Yu. V. Tarannikov, On values of the affine rank of the support of spectrum of a plateaued function,
Diskr. Mat., 2006, Volume 18, Issue 3, 120–137

Дискретная математика

том 18 выпуск 3 * 2006

УДК 519.7

О значениях аффинного ранга носителя спектра платовидной функции

© 2006 г. Ю. В. Таранников

В статье доказывается, что аффинный ранг любой платовидной функции с носителем спектра мощности 16 равен 4, 5 или 6. Для любого натурального h рассматриваются платовидные функции с носителем спектра мощности 4^h, даются оценки аффинного ранга таких функций и строятся функции, аффинный ранг которых принимает все возможные значения от $2h$ до $2^{h+1}-2$.

1. Введение и основные определения

Пусть F_2^n — векторное пространство наборов длины n с компонентами из поля F_2 из двух элементов 0 и 1, операции сложения и умножения в котором вводятся как обычные операции сложения и умножения чисел 0 и 1 по модулю 2. Булева функция от n переменных — это отображение из F_2^n в F_2. В дальнейшем мы будем обозначать набор из F_2^n буквой без нижнего индекса, а компоненту этого набора — той же буквой с нижним индексом, указывающим на порядковый номер этой компоненты в наборе. Наборы x' и x'' называются соседними, если они различаются только в одной компоненте. Обозначим через x^i набор, который отличается от x только в i-й компоненте, $i = 1, \ldots, n$. Переменная x_i называется фиктивной для функции f, если для любых наборов x' и x'', соседних по i-й компоненте, выполняется равенство $f(x') = f(x'')$. Расстоянием Хэмминга $d(x', x'')$ между двумя наборами x' и x'' называют число компонент, в которых наборы x' и x'' различаются. Для заданной функции f из F_2^n минимум расстояний $d(f, l)$, где l пробегает множество всех аффинных функций из F_2^n называется нелинейностью функции f и обозначается через $\mathrm{nl}(f)$. Подфункцией булевой функции f называется функция f', полученная подстановкой в f констант 0 или 1 вместо некоторых переменных.

Хорошо известно, что функция f, заданная на F_2^n, имеет единственное полиномиальное представление над F_2, степень которого по каждой переменной не превосходит 1, а именно,

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

где g — также функция над F_2^n. Такое полиномиальное представление f называется алгебраической нормальной формой функции, а каждое выражение $x_1^{a_1} \ldots x_n^{a_n}$ называется слагаемым в алгебраической нормальной форме функции f (алгебраическую нормальную форму называют также полиномом Жегалкина). Отображение $f(x) \to g(x)$ иногда называют преобразованием Мебиуса.

Алгебраическая степень функции f, обозначаемая через $\deg(f)$, определяется как число переменных в самом длинном слагаемом в алгебраической нормальной форме функции f.

Вес $\mathrm{wt}(f)$ функции f над F_2^n — это число наборов x из F_2^n, для которых $f(x) = 1$. Функция f называется уравновешенной, если

$$\mathrm{wt}(f) = \mathrm{wt}(f \oplus 1) = 2^{n-1},$$

то есть если функция принимает значения 0 и 1 на одинаковом числе наборов.

Пусть $x = (x_1, \ldots, x_n)$ и $u = (u_1, \ldots, u_n)$ — это наборы длины n над F_2. Скалярное произведение x и u — это функция, которая определяется как

$$\langle x, u \rangle = \sum_{i=1}^{n} x_i u_i,$$

где сложение и умножение берутся над F_2. Под суммой $x + u$ двух двоичных наборов x и u мы понимаем их покомпонентную сумму над F_2.

Преобразованием Уолша булевой функции f называется целочисленная функция над F_2^n, определяемая равенством

$$W_f(u) = \sum_{x \in F_2^n} (-1)^{f(x)+\langle u,x \rangle}.$$

Для каждого $u \in F_2^n$ значение $W_f(u)$ называется коэффициентом Уолша. Коэффициенты Уолша будем называть спектральными коэффициентами, а совокупность всех 2^n коэффициентов Уолша — спектром булевой функции. Справедливы формула обращения

$$(-1)^{f(x)} = 2^{-n} \sum_{u \in F_2^n} W_f(u)(-1)^{\langle u,x \rangle}$$

и равенство Парсеваля

$$\sum_{u \in F_2^n} W_f^2(u) = 2^{2n}.$$

Нелинейность булевой функции f выражается через ее коэффициенты Уолша следующим образом:

$$\mathrm{nl}(f) = 2^{n-1} - \frac{1}{2} \max_{u \in F_2^n} |W_f(u)|.$$

Множество S_f всех наборов u таких, что $W_f(u) \neq 0$, называется носителем спектра функции f.

Булева функция называется бент-функцией, если значение коэффициентов на всех наборах равно $\pm 2^{n/2}$. Бент-функции существуют при всех четных n, а при нечетных не существуют. Бент-функция является функцией с максимально возможной нелинейностью $2^{n-1} - 2^{(n/2)-1}$ среди всех функций от n переменных при четном n. Булева функция называется платовидной, если ее коэффициенты Уолша принимают ровно три возможных значения. Несложно показать, что эти значения могут быть только 0 и $\pm 2^c$ для некоторого c. Платовидные функции представляют большой интерес для изучения бент-функций (например, потому, что при разложении бент-функции по переменной возникают две платовидные функции), а также потому, что многие криптографически важные функции являются платовидными (например, m-устойчивые функции с максимально возможной для

них нелинейностью $2^{n-1}-2^{m+1}$). Для платовидных функций положим $\varphi(x)=2^{-c}W_f(x)$, тогда для любого $x \in F_2^n$ величина $\varphi(x)$ может принимать только три значения: 0, -1 и 1. Множество S_f всех наборов u таких, что $W_f(u) \neq 0$, называется носителем спектра платовидной функции. Множество всех наборов, на которых $\varphi(x)=-1$, будем обозначать T^-, а множество всех наборов, на которых $\varphi(x)=1$, будем обозначать T^+. Из равенства Парсеваля следует, что мощность носителя спектра равна 4^{n-c}. Бент-функцию удобно рассматривать как частный случай платовидной при $c=n/2$ и $|S_f|=2^n$, что мы и будем часто делать (хотя часто формально бент-функции к платовидным не относят). Платовидные функции изучались в большом числе работ, см., например, [1, 4, 9].

