $\pm 2^{n/2}$.

Бент-функции являются максимально нелинейными. Множество бент-функций от n переменных обозначается как $\mathcal{B}_n$. Дадим два интересующих нас утверждения о бент-функциях.

Утверждение 4. *Пусть булева функция f является бент-функцией от n переменных, тогда справедливо следующее равенство:* $\|f\| = 2^{n-1} \pm 2^{n/2-1}$.

Утверждение 5. *Пусть булева функция f является бент-функцией от n переменных, а l — некоторая аффинная функция от n переменных, тогда* $d(f, l) = 2^{n-1} \pm 2^{n/2-1}$.

2. Число функций, имеющих аффинные аннигиляторы

Мы будем обозначать множество булевых функций от n переменных, имеющих аффинные аннигиляторы, как $\mathcal{AA}_n$. Сразу заметим, что функция $g \equiv 0$ является аффинной и аннигилирует любую булеву функцию f, поэтому формально каждая булева функция имеет аффинный аннигилятор. Однако этот случай является тривиальным, поэтому, когда мы говорим о том, что некоторая функция f имеет аффинный аннигилятор, мы подразумеваем, что этот аннигилятор не является тождественным нулем.

В этом разделе мы оценим количество булевых функций, имеющих аффинные аннигиляторы. Рассмотрим произвольную функцию $f \in \mathcal{AA}_n$ и разложим ее по первой переменной: $f = \overline{x}_1 f_1(x_2, \ldots, x_n) + x_1 f_2(x_2, \ldots, x_n)$. Пусть функция f имеет некоторый аффинный аннигилятор g. Представим g в следующем виде: $g = x_1 g_1(x_2, \ldots, x_n) + g_2(x_2, \ldots, x_n)$, где $\deg g_1 = 0$ и $\deg g_2 \leq 1$. Нам известно, что $fg \equiv 0$, т.е.

$$(\overline{x}_1 f_1 + x_1 f_2)(x_1 g_1 + g_2) \equiv 0.$$

Раскрыв скобки, получим

$$\overline{x}_1 f_1 g_2 + x_1 f_2 (g_1 + g_2) \equiv 0.$$

Заметим, что функции $f_1 g_2$ и $f_2(g_1 + g_2)$ не зависят от переменной x_1, поэтому верхнее равенство равносильно следующей системе уравнений:

$$\begin{cases} f_1 g_2 \equiv 0, \\ f_2(g_1 + g_2) \equiv 0. \end{cases} \tag{1}$$

Учтем также ограничения на степени функций g_1 и g_2: $\deg g_1 = 0$. следовательно, либо $g_1 \equiv 1$, либо $g_1 \equiv 0$, поэтому система уравнений (1) эквивалентна совокупности двух следующих систем уравнений:

$$\begin{cases} f_1 g_2 \equiv 0, \\ f_2 g_2 \equiv 0; \end{cases} \tag{2}$$

$$\begin{cases} f_1 g_2 \equiv 0, \\ f_2 \overline{g}_2 \equiv 0. \end{cases} \tag{3}$$

Лемма 1. Число булевых функций от n переменных, имеющих аффинные аннигиляторы, удовлетворяет следующему неравенству:

$$|\mathcal{AA}_n| \geq 2|\mathcal{AA}_{n-1}|(2^{2^{n-2}} - 1) + 2^{2^{n-1}}.$$

Доказательство. Рассмотрим систему уравнений (2). Необходимо оценить количество пар (f_1, f_2), для которых найдется функция $g_2 \in \mathcal{A}_{n-1} \setminus \{0\}$, такая, что $(f_1 g_2 \equiv 0)$ и $(f_2 g_2 \equiv 0)$. Каждой такой паре функций однозначно соответствует $f \in \mathcal{AA}_n$, поэтому, посчитав количество пар (f_1, f_2), мы узнаем количество функций f, удовлетворяющих системе (2).