Для каждого $u \in F_2{}^n$ автокорреляционный коэффициент функции f на наборе u определяется как

$$\Delta_f(u)=\sum_{x\in F_2{}^n}(-1)^{f(x)+f(x+u)}.$$

Функция $D_u f = f(x)+f(x+u)$ называется производной функции f по направлению u. Множество наборов $u \in F_2{}^n$ таких, что $D_u f$ есть постоянная, называется линейной структурой функции f. Легко проверить, что линейная структура функции f образует линейное пространство в F_2^n. Наличие у функции линейных структур в некоторых случаях (но не во всех) является криптографической слабостью.

Пусть E — произвольное подмножество F_2^n. Рангом множества E называется размерность подпространства, порожденного E в F_2^n. Аффинным рангом множества E называется размерность наименьшего класса смежности в F_2^n, содержащего E. Ранг и аффинный ранг носителя спектра булевой функции будем обозначать через k и k_a, соответственно. Для краткости в данной работе аффинный ранг и ранг носителя спектра булевой функции мы будем называть просто ее аффинным рангом и рангом, соответственно. Легко убедиться, что $k_a \in \{k, k-1\}$. Известно (см., например, [5]), что размерность линейной структуры функции f равна $n-k_a$. Если существует набор $u \in F_2^n$ такой, что $D_u f \equiv 1$, то $k=k_a+1$. Если такого набора не существует, то $k=k_a$.

Дополнительные сведения о свойствах булевых функций можно найти в [2] и [3].

2. Об аффинных преобразованиях в F_2^n

Аффинным преобразованием в F_2^n называется отображение

$$x \to x' = \mathbf{A}x = xA^T + a,$$

где A — квадратная двоичная невырожденная над F_2 матрица порядка n, а a — вектор длины n. Аффинное преобразование является автоморфизмом F_2^n, при котором все классы смежности переходят в классы смежности той же размерности. Если $a=0$, то аффинное преобразование называется также линейным.

Аффинным преобразованием функции f, заданной на F_2^n, называется преобразование

$$f(x) \to f'(x) = f(\mathbf{A}x).$$

Если для функций f и f' существует аффинное преобразование функции, переводящее f в f', то f и f' называются аффинно эквивалентными. Если для функций f и f' существует линейное преобразование функции, переводящее f в f', то f и f' называются линейно эквивалентными.

Лемма 1. *Пусть* $f(x) \to f'(x) = f(\mathbf{A}x)$ *— аффинное преобразование функции* f*, заданной на* F_2^n*. Тогда*

$$W_{f'(x)}(u) = (-1)^{\langle a, uA^{-1}\rangle} W_f(uA^{-1}).$$

Доказательство. По формуле для коэффициентов Уолша

$$\begin{aligned} W_{f'(x)}(u) &= \sum_{x \in F_2^n} (-1)^{f'(x)+\langle x,u\rangle} = \sum_{x \in F_2^n} (-1)^{f(\mathbf{A}x)+\langle x,u\rangle} = \sum_{x \in F_2^n} (-1)^{f(x)+\langle \mathbf{A}^{-1}x,u\rangle} \\ &= \sum_{x \in F_2^n} (-1)^{f(x)+\langle x,uA^{-1}\rangle+\langle a,uA^{-1}\rangle} = (-1)^{\langle a,uA^{-1}\rangle} \sum_{x \in F_2^n} (-1)^{f(x)+\langle x,uA^{-1}\rangle} \\ &= (-1)^{\langle a,uA^{-1}\rangle} W_f(uA^{-1}). \end{aligned}$$

Пусть булева функция f задана на F_2^n. Аффинным преобразованием спектра функции f называется преобразование

$$W_f(x) \to W'(x) = W_f(\mathbf{A}x).$$

Можно показать, что коэффициенты $W'(x)$ являются коэффициентами Уолша некоторой функции f', которая, вообще говоря, не является аффинно эквивалентной функции f.

Лемма 2. *Пусть* $W_f(x) \to W'(x) = W_f(\mathbf{A}x)$ *— аффинное преобразование спектра функции* f*, заданной на* F_2^n*. Тогда коэффициенты* $W'(x)$ *являются коэффициентами Уолша некоторой функции* f'*, причем*

$$f'(x) = f(xA^{-1}) + \langle a, xA^{-1}\rangle.$$

Доказательство. Проверим, что для всех $x \in F_2^n$ суммы в формуле обращения для гипотетически существующей функции $f'(x)$ равны ± 1. Введем обозначение

$$F(x) = 2^{-n} \sum_{u \in F_2^n} W'(u)(-1)^{\langle u,x\rangle}.$$

Справедливы равенства

$$\begin{aligned} F(x) &= 2^{-n} \sum_{u \in F_2^n} W'(u)(-1)^{\langle u,x\rangle} = 2^{-n} \sum_{u \in F_2^n} W_f(\mathbf{A}u)(-1)^{\langle u,x\rangle} \\ &= 2^{-n} \sum_{v \in F_2^n} W_f(v)(-1)^{\langle \mathbf{A}^{-1}v,x\rangle} = 2^{-n} \sum_{v \in F_2^n} W_f(v)(-1)^{\langle v,xA^{-1}\rangle+\langle a,xA^{-1}\rangle} \\ &= (-1)^{\langle a,xA^{-1}\rangle} 2^{-n} \sum_{v \in F_2^n} W_f(v)(-1)^{\langle v,xA^{-1}\rangle} = (-1)^{f(xA^{-1})+\langle a,xA^{-1}\rangle}. \end{aligned}$$

Таким образом, для всех $x \in F_2^n$ справедливо равенство $F(x) = \pm 1$. Поэтому функция $f'(x)$ существует, более того,

$$f'(x) = f(xA^{-1}) + \langle a, xA^{-1}\rangle.$$

Спектры функций f и f', переводимые один в другой аффинным преобразованием спектра, называются аффинно эквивалентными. Спектры функций f и f', переводимые

один в другой линейным преобразованием спектра, называются линейно эквивалентными. Из аффинной эквивалентности функций не следует аффинная эквивалентность их спектров. Например, потому, что при аффинном преобразовании функции f величина $\mathrm{wt}(f)$ остается неизменной, но $\mathrm{wt}(f) = 2^{n-1} - (1/2)W_f(0)$, поэтому переводя при аффинном преобразовании спектра в 0 набор с другим значением коэффициента Уолша, мы получим функцию, не являющуюся аффинно эквивалентной f. В то же время из лемм 1 и 2 видно, что линейное преобразование спектра является линейным преобразованием функции, и наоборот.

Очевидно, что аффинное преобразование спектра платовидной функции f переводит его в спектр также некоторой платовидной функции f' с той же мощностью носителя спектра, а аффинное преобразование платовидной функции f переводит ее в платовидную функцию f' с той же мощностью носителя спектра.

Лемма 3. *Пусть f — булева функция, заданная на F_2^n, причем носитель спектра этой функции лежит в $F_2^l \otimes (0,\dots,0)$, где $(0,\dots,0) \in F_2^{n-l}$. Тогда функция f зависит от переменных $x_{l+1}, \dots, x_n$ фиктивно.*

Пусть f' — функция на F_2^n, полученная из f удалением фиктивных переменных $x_{l+1},\dots,x_n$. Тогда для любого u из F_2^l справедливо равенство

$$W_{f'}(u) = 2^{-(n-l)} W_f(u,0,\dots,0),$$

где $(u,0,\dots,0) \in F_2^n$.

Доказательство. Пусть x и x^i — произвольная пара наборов, соседних по i-й компоненте, $i \in \{l+1,\dots,n\}$. По формуле обращения

$$\begin{aligned}(-1)^{f(x)} - (-1)^{f(x^i)} &= 2^{-n} \sum_{u \in F_2^n} W_f(u)((-1)^{\langle x,u\rangle} - (-1)^{\langle x^i,u\rangle}) \\ &= 2^{-n} \sum_{u \in F_2^l \otimes (0,\dots,0)} W_f(u)((-1)^{\langle x,u\rangle} - (-1)^{\langle x^i,u\rangle}) = 0.\end{aligned}$$

Поэтому $f(x) = f(x^i)$, и переменные $x_{l+1}, \dots, x_n$, таким образом, действительно являются фиктивными. Рассмотрим теперь функцию f' на F_2^n, полученную из f удалением фиктивных переменных $x_{l+1}, \dots, x_n$. Для любого ее коэффициента Уолша

$$\begin{aligned}W_{f'}(u) &= \sum_{x \in F_2^l} (-1)^{f'(x)+\langle x,u\rangle} = 2^{-(n-l)} \sum_{x \in F_2^n} (-1)^{f(x)+\langle x,(u,0,\dots,0)\rangle} \\ &= 2^{-(n-l)} W_f(u,0,\dots,0),\end{aligned}$$

где $u \in F_2^l$ и $(u,0,\dots,0) \in F_2^n$.

Лемма 4. *Пусть f — булева функция, заданная на F_2^n. Пусть f' — функция на F_2^{n+1}, определенная равенством*

$$f'(x_1,\dots,x_n,x_{n+1}) = f(x_1,\dots,x_n) + x_{n+1}.$$

Тогда если u — набор из F_2^{n+1}, принадлежащий носителю спектра функции f', то

$$u_{n+1} = 1, \qquad W_{f'}(u_1,\dots,u_n,1) = 2W_f(u_1,\dots,u_n).$$

Доказательство. Пусть $u \in F_2^{n+1}$. В сумме

$$W_{f'}(u) = \sum_{x \in F_2^{n+1}} (-1)^{f(x)+\langle x,u\rangle}$$

сгруппируем в пары наборы x и x^{n+1}, различающиеся только в $(n+1)$-й компоненте. Для определенности пусть $x_{n+1} = 0$. Для этих наборов $f'(x) = f'(x^{n+1}) + 1$. Если $u_{n+1} = 0$, то $\langle x, u\rangle = \langle x^{n+1}, u\rangle$. Отсюда получаем, что

$$(-1)^{f'(x)+\langle x,u\rangle} + (-1)^{f'(x^{n+1})+\langle x^{n+1},u\rangle} = 0.$$

Поэтому и $W_{f'}(u) = 0$. Если $u_{n+1} = 1$, то $\langle x, u\rangle = \langle x^{n+1}, u\rangle + 1$. Отсюда получаем, что

$$\begin{aligned}(-1)^{f'(x)+\langle x,u\rangle} + (-1)^{f'(x^{n+1})+\langle x^{n+1},u\rangle} &= 2(-1)^{f'(x)+\langle x,u\rangle} \\ &= 2(-1)^{f(x_1,\ldots,x_n)+\langle(x_1,\ldots,x_n),(u_1,\ldots,u_n)\rangle}.\end{aligned}$$

Поэтому $W_{f'}(u) = 2W_f(u_1, \ldots, u_n)$.

Из лемм 1, 2 и 3 следует, что изучение платовидных функций на F_2^n с носителем спектра мощности 4^h можно в некотором смысле свести к изучению платовидных функций с носителем спектра той же мощности 4^h, заданных на $F_2^{k_a}$. Более того, если $k_a > 2h$, то любую платовидную функцию f' на F_2^n с носителем мощности 4^h можно получить из некоторой функции f на $F_2^{k_a}$ с носителем той же мощности 4^h, добавив $n - k_a$ фиктивных переменных и выполнив некоторое линейное преобразование функции. Того же можно добиться и в случае, если $k_a = 2h$ и $W_{f'}(0) \neq 0$ (в этом случае функция f будет бент-функцией). Если $k_a = 2h$ и $W_{f'}(0) = 0$, то указанного линейного преобразования функции не существует, но можно использовать аффинное преобразование спектра, либо же взять функцию f от $k_a + 1$ переменной.

Заметим, что указанного сведения может быть недостаточно, если требуется исследовать дополнительные свойства функций, не сохраняющиеся при аффинных преобразованиях (например, корреляционную иммунность).

Укажем также на следующее свойство, позволяющее не рассматривать специально вопрос о возможных значениях, принимаемых рангом k.

Лемма 5. *Если существует платовидная функция с носителем спектра мощности* 4^h *и аффинным рангом, равным* k_a, *то существуют платовидные функции с носителем спектра той же мощности* 4^h *и рангами, равными и* $k = k_a$, *и* $k = k_a + 1$.

Доказательство. По лемме 2 аффинное преобразование носителя спектра платовидной функции снова дает платовидную функцию с носителем спектра той же мощности и с тем же аффинным рангом. Если аффинным преобразованием перевести в ноль один из наборов, входящий в наименьший класс смежности, содержащий S_f, то для получившейся функции, очевидно, будет выполнено равенство $k = k_a$. Если же перевести в ноль набор, не принадлежащий наименьшему классу смежности, содержащему S_f, то для получившейся функции $k = k_a + 1$. Если для исходной функции не было наборов, не принадлежащих наименьшему классу смежности, содержащему S_f (то есть, если k_a совпадало с числом переменных), то можно просто добавить фиктивную переменную и такие наборы появятся, а функция останется платовидной с той же мощностью спектра.