Функция g_2 аффинная. Следовательно, $f_1,\ f_2 \in \mathcal{AA}_{n-1}$. Выберем произвольную $f_1 \in$ $\in \mathcal{AA}_{n-1}$. Нам известно, что она имеет хотя бы один нетривиальный аффинный аннигилятор g_2. В свою очередь, $|\operatorname{Ann}(g_2)| = 2^{2^{n-2}}$, поэтому для выбранной f_1 существует, как минимум, $2^{2^{n-2}}$ подходящих функций f_2. Мы не можем оценить в точности число подходящих к f_1 функций f_2, так как в общем случае функция f_1 может иметь более одного нетривиального аффинного аннигилятора. Таким образом, число функций из $\mathcal{F}_n$, удовлетворяющих системе уравнений (2), не может быть меньше, чем $2^{2^{n-2}}|\mathcal{AA}_{n-1}|$.

Теперь обратимся к системе уравнений (3). Опять-таки будем оценивать количество удовлетворяющих ей пар функций (f_1, f_2). В отличие от предыдущего случая, функции f_1, f_2 не всегда обязаны принадлежать $\mathcal{AA}_{n-1}$. Например, при $g_2 \equiv 0$ и $f_2 \equiv 0$ функция f_1 может быть выбрана любой. Рассмотрим, для начала, случай, когда $f_1,\ f_2 \in \mathcal{AA}_{n-1}$. По аналогии с предыдущим случаем зафиксируем $f_1 \in \mathcal{AA}_{n-1}$ и тот же самый ее аннигилятор g_2, а функцию f_2 будем выбирать из $\operatorname{Ann}(\overline{g}_2)$. Так как $\overline{g}_2$ также является нетривиальной аффинной функций, значит, число функций в $\operatorname{Ann}(\overline{g}_2)$ равно $2^{2^{n-2}}$. Заметим, что среди подсчитанных функций ровно $|\mathcal{AA}_{n-1}| \times |\operatorname{Ann}(g_2) \cap \operatorname{Ann}(\overline{g}_2)|$ были нами уже учтены при рассмотрении системы уравнений (2). Очевидно, что $|\operatorname{Ann}(g_2) \cap \operatorname{Ann}(\overline{g}_2)| = 1$, поэтому на данный момент мы можем заключить, что

$$|\mathcal{AA}_n| \geq 2^{2^{n-2}}|\mathcal{AA}_{n-1}| + 2^{2^{n-2}}|\mathcal{AA}_{n-1}| - |\mathcal{AA}_{n-1}|; \tag{4}$$

$$|\mathcal{AA}_n| \geq 2^{2^{n-2}+1}|\mathcal{AA}_{n-1}| - |\mathcal{AA}_{n-1}|. \tag{5}$$

Теперь рассмотрим случай, когда какая-то из двух функций f_1, f_2 не принадлежит $\mathcal{AA}_{n-1}$. Как было сказано ранее, при $f_2 \equiv 0$ и при произвольной f_1 функция f имеет нетривиальный аффинный аннигилятор $g = x_1$. Таким образом, мы можем добавить еще $2^{2^{n-1}} - |\mathcal{AA}_{n-1}|$ не подсчитанных нами функций. Итого, имеем

$$|\mathcal{AA}_n| \geq 2|\mathcal{AA}_{n-1}|(2^{2^{n-2}} - 1) + 2^{2^{n-1}}.$$

Лемма доказана.

Дадим простую оценку сверху количества функций в $\mathcal{AA}_n$.

Лемма 2. Число булевых функций от n переменных, имеющих аффинные аннигиляторы, имеет следующую оценку сверху:

$$|\mathcal{AA}_n| \le 2^{2^{n-1}+n+1}.$$

Доказательство. Рассмотрим произвольную нетождественную аффинную функцию g от n переменных. Очевидно, что $|\operatorname{Ann}(g)| = 2^{2^{n-1}}$ и $\mathcal{AA}_n = \cup_{g\in\mathcal{A}_n\setminus\{0\}} \operatorname{Ann}(g)$. Таким образом, $|\mathcal{AA}_n| \le |\mathcal{A}_n| \times 2^{2^{n-1}} = 2^{2^{n-1}+n+1}$.

Теперь воспользуемся полученной оценкой для улучшения оценки снизу.