Из вышесказанного следует, что аффинный ранг является важной характеристикой платовидных функций. Очевидно, что аффинный ранг любой платовидной функции с носителем спектра мощности 4^h не меньше $2h$, потому что меньшие классы смежности не содержат 4^h наборов. Любая платовидная функция с носителем спектра мощности 1 есть аффинная функция и, очевидно, ее аффинный ранг равен 0. Аффинный ранг любой платовидной функции с носителем спектра мощности 4 равен 2. Этот факт доказан в [8], но, по-видимому, был известен намного раньше. Платовидные функции с носителем спектра мощности 16, не называясь платовидными, фактически рассматривались в [7], а в [5] для подкласса платовидных функций с носителем спектра мощности 16 (более точно, для кубических устойчивых порядка $n-4$ функций) была получена оценка $k_a \leqslant k \leqslant 9$. В настоящей работе мы докажем, что аффинный ранг любой платовидной функции с носителем спектра мощности 16 равен 4, 5 или 6. Кроме того, мы рассмотрим для любого натурального h платовидные функции с носителем спектра мощности 4^h, дадим оценки аффинного ранга для таких функций и построим функции, аффинный ранг которых принимает все возможные значения от $2h$ до $2^{h+1}-2$.

3. Вспомогательные результаты

Следующее утверждение хорошо известно (см., например, соотношение (2.16) в [2]). Ранее его доказательство было дано в [6].

Лемма 6. *Пусть f — булева функция на F_2^n. Пусть U является линейным подпространством в F_2^n размерности l, а $U^\perp$ — пространство, ортогональное к U в F_2^n. Пусть v — произвольный вектор из F_2^n. Тогда*

$$\sum_{u\in U+v} W_f(u) = 2^l \sum_{x\in U^\perp} (-1)^{f(x)+(x,v)}.$$

Лемма 7. *Пусть f — платовидная функция с носителем спектра мощности 4^h, заданная на F_2^n. Тогда*

$$\sum_{a\in F_2^n} \varphi(a) \in \{-2^h, 2^h\}.$$

Доказательство. Возьмем в лемме 6 в качестве подпространства U все F_2^n. В обозначениях леммы 6

$$W_f(u) = \varphi(u)2^{n-h}, \qquad l = n.$$

Тогда $U^\perp = \{0\}$. Поэтому

$$\sum_{u\in F_2^n} W_f(u) = 2^n(-1)^{f(0)}.$$

Отсюда следует, что

$$\sum_{u\in F_2^n} \varphi(u) = 2^h(-1)^{f(0)} \in \{-2^h, 2^h\}.$$

Лемма 8. *Пусть f — платовидная функция с носителем спектра мощности 4^h, заданная на F_2^n. Пусть*

$$\sum_{a\in F_2^n} \varphi(a) = 2^h.$$

Пусть H является $(n-1)$-мерным классом смежности в F_2^n. Тогда

$$\sum_{a\in H}\varphi(a)\in\{0,2^h\}.$$

Доказательство. В обозначениях леммы 6

$$W_f(u)=\varphi(u)\,2^{n-h},\qquad l=n-1.$$

Поэтому из леммы 6 следует, что

$$\sum_{a\in H}\varphi(a)\in\{-2^h,0,2^h\}.$$

Но если сумма равна -2^h, то $\sum_{a\in F_2^n\setminus H}\varphi(a)=2^{h+1}$, что невозможно по сказанному выше.

Следующее утверждение также хорошо известно (см., например, теорему 2.89 в [2]).

Лемма 9. *Пусть f — булева функция на F_2^n. Пусть U является линейным подпространством в F_2^n размерности l, а $U^\perp$ — пространство, ортогональное к U в F_2^n. Тогда*

$$\sum_{u\in U}W_f^2(u)=2^l\sum_{v\in U^\perp}\Delta_f(v).$$

Лемма 10. *Пусть f — булева функция на F_2^n, $n\geqslant 1$. Тогда* $\mathrm{wt}(f)$ *нечетно тогда и только тогда, когда* $\deg(f)=n$.

Доказательство очевидно (см., например, следствие 1 в [3]).

Лемма 11. *Пусть f — булева функция на F_2^n, не равная тождественно постоянной. Тогда*

$$2^{n-\deg(f)}\leqslant\mathrm{wt}(f)\leqslant 2^n-2^{n-\deg(f)}.$$

Доказательство очевидно (см., например, лемму 5.6 в [2] или лемму 3 в [3]).

Лемма 12 ([9]). *Пусть f — платовидная булева функция на F_2^n с носителем спектра мощности 4^h. Тогда* $\deg(f)\leqslant h+1$.

Доказательство. Коэффициенты Уолша функции f принимают значения из множества $\{0,\pm 2^{n-h}\}$. Рассмотрим самое длинное слагаемое $x_{i_1}x_{i_2}\dots x_{i_s}$ функции f (если таких слагаемых несколько, берем любое из них). Можно считать, что $s\geqslant 2$, иначе утверждение автоматически является верным. Воспользуемся леммой 6. Возьмем в качестве U линейное подпространство $U=\{x\in F_2^n\mid x_{i_1}=0,\dots,x_{i_s}=0\}$ размерности $l=n-s$, вектор v возьмем нулевым. Тогда ортогональное пространство $U^\perp$ по лемме 10 содержит нечетное число наборов x таких, что $f(x)=1$. Поэтому сумма $\sum_{x\in U^\perp}(-1)^{f(x)}$ при $s\geqslant 2$ не делится на 4. Следовательно, в равенстве

$$\sum_{u\in U}W_f(u)=2^{n-s}\sum_{x\in U^\perp}(-1)^{f(x)}$$

левая часть делится на 2^{n-h}, а правая часть не делится на 2^{n-s+2}. Отсюда следует, что $n-h<n-s+2$, и учитывая целочисленность, получаем, что $s\leqslant h+1$, что и требовалось доказать.

Лемма 13. *Пусть f — платовидная булева функция на F_2^n с носителем спектра мощности 4^h. Пусть H является $(n-1)$-мерным классом смежности в F_2^n. Тогда либо $\sum_{u\in H}|\varphi(u)|=0$, либо $\sum_{u\in H}|\varphi(u)|=4^h$, либо $2^h\leqslant\sum_{u\in H}|\varphi(u)|\leqslant 4^h-2^h$.*

Доказательство. Пусть H — линейное подпространство в F_2^n. Тогда $H^\perp=\{0,v\}$ для некоторого ненулевого $v\in F_2^n$. Очевидно, $\Delta_f(0)=2^n$. По лемме 9

$$4^{n-h}\sum_{u\in H}|\varphi(u)|=2^{n-1}(2^n+\Delta_f(v))=4^n-2^n\,\mathrm{wt}(D_vf).$$

В силу леммы 12 справедливо неравенство $\deg(f)\leqslant h+1$. Функция D_vf является производной функции f, поэтому $\deg(D_vf)\leqslant h$. Если $D_vf\equiv 0$, то $\sum_{u\in H}|\varphi(u)|=4^h$. Если $D_vf\equiv 1$, то $\sum_{u\in H}|\varphi(u)|=0$. Если D_vf не является постоянной, то в силу леммы 11

$$2^{n-h}\leqslant\mathrm{wt}(D_vf)\leqslant 2^n-2^{n-h}.$$

Отсюда, $2^h\leqslant\sum_{u\in H}|\varphi(u)|\leqslant 4^h-2^h$, что и требовалось доказать. Для класса смежности $F_2^n\setminus H$ точно такие же три случая имеют место в силу только что доказанного и равенства Парсеваля.