Лемма 3. $|\mathcal{AA}_n| \ge c2^{2^{n-1}+n+1}$ для $n \ge 5$, где $0 < c \le 0.5$.

Доказательство. Согласно лемме 1,

$$|\mathcal{AA}_n| \ge 2^{2^{n-2}+1}|\mathcal{AA}_{n-1}| + 2^{2^{n-1}} - 2|\mathcal{AA}_{n-1}|.$$

Докажем, что $2^{2^{n-1}} \ge 2|\mathcal{AA}_{n-1}|$. Согласно предыдущей оценке, $2|\mathcal{AA}_{n-1}| \le 2^{2^{n-2}+n+1}$. Таким образом, при $2^{n-1} \ge 2^{n-2}+n+1$ доказываемое неравенство точно выполнено. Далее, $2^{n-2} \ge n+1$ для любого $n \ge 5$, поэтому $2^{2^{n-1}} \ge 2|\mathcal{AA}_{n-1}|$ для любого $n \ge 5$. Таким образом, установлено, что

$$|\mathcal{AA}_n| \ge 2^{2^{n-2}+1}|\mathcal{AA}_{n-1}|, \quad n \ge 5.$$

Данное рекуррентное выражение можно упростить следующим образом:

$$|\mathcal{AA}_n| \ge 2^{\sum\limits_{i=3}^{n-2} 2^i+n-5}|\mathcal{AA}_4| = 2^{\sum\limits_{i=0}^{n-2} 2^i+n-5-7}|\mathcal{AA}_4| = 2^{2^{n-1}+n-13}|\mathcal{AA}_4|.$$

Таким образом,

$$|\mathcal{AA}_n| \ge c2^{2^{n-1}+n+1}, \quad n \ge 5,$$

где $c = \dfrac{|\mathcal{AA}_4|}{2^{14}}$.

Используя оценку из леммы 2, заключаем, что $c \le \dfrac{1}{2}$. Также очевидно, что $c > 0$.

Пусть $g(n) = 2^{2^{n-1}+n+1}$. Как мы видим, при $n \ge 5$ выполнено условие

$$cg(n) \le |\mathcal{AA}_n| \le g(n),$$

где $0 < c \le \dfrac{1}{2}$.

Приходим к следующему утверждению.

Теорема 1. Функции $|\mathcal{AA}_n|$ и $g(n) = 2^{2^{n-1}+n+1}$ при $n \to \infty$ являются функциями одного порядка.

3. Расстояние между $\mathcal{AA}_n$ и произвольной булевой функцией

Уравнение вида $f(x) = 1$, где $f \in \mathcal{AA}_n$, может быть заменено на линейное уравнение вида $l(x) = 0$. Здесь l является нетривиальным аффинным аннигилятором функции f. Теперь предположим, что мы решаем уравнение $h(x) = 1$, где функция h находится на небольшом расстоянии от функции f. В этом случае для решения уравнения $h(x) = 1$ мы предлагаем решать уравнение $l(x) = 0$. А именно, мы исходим из того, что маленькое расстояние между h и f позволяет считать, что с высокой вероятностью на тех x, где $h(x) = 1$, функция f принимает также значение 1, а, значит, с высокой вероятностью мы можем заменить уравнение $h(x) = 1$ на уравнение $l(x) = 0$. Этот метод напоминает метод замены функции ее линейным статаналогом, однако может быть более успешным в виду того, что мощность $\mathcal{AA}_n$ существенно превосходит мощность $\mathcal{A}_n$. Более того, $\mathcal{A}_n \setminus \{1\}$ является подмножеством $\mathcal{AA}_n$.

Отметим, что любая аффинная функция $l(x)$ может быть представлена в виде $l(x) = b + (u, x)$, где $u \in V_n$, а $b \in \{0, 1\}$. Сейчас мы свяжем спектр булевой функции с ее расстоянием до $\mathcal{AA}_n$. Для начала установим связь между значением коэффициента Уолша — Адамара $W_f(u)$ и расстоянием между f и множеством $\mathrm{Ann}((u, x))$.

Лемма 4. Пусть $f \in \mathcal{F}_n$, а $l \in \mathcal{L}_n \setminus \{0\}$ и $l = (u, x)$. Тогда $d(f, \mathrm{Ann}(l)) = \dfrac{\|f\|}{2} + \dfrac{W_f(u)}{4}$.

Доказательство. Пусть $v = fl$. $v = fl$. Тогда $vl = fl$, а поэтому $(f + v)l \equiv 0$, т.е. $(f + v) \in \mathrm{Ann}(l)$. Найдем расстояние $d(f, f + v)$, для этого введем четыре переменных:

1) $k_1 = \{x \in V_n : f(x) = 0 \wedge l(x) = 0\}$;
2) $k_2 = \{x \in V_n : f(x) = 1 \wedge l(x) = 1\}$;
3) $m_1 = \{x \in V_n : f(x) = 0 \wedge l(x) = 1\}$;
4) $m_2 = \{x \in V_n : f(x) = 1 \wedge l(x) = 0\}$.

Очевидно, что $d(f, f + v) = \|v\| = k_2$. Найдем k_2 из следующей системы линейных уравнений:

$$\begin{cases} k_2 + m_2 = \|f\|, \\ k_2 + m_1 = 2^{n-1}, \\ m_1 + m_2 = d(f, l) = 2^{n-1} - W_f(u)/2. \end{cases}$$

Таким образом, $k_2 = d(f, f + v) = W_f(u)/4 + \|f\|/2$. Для любой функции $h \in \mathrm{Ann}(l)$ имеем $h(x) = 0$ при всех x, удовлетворяющих условию $l(x) = 1$. Следовательно, $d(f, \mathrm{Ann}(l)) \geq k_2$. Таким образом, $d(f, \mathrm{Ann}(l)) = W_f(u)/4 + \|f\|/2$. Лемма доказана.

Нетрудно видеть, что $d(f, \mathrm{Ann}(l + 1)) = \dfrac{\|f\|}{2} - \dfrac{W_f(u)}{4}$. Заметим также, что ближайшая к f функция из $\mathrm{Ann}(l)$ или из $\mathrm{Ann}(l + 1)$ отличается от f только на тех наборах x, где $f(x) = 1$. Это говорит о том, что вероятность успешной замены уравнения $f(x) = 1$ на $l(x) = 0$ равна $1 - \dfrac{d(f, \mathrm{Ann}(l))}{\|f\|}$.

Теперь перейдем к вычислению величины $d(f, \mathcal{AA}_n)$. Поскольку $\mathcal{AA}_n = \bigcup\limits_{g \in \mathcal{A}_n} \mathrm{Ann}(g)$, имеем $d(f, \mathcal{AA}_n) = \min\limits_{g \in \mathcal{A}_n} d(f, \mathrm{Ann}(g))$. Таким образом, справедлива следующая теорема.

Теорема 2. Пусть $f \in \mathcal{F}_n$. Тогда

$$d(f, \mathcal{AA}_n) = \frac{\|f\|}{2} - \max_{u \in V_n \setminus \{0\}} \frac{|W_f(u)|}{4}.$$

Теперь сформулируем критерий принадлежности булевой функции множеству $\mathcal{AA}_n$.

Теорема 3. Булева функция $f \in \mathcal{F}_n$ имеет нетождественный аффинный аннигилятор тогда и только тогда, когда найдется спектральный коэффициент $W_f(u)$, где $u \neq 0$, такой, что $W_f(u) = \pm 2\|f\|$.

Доказательство. Пусть f имеет нетождественный аффинный аннигилятор l. Пусть l представляется в виде $(u, x) + b$, где $b \in \{0, 1\}$. Очевидно, что $d(f, \mathrm{Ann}(l)) = 0$, поэтому $\frac{\|f\|}{2} \pm \frac{W_f(u)}{4} = 0$. Отсюда следует, что $W_f(u) = \pm 2\|f\|$. А так как l — нетождественная аффинная функция, то $u \neq 0$. Необходимость доказана.