Лемма 14. *Пусть f_1, f_2 — булевы функции на F_2^n, а f — булева функция на F_2^{n+1}, причем $f(xx_{n+1})=(x_{n+1}+1)f_1(x)+x_{n+1}f_2(x)$. Тогда*

$$W_f(u0)=W_{f_1}(u)+W_{f_2}(u),\qquad W_f(u1)=W_{f_1}(u)-W_{f_2}(u).$$

Эта лемма хорошо известна. Фактически на ее применении основано быстрое преобразование Уолша.

4. Об аффинном ранге платовидных булевых функций с носителем спектра мощности 16

Во всех утверждениях этого раздела предполагается, что f — платовидная булева функция на F_2^n и $|S_f|=16$. В этом случае $c=n-2$. По лемме 7 имеет место один из двух случаев $|T^+|=10$, $|T^-|=6$, или же $|T^+|=6$, $|T^-|=10$. Учитывая, что для всех u справедливо равенство $W_f(u)=-W_{f+1}(u)$, можно без ограничения общности считать, что $|T^+|=10$, $|T^-|=6$, что мы и будем делать в дальнейшем в этом разделе. Таким образом, $|S_f|=16$, $|T^+|=10$, $|T^-|=6$.

Нашей целью является доказательство следующей теоремы.

Теорема 1. *Пусть f является платовидной функцией, $|S_f|=16$. Тогда для аффинного ранга k_a носителя спектра S_f справедливо неравенство $k_a\leqslant 6$.*

Доказательство теоремы 1 будет получено путем доказательства серии лемм.

Предположим, что аффинный ранг носителя спектра S_f равен k_a и аффинный ранг T^- равен k^-. Очевидно, $3\leqslant k^-\leqslant 5$. Легко видеть, что с помощью некоторого аффинного отображения в F_2^n можно вложить наименьший класс смежности, содержащий носитель спектра S_f, в $F_2^{k_a}\otimes(0,\ldots,0)$, так чтобы некоторые k^-+1 наборов из T^- перешли в наборы $(0,0,0,\ldots,0)$, $(1,0,0,\ldots,0)$, $(0,1,0,\ldots,0)$, $\ldots$, $(0,0,\ldots,0,1,0,\ldots,0)$, где в последнем наборе 1 стоит на месте k^-. Заметим, что после такого отображения все наборы

из T^- перейдут в наборы, имеющие только нули во всех компонентах i, $i > k^-$. Отметим, что описанное выше аффинное отображение спектра не является, вообще говоря, аффинным преобразованием функции f, однако нам этого и не нужно. Нам достаточно того, что получившаяся в результате отображения булева функция будет платовидной с тем же наборов значений, принимаемых коэффициентами Уолша, и теми же значениями k_a и k^-. По лемме 3 переменные с $(k_a + 1)$-й по n-ю у получившейся функции будут фиктивными. Отбрасывая их и деля все коэффициенты Уолша на 2^{n-k_a}, мы по леммам 2 и 3 получим платовидную функцию, заданную на $F_2^{k_a}$, с носителем спектра той же мощности 16. Таким образом, без потери общности в оставшейся части этого раздела мы будем рассматривать именно такой носитель спектра.

Лемма 15. *Пусть H является $(k_a - 1)$-мерным классом смежности в $F_2^{k_a}$. Тогда*

$$\sum_{a \in H} \varphi(a) \in \{0, 4\}.$$

Утверждение леммы является частным случаем леммы 8.

Лемма 16 ([5]). *Пусть H является $(k_a - 1)$-мерным классом смежности в $F_2^{k_a}$. Тогда H содержит* 4, 6, 8, 10 *или* 12 *наборов из S_f.*

Доказательство. В силу леммы 15 класс H содержит четное число наборов из S_f. Случаи 2 и 14 невозможны в силу леммы 13. Если H содержит 16 наборов из S_f, то S_f содержится в H; если H содержит 0 наборов из S_f, то S_f содержится в $F_2^{k_a} \setminus H$. Оба последних случая невозможны в силу того, что $F_2^{k_a}$ — наименьший класс смежности, содержащий носитель спектра S_f.

Наша цель — доказать, что $k_a \leqslant 6$. Предположим противное. Пусть $k_a \geqslant 7$. Докажем, что это невозможно.

Образуем матрицу M размера 16×7. В строках M будем записывать слева направо первые 7 компонент наборов из S_f (в случае $k_a > 7$ мы опустим все компоненты после седьмой). В первых 10 строках M запишем наборы из T^+, а в последних 6 строках M запишем наборы из T^-. Левые k^- столбцов M назовем левой частью M, оставшиеся $7 - k^-$ столбцов назовем правой частью M.

$$\left(\begin{array}{ccc|c} & & & \\ & & & \\ & & & \\ & & & \\ & & & \\ & & & \\ & & & \\ & & & \\ & & & \\ & & & \\ \hline & & & \\ & & & \\ & & & \\ & & & \\ & & & \\ & & & \\ 0 & \dots & 0 & \end{array}\right) \quad \begin{matrix} \\ \\ \\ \\ \\ \\ \\ \\ \\ \\ \\ \\ \\ \\ \\ \\ \\ \end{matrix} \quad \left(\begin{array}{c} \\ \\ \\ \\ \\ \\ \\ \\ \\ \\ \\ \\ \\ \\ \\ \\ \\ \mathbf{0} \end{array}\right)$$

Обозначим через γ_i столбцы из левой части M, а через x_i соответствующие этим столбцам переменные. Обозначим через δ_j столбцы из правой части M, а через y_j соответствующие этим столбцам переменные. Обозначим через γ_i^+ и δ_j^+ подстолбцы, содержащие верхние 10 элементов столбцов γ_i и δ_j, соответственно.

Лемма 17. *Для любого множества* $\delta_{j_1}, \ldots, \delta_{j_s}$, $1 \leqslant s \leqslant 7 - k^-$, *различных столбцов из правой части* M *справедливо равенство* $\mathrm{wt}(\delta_{j_1}^+ + \ldots + \delta_{j_s}^+) = 4$.