Теперь предположим, что нашелся такой ненулевой u, что $W_f(u) = \pm 2\|f\|$. Это значит, что либо $\frac{\|f\|}{2} - \frac{W_f(u)}{4}$, либо $\frac{\|f\|}{2} + \frac{W_f(u)}{4} = 0$. Следовательно, либо $d(f, \mathrm{Ann}((u, x))) = 0$, либо $d(f, \mathrm{Ann}((u, x) + 1)) = 0$. Таким образом, либо (u, x) — аннигилятор f, либо $(u, x) + 1$ — аннигилятор f. В обоих случаях эти аннигиляторы нетождественны, так как $u \neq 0$. Достаточность доказана.

Из этого утверждения вытекают следующие ограничения на коэффициенты Уолша — Адамара.

Теорема 4. Пусть $f \in \mathcal{F}_n$. Тогда каждый ее коэффициент Уолша — Адамара $W_f(u)$, за исключением коэффициента, соответствующего $u = 0$, ограничен следующим образом:

$$-2\|f\| \leq W_f(u) \leq 2\|f\|.$$

Доказательство. Выберем произвольный вектор $u \in V_n \setminus \{0\}$ и свяжем с ним линейную функцию $l(x) = (u, x)$. Согласно лемме 4, $d(f, \mathrm{Ann}((u, x))) = \frac{\|f\|}{2} + \frac{W_f(u)}{4}$. Также очевидно, что $d(f, \mathrm{Ann}((u, x))) \geq 0$. Следовательно, $W_f(u) \geq -2\|f\|$.

Теперь свяжем с вектором u аффинную функцию $(u, x) + 1$. Аналогично запишем, что $\frac{\|f\|}{2} - \frac{W_f(u)}{4} \geq 0$. Таким образом, $W_f(u) \leq 2\|f\|$. Теорема доказана.

Перейдем к рассмотрим отношения $\frac{d(f, \mathcal{AA}_n)}{\|f\|}$. Оно демонстрирует вероятность некорректной замены уравнения $f(x) = 1$ на линейное: чем выше значение этой дроби, тем меньше вероятность успешной замены. Нетрудно видеть, что

$$\frac{d(f, \mathcal{AA}_n)}{\|f\|} = \frac{1}{2} - \frac{\max\limits_{u \in V_n \setminus \{0\}} |W_f(u)|}{4\|f\|} \leq \frac{1}{2}.$$

Теорема 5. Пусть булева функция f является бент-функцией от n переменных. Тогда

$$\lim_{n \to \infty} \frac{d(f, \mathcal{AA}_n)}{\|f\|} = \frac{1}{2},$$

т.е. для каждой бент-функции отношение ее расстояния до $\mathcal{AA}_n$ к ее весу достигает верхней границы при $n \to \infty$.

Доказательство. Нетрудно видеть, что если $f \in \mathcal{B}_n$, то

$$\frac{d(f, \mathcal{AA}_n)}{\|f\|} = \frac{1}{2} - \frac{1}{4\|f\|} 2^{\frac{n}{2}}.$$

Вес такой функции f равен $2^{n-1} \pm 2^{n/2-1}$. Следовательно,

$$\frac{d(f, \mathcal{AA}_n)}{\|f\|} = \frac{1}{2} - \frac{2^{\frac{n}{2}-2}}{2^{n-1} \pm 2^{\frac{n}{2}-1}}.$$

Легко видеть, что

$$\lim_{n\to\infty} \frac{d(f, \mathcal{AA}_n)}{\|f\|} = \frac{1}{2}.$$

Теорема доказана.

Таким образом, асимптотически бент-функции имеют максимально возможное отношение $\frac{d(f, \mathcal{AA}_n)}{\|f\|}$. Тем самым они являются одними из наиболее неподходящих для предложенного метода анализа булевых уравнений. В некотором смысле бент-функции максимально удалены не только от аффинных функций, но и от функций, имеющих аффинные аннигиляторы.

Заключение

В данной работе были исследованы булевы функции, имеющие аффинные аннигиляторы. Удалось оценить количество таких функций. Был предложен метод анализа булевых уравнений, основанный на замене функции из уравнения на ближайшую к ней функцию с аффинным аннигилятором. Для реализации предложенного метода была получена взаимосвязь между спектром булевой функции и ее расстоянием до множества функций, имеющих аффинные аннигиляторы, а также был получен криАий принадлежности функции к данному множеству. Было доказано, что бент-функции «максимально удалены» от функций с аффинными аннигиляторами.

Список литературы

1. Courtois N., Meier W. Algebraic attacks on stream ciphers with linear feedback // Advances in cryptology — EUROCRYPT 2003: Intern. conf. on the theory and applications of cryptographic techniques (Warszaw, Poland, May 4-8, 2003): Proc. B.: Springer, 2003. Pp. 345–359. DOI: 10.1007/3-540-39200-9_21
2. Meier W., Pasalic E., Carlet C. Algebraic attacks and decomposition of Boolean functions // Advances in cryptology — EUROCRYPT 2004: Intern. conf. on the theory and applications of cryptographic techniques (Interlaken, Switzerland, May 2-6, 2004): Proc. B.: Springer, 2004. Pp. 474–491. DOI: 10.1007/978-3-540-24676-3_28

3. Courtois N. Fast algebraic attacks on stream ciphers with linear feedback // Advances in cryptology — CRYPTO 2003: 23rd Annual intern. cryptology conf. (Santa Barbara, CA, USA, August 17-21, 2003): Proc. B.: Springer, 2003. Pp. 176–194. DOI: 10-1007/978-3-540-45146-4_11
4. Баев В.В. О некоторых алгоритмах построения аннигиляторов низкой степени для булевых функций // Дискретная математика. 2006. Т. 18, № 3. С. 138–151. DOI: 10.4213/dm66
5. Баев В.В. Усовершенствованный алгоритм поиска аннигиляторов низкой степени для многочлена Жегалкина // Дискретная математика. 2007. Т. 19, № 4. с.132–138. DOI: 10.4213/dm982
6. Armknecht F. On the existence of low-degree equations for algebraic attacks // Cryptology ePrint Archive: Report 2004/185. Режим доступа: https://eprint.iacr.org/2004/185.pdf (дата обращения 09.04.2021).
7. Dalai D.K., Gupta K.C., Maitra S. Results on algebraic immunity for cryptographically significant Boolean functions // Progress in cryptology — INDOCRYPT 2004: 5th intern. conf. on cryptology in India (Chennai, India, December 20-22, 2004): Proc. B.: Springer, 2005. Pp. 92–106. DOI: 10.1007/978-3-540-30556-9_9
8. Carlet C. On the higher order nonlinearities of algebraic immune functions // Advances in cryptology — CRYPTO 2006: 26th Annual intern. cryptology conf. (Santa Barbara, CA, USA, August 20-24, 2006): Proc. B.: Springer, 2006. Pp. 584–601. DOI: 10.1007/11818175_35
9. Mesnager S. Improving the lower bound on the higher order nonlinearity of Boolean functions with prescribed algebraic immunity // Cryptology ePrint Archive: Report 2007/117. Режим доступа: https://eprint.iacr.org/2007/117.pdf (дата обращения 09.04.2021).
10. Логачев О.А., Сальников А.А., Смышляев С.В., Ященко В.В. Булевы функции в теории кодирования и криптологии: учеб. пособие. М.: ЛЕНАНД, 2015. 573 с.

Mathematics and Mathematical Modeling, 2020, no. 6, pp. 1–12.
DOI: **10.24108/mathm.0620.0000246**

Mathematics & Mathematical Modelling
Electronic journal
http://mathmelpub.ru ISSN 2412-5911

Boolean Functions with Affine Annihilators

Zelenetsky A. S.[1,*], **Klyucharev P. G.**[1]

[1]Bauman Moscow State Technical University, Moscow, Russia
[*]Zelenetskiy_alexey@mail.ru

Keywords: boolean function, annihilator, affine function; linear function; Walsh — Hadamard transformation, bent function

Received: 15.01.2021.