Доказательство. Положим $H = \{F_2^{k_a} \mid y_{j_1} + \ldots + y_{j_s} = 0\}$. Гиперплоскость H содержит все 6 наборов из T^-, поэтому по лемме 15 гиперплоскость H должна содержать 6 или 10 наборов из T^+. Но если H содержит 10 наборов из T^+, то H содержит S_f. Это невозможно, поскольку k_a есть размерность наименьшего класса смежности, содержащего S_f. Поэтому H содержит 12 наборов из S_f и $F_2^n \setminus H$ содержит в точности 4 набора из S_f.

Лемма 18. *Существует не более трех столбцов, удовлетворяющих условию леммы* 17. *Без потери общности можно выбрать в качестве этих столбцов*

$$\delta_1^+ = (0,0,0,0,0,0,1,1,1,1)^T,$$
$$\delta_2^+ = (0,0,0,0,1,1,0,0,1,1)^T,$$
$$\delta_3^+ = (0,0,0,1,0,1,0,1,0,1)^T.$$

Доказательство. Легко проверить, что наборы δ_1^+, δ_2^+, δ_3^+, указанные в условии, могут быть взяты без потери общности. Предположим, что можно добавить к этому множеству некоторый набор δ_4^+. Для $c_1, c_2, c_3 \in \{0,1\}$ положим

$$\delta^+(c_1,c_2,c_3) = c_1\delta_1^+ + c_2\delta_2^+ + c_3\delta_3^+.$$

Рассмотрим сумму

$$S = \sum_{c_1,c_2,c_3 \in \{0,1\}} d(\delta_4^+, \delta^+(c_1,c_2,c_3)).$$

Заметим, что для любой строки с 4-й по 10-ю в точности 4 из 8 наборов $\delta^+(c_1,c_2,c_3)$ имеют единицу в этой строке. Поэтому $S = 28 + 8w_0 = 32$, где w_0 — это число единиц в δ_4^+ в строках с 1-й по 3-ю. Отсюда следует, что $w_0 = 0{,}5$, но w_0 должно быть целым числом. Это противоречие доказывает лемму 18.

Лемма 19. *Правая часть матрицы* M *содержит не более* 3 *столбцов.*

Утверждение леммы следует из лемм 17 и 18.

Из леммы 19 следует, что случай $k^- = 3$ невозможен. Остались случаи $k^- = 4$ и $k^- = 5$.

Лемма 20. *Пусть* γ_i — *столбец из левой части матрицы* M. *Предположим, что* γ_i *содержит одну единицу и* 5 *нулей в нижних* 6 *строках. Тогда* $\mathrm{wt}(\gamma_i^+) = 5$.

Доказательство. Положим $H = \{F_2^{k_a} \mid x_i = 0\}$. Гиперплоскость H содержит в точности 5 наборов из T^-, поэтому по лемме 15 гиперплоскость H должна содержать 5 или 9 наборов из T^+. Но если H содержит 9 наборов из T^+, то H содержит в точности 14 наборов из S_f. Это невозможно по лемме 16. Отсюда следует, что $\mathrm{wt}(\gamma_i^+) = 5$.

Лемма 21. *Пусть γ_i — столбец из левой части матрицы M. Предположим, что γ_i содержит 2 единицы и 4 нуля в нижних 6 строках. Тогда* $\mathrm{wt}(\gamma_i^+) \in \{2, 6\}$.

Доказательство. Положим $H = \{F_2^{k_a} \mid x_i = 0\}$. Гиперплоскость H содержит в точности 4 набора из T^-, поэтому по лемме 15 гиперплоскость H должна содержать 4 или 8 наборов из T^+. Отсюда следует, что $\mathrm{wt}(\gamma_i^+)$ равно 2 или 6.

Рассмотрим теперь отдельно случаи $k^- = 4$ и $k^- = 5$.

Случай $k^- = 5$. В этом случае правая часть матрицы M содержит два столбца. По лемме 18 без ограничения общности можно предположить, что эти столбцы суть

$$\delta_1 = (0,0,0,0,0,0,1,1,1,1)^T, \qquad \delta_2 = (0,0,0,0,1,1,0,0,1,1)^T.$$

Без ограничения общности можно считать, что матрица M имеет вид

$$\left(\begin{array}{ccccc|cc}
* & * & * & * & * & 0 & 0 \\
* & * & * & * & * & 0 & 0 \\
* & * & * & * & * & 0 & 0 \\
* & * & * & * & * & 0 & 0 \\
* & * & * & * & * & 0 & 1 \\
* & * & * & * & * & 0 & 1 \\
* & * & * & * & * & 1 & 0 \\
* & * & * & * & * & 1 & 0 \\
* & * & * & * & * & 1 & 1 \\
* & * & * & * & * & 1 & 1 \\
\hline
1 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 1 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 1 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 1 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 1 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0
\end{array}\right).$$

По лемме 20 все столбцы γ_i^+, $i = 1,2,3,4,5$, содержат в точности 5 единиц.

Лемма 22. *Пусть $k^- = 5$. Тогда при $1 \leqslant i_1 < i_2 \leqslant 5$ справедливо включение $d(\gamma_{i_1}^+, \gamma_{i_2}^+) \in \{2, 6\}$.*

Доказательство. Положим $H = \{F_2^{k_a} \mid x_{i_1} + x_{i_2} = 0\}$. Гиперплоскость H содержит в точности 4 набора из T^-, поэтому по лемме 15 гиперплоскость H должна содержать 4 или 8 наборов из T^+. Отсюда следует, что

$$d(\gamma_{i_1}^+, \gamma_{i_2}^+) = \mathrm{wt}(\gamma_{i_1}^+ + \gamma_{i_2}^+) \in \{2, 6\}.$$

Лемма 23. *Пусть $k^- = 5$. Тогда для любых $i \in \{1,2,3,4,5\}$ и $c_1, c_2 \in \{0,1\}$*

$$d(\gamma_i^+, c_1\delta_1^+ + c_2\delta_2^+) = 5.$$

Доказательство. Положим $H = \{F_2^{k_a} \mid x_i + c_1y_1 + c_2y_2 = 0\}$. Гиперплоскость H содержит в точности 5 наборов из T^-, поэтому по лемме 15 гиперплоскость H должна содержать 5 или 9 наборов из T^+. Но если H содержит 9 наборов из T^+, то H содержит в точности 14 наборов из S_f. Это невозможно по лемме 16. Отсюда следует, что

$$d(\gamma_i^+, c_1\delta_1^+ + c_2\delta_2^+) = \mathrm{wt}(\gamma_i^+ + c_1\delta_1^+ + c_2\delta_2^+) = 5.$$

Лемма 24. *Пусть* $k^- = 5$. *Тогда для любого* i, $i \in \{1,2,3,4,5\}$, *столбец* γ_i^+ *содержит в точности* 2 *единицы в строках с* 1*-й по* 4*-ю, в точности* 1 *единицу в строках* 5, 6, *в точности* 1 *единицу в строках* 7, 8, *в точности* 1 *единицу в строках* 9, 10.

Доказательство. Если γ_i^+ содержит 0 единиц в строках 9, 10, то из равенства $d(\gamma_i^+, \delta_1^+) = d(\gamma_i^+, \delta_2^+) = 5$ следует, что γ_i^+ содержит только единицы в строках 5, 6, 7, 8. Но в этом случае $d(\gamma_i^+, \delta_1^+ + \delta_2^+) = 1$, что противоречит лемме 23. Если γ_i^+ содержит 2 единицы в строках 9, 10, то из равенства $d(\gamma_i^+, \delta_1^+) = d(\gamma_i^+, \delta_2^+) = 5$ следует, что γ_i^+ содержит только нули в строках 5, 6, 7, 8. Но в этом случае $d(\gamma_i^+, \delta_1^+ + \delta_2^+) = 9$, что противоречит лемме 23. Поэтому γ_i^+ содержит в точности 1 единицу в строках 9, 10. Отсюда следует, что γ_i^+ содержит в точности 1 единицу в строках 7, 8, в точности 1 единицу в строках 5, 6 и в точности 2 единицы в строках с 1-й по 4-ю.

Лемма 25. *Случай* $k^- = 5$ *невозможен.*

Доказательство. Существует ровно 3 пары противоположных наборов длины 4 с в точности 2 единицами. Поэтому в левой части M найдутся два столбца γ_{i_1} и γ_{i_2}, которые либо идентичны, либо противоположны в верхних 4 строках. Пусть γ_{i_3} — еще какой-то столбец в левой части M, $i_1 \neq i_3$, $i_2 \neq i_3$. Тогда из леммы 24 легко видеть, что каждая группа строк (1–4), (5, 6), (7, 8), (9, 10) дает в сумму $S = d(\gamma_{i_1}^+, \gamma_{i_2}^+) + d(\gamma_{i_1}^+, \gamma_{i_3}^+) + d(\gamma_{i_2}^+, \gamma_{i_3}^+)$ вклад, делящийся на 4. Поэтому сумма S делится на 4. С другой стороны, по лемме 22 все слагаемые в S сравнимы с 2 по модулю 4. Поэтому S также сравнима с 2 по модулю 4. Это противоречие доказывает лемму 25.

Таким образом, мы доказали, что случай $k^- = 5$ невозможен.

Случай $k^- = 4$. В этом случае правая часть матрицы M содержит в точности три столбца. По лемме 18 без ограничения общности мы можем предположить, что эти столбцы есть

$$\delta_1 = (0,0,0,0,0,0,1,1,1,1)^T,$$
$$\delta_2 = (0,0,0,0,1,1,0,0,1,1)^T,$$
$$\delta_3 = (0,0,0,1,0,1,0,1,0,1)^T.$$

Без ограничения общности мы можем предположить, что матрица M имеет вид

$$\left(\begin{array}{cccc|ccc}
* & * & * & * & 0 & 0 & 0 \\
* & * & * & * & 0 & 0 & 0 \\
* & * & * & * & 0 & 0 & 0 \\
* & * & * & * & 0 & 0 & 1 \\
* & * & * & * & 0 & 1 & 0 \\
* & * & * & * & 0 & 1 & 1 \\
* & * & * & * & 1 & 0 & 0 \\
* & * & * & * & 1 & 0 & 1 \\
* & * & * & * & 1 & 1 & 0 \\
* & * & * & * & 1 & 1 & 1 \\
\hline
* & * & * & * & 0 & 0 & 0 \\
1 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 1 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 1 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 1 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0
\end{array}\right)$$

Пусть $c_1, c_2, c_3 \in \{0, 1\}$. Положим

$$\delta^+(c_1, c_2, c_3) = c_1\delta_1^+ + c_2\delta_2^+ + c_3\delta_3^+.$$

Лемма 26. *Пусть* $k^- = 4$. *Тогда никакой столбец* γ_i *в левой части матрицы* M *не может иметь ноль в* 11*-й строке.*

Доказательство. Предположим, что некоторый столбец γ_i имеет ноль в 11-й строке. Тогда по лемме 20 имеет место равенство $\mathrm{wt}(\gamma_i^+) = 5$. Тем же путем, что и в доказательстве леммы 23, можно показать, что для любых $c_1, c_2, c_3 \in \{0, 1\}$ справедливо равенство $d(\gamma_i^+, \delta^+(c_1, c_2, c_3)) = 5$. Рассмотрим сумму

$$S = \sum_{c_1, c_2, c_3 \in \{0,1\}} d(\gamma_i^+, \delta^+(c_1, c_2, c_3)).$$

Заметим, что для любой строки с 4-й по 10-ю в точности 4 из 8 наборов $\delta^+(c_1, c_2, c_3)$ имеют единицу в этой строке. Поэтому $S = 28 + 8w_0 = 40$, где w_0 — это число единиц в γ_i в строках с 1-й по 3-ю. Отсюда следует, что $w_0 = 1, 5$, но w_0 должно быть целым числом. Это противоречие доказывает лемму 26.

Из леммы 26 следует, что без ограничения общности матрица M имеет вид

$$\left(\begin{array}{cccc|ccc}
* & * & * & * & 0 & 0 & 0 \\
* & * & * & * & 0 & 0 & 0 \\
* & * & * & * & 0 & 0 & 0 \\
* & * & * & * & 0 & 0 & 1 \\
* & * & * & * & 0 & 1 & 0 \\
* & * & * & * & 0 & 1 & 1 \\
* & * & * & * & 1 & 0 & 0 \\
* & * & * & * & 1 & 0 & 1 \\
* & * & * & * & 1 & 1 & 0 \\
* & * & * & * & 1 & 1 & 1 \\
\hline
1 & 1 & 1 & 1 & 0 & 0 & 0 \\
1 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 1 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 1 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 1 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0
\end{array}\right)$$

Лемма 27. *Пусть* $k^- = 4$. *Тогда* $d(\gamma_{i_1}^+, \gamma_{i_2}^+) \in \{2, 6\}$ *для любых* $1 \leqslant i_1 < i_2 \leqslant 4$.

Доказательство. Положим $H = \{F_2^{k_a} \mid x_{i_1} + x_{i_2} = 0\}$. Гиперплоскость H содержит в точности 4 набора из T^-, поэтому по лемме 15 гиперплоскость H должна содержать 4 или 8 наборов из T^+. Отсюда следует, что $d(\gamma_{i_1}^+, \gamma_{i_2}^+) \in \{2, 6\}$.

Лемма 28. *Пусть* $k^- = 4$. *Тогда любой столбец* γ_i *в левой части матрицы* M *имеет в точности* 2 *единицы в строках с* 1*-й по* 3*-ю и совпадает в строках с* 4*-й по* 10*-ю с вектор-столбцом* $\delta^+(c_1, c_2, c_3)$ *при некоторых* $c_1, c_2, c_3 \in \{0, 1\}$.

Доказательство. В силу леммы 21 справедливо включение $\mathrm{wt}(\gamma_i^+) \in \{2, 6\}$. Тем же способом можно показать, что для любых $c_1, c_2, c_3 \in \{0, 1\}$ справедливо включение $d(\gamma_i^+, \delta^+(c_1, c_2, c_3)) \in \{2, 6\}$.

Предположим, что $\mathrm{wt}(\gamma_i^+) = 2$. Если γ_i^+ не содержит обе свои единицы в строках с 1-й по 3-ю, то легко найти $c_1, c_2, c_3 \in \{0, 1\}$ такие, что набор $\delta^+(c_1, c_2, c_3)$ содержит в точности одну единицу в тех строках, где и γ_i^+ имеет единицу. Тогда будет справедливо равенство $d(\gamma_i^+, \delta^+(c_1, c_2, c_3)) = 4$, что невозможно. Поэтому γ_i^+ содержит обе свои единицы в строках с 1-й по 3-ю и совпадает в строках с 4-й по 10-ю с набором $\delta^+(0, 0, 0)$, то есть имеет требуемый вид.

Теперь предположим, что $\mathrm{wt}(\gamma_i^+) = 6$. Рассмотрим сумму

$$S = \sum_{c_1, c_2, c_3 \in \{0,1\}} d(\gamma_i^+, \delta^+(c_1, c_2, c_3)).$$

Заметим, что для любой строки с 4-й по 10-ю в точности 4 из 8 наборов $\delta^+(c_1, c_2, c_3)$ имеют единицу в этой строке. Поэтому $S = 28 + 8w_0$, где w_0 — число единиц в γ_i в строках с 1-й по 3-ю. Если для любых $c_1, c_2, c_3 \in \{0, 1\}$ справедливо равенство $d(\gamma_i^+, \delta^+(c_1, c_2, c_3)) = 6$, то $S = 48$ и $w_0 = 2, 5$. Но w_0 должно быть целым числом. Поэтому существуют $c_1, c_2, c_3 \in \{0, 1\}$ такие, что $d(\gamma_i^+, \delta^+(c_1, c_2, c_3)) = 2$. Обозначим $\delta^+(c_1, c_2, c_3)$ через δ_0^+. Тогда $\mathrm{wt}(\gamma_i^+ + \delta_0^+) = 2$ и для любых $c_1, c_2, c_3 \in \{0, 1\}$ справедливо включение $d(\gamma_i^+ + \delta_0^+, \delta^+(c_1, c_2, c_3)) \in \{2, 6\}$. Как было указано в начале этого доказательства, набор $\gamma_i^+ + \delta_0^+$ должен иметь в точности 2 единицы в строках с 1-й по 3-ю и одни нули в строках с 4-й по 10-ю. Следовательно, набор γ_i^+ имеет в точности 2 единиц в строках с 1-й по 3 и совпадает с набором δ_0^+ в строках с 4-й по 10-ю.

Лемма 29. *Случай $k^- = 4$ невозможен.*

Доказательство. По лемме 28 все столбцы γ_i в левой части M имеют в точности 2 единицы в строках с 1-й по 3-ю. Левая часть M содержит 4 столбца, поэтому среди них найдутся столбцы γ_{i_1} и γ_{i_2}, $1 \leqslant i_1 < i_2 \leqslant 4$, совпадающие в строках с 1-й по 3-ю. В строках с 4-й по 10-ю столбцы γ_{i_1} и γ_{i_2} совпадают по лемме 28 с некоторыми вектор-столбцами $\delta^+(c_1', c_2', c_3')$ и $\delta^+(c_1'', c_2'', c_3'')$, соответственно. В силу леммы 17 справедливо включение $d(\delta^+(c_1', c_2', c_3'), \delta^+(c_1'', c_2'', c_3'')) \in \{0, 4\}$. Отсюда, $d(\gamma_{i_1}^+, \gamma_{i_2}^+) \in \{0, 4\}$, что противоречит лемме 27.

Все случаи рассмотрены. Теорема 1 доказана.

Таким образом, мы показали, что аффинный ранг платовидных функций с носителем спектра мощности 16 не может принимать никаких значений, кроме 4, 5 и 6. Функции с такими параметрами известны, и их примеры приводились, например, в [5]. Мы не будем здесь приводить примеры. Эти примеры построены в следующем разделе в рамках общей конструкции.

5. Оценки аффинного ранга платовидных функций с произвольной мощностью носителя спектра

Лемма 30. *Пусть существует платовидная функция с носителем спектра мощности 4^h и аффинным рангом k_a. Тогда для любого натурального s, удовлетворяющего неравенствам $k_a + 2 \leqslant s \leqslant 2k_a + 2$, существует платовидная функция с носителем спектра мощности 4^{h+1} и аффинным рангом s.*

Доказательство. Если существует платовидная функция с носителем спектра мощности 4^h и аффинным рангом k_a, то из нее по леммам 2 и 3 аффинным преобразованием спектра и последующим удалением фиктивных переменных можно получить платовидную функцию f на $F_2^{k_a}$ с носителем спектра мощности 4^h, причем так, чтобы спектру функции f принадлежал и нулевой набор, и все наборы веса 1. Рассмотрим функцию $f_1(x_1,\dots,x_s) = f(x_{s-k_a},\dots,x_{s-1}) + x_s$ на F_2^s (переменные $x_1,\dots,x_{s-k_a-1}$ у функции f_1 будут фиктивными). По леммам 3 и 4 функция f_1 снова будет платовидной с той же мощностью носителя, причем ко всем наборам из S_f в носителе спектра S_{f_1} слева припишется $s-k_a-1$ нулей, а справа припишется единица. Линейное подпространство размерности k_a в $F_2^{k_a}$, содержавшее S_f, при переходе к функции f_1 перейдет в класс смежности размерности k_a в F_2^s, содержащий S_{f_1}, но линейным подпространством не являющийся. Поэтому ранг функции f_1 равен