In the article we study boolean functions with affine annihilators. We have obtained results in both, estimating the number of functions under study and defining the relationship between Walsh-Hadamard coefficients of an arbitrary boolean function and its affine annihilator available. The second section of this article focuses on estimating the number of boolean functions with affine annihilators. The value has top and bottom bound. Besides, we have obtained the asymptotic estimate of the number of boolean functions with affine annihilators. The third section studies the Walsh-Hadamard coefficients of boolean functions with affine annihilators. First, we have derived the dependence of the Walsh-Hadamard coefficient on the distance between an arbitrary boolean function and a vector space of the affine function's annihilators. Based on this result, we have obtained the dependence of distance between an arbitrary boolean function and a set of functions with affine annihilators on the spectrum of given function. Also we have defined the necessary and sufficient condition for the arbitrary boolean function to be with an affine annihilator available. Using the results obtained we bounded an absolute value of Walsh-Hadamard coefficients.

Also we suggested a method for boolean equations analysis, which is based on two known methods. Namely, we used an analysis using annihilators and an analysis using linear analogs. We have obtained an estimate of the success probability of the suggested method for an arbitrary boolean function. Also we proved that bent functions are the most resistant to this analysis.

The results obtained can be used in analysis of boolean equations. Also obtained dependences can be used, for instance, to study bent functions and algebraic immunity of boolean functions.

References

1. Courtois N., Meier W. Algebraic attacks on stream ciphers with linear feedback. *Advances in cryptology — EUROCRYPT 2003: Intern. conf. on the theory and applications of crypto-*

graphic techniques (Warszaw, Poland, May 4-8, 2003): Proc. B.: Springer, 2003. Pp. 345–359. DOI: 10.1007/3-540-39200-9_21

2. Meier W., Pasalic E., Carlet C. Algebraic attacks and decomposition of Boolean functions. *Advances in cryptology — EUROCRYPT 2004: Intern. conf. on the theory and applications of cryptographic techniques (Interlaken, Switzerland, May 2-6, 2004): Proc.* B.: Springer, 2004. Pp. 474–491. DOI: 10.1007/978-3-540-24676-3_28
3. Courtois N. Fast algebraic attacks on stream ciphers with linear feedback. *Advances in cryptology — CRYPTO 2003: 23rd Annual intern. cryptology conf. (Santa Barbara, CA, USA, August 17-21, 2003): Proc.* B.: Springer, 2003. Pp. 176–194. DOI: 10-1007/978- 3-540-45146-4_11
4. Baev V.V. On some algorithms for constructing low-degree annihilators for Boolean functions. *Discrete Mathematics and Applications*, 2006, vol. 16, no. 5, pp. 439–452. DOI: 10.1515/156939206779238427
5. Baev V.V. An enhanced algorithm to search for low-degree annihilators for a Zhegalkin polynomial. *Discrete Mathematics and Applications*, 2007, vol. 17, no. 5, pp. 533–538. DOI: *10.1515/dma.2007.041*
6. Armknecht F. On the existence of low-degree equations for algebraic attacks. *Cryptology ePrint Archive, 2004, report 2004/185*. Available at: https://eprint.iacr.org/2004/185.pdf, accessed 09.04.2021.
7. Dalai D.K., Gupta K.C., Maitra S. Results on algebraic immunity for cryptographically significant Boolean functions. *Progress in cryptology — INDOCRYPT 2004: 5th intern. conf. on cryptology in India (Chennai, India, December 20-22, 2004): Proc.* B.: Springer, 2005. Pp. 92–106. DOI: 10.1007/978-3-540-30556-9_9
8. Carlet C. On the higher order nonlinearities of algebraic immune functions. *Advances in cryptology — CRYPTO 2006: 26th Annual intern. cryptology conf. (Santa Barbara, CA, USA, August 20-24, 2006): Proc.* B.: Springer, 2006. Pp. 584–601. DOI: 10.1007/11818175_35
9. Mesnager S. Improving the lower bound on the higher order nonlinearity of Boolean functions with prescribed algebraic immunity. *Cryptology ePrint Archive, 2007, report 2007/117*. Available at: https://eprint.iacr.org/2007/117.pdf, accessed 09.04.2021.
10. Logachev O.A., Salnikov A.A., Smyshlyaev S.V., Yashchenko V.V. *Bulevy funktsii v teorii kodirovaniia i kriptologii* [Boolean functions in coding theory and cryptology]: a textbook. Moscow: LENAND Publ., 2015. 573 p. (in Russian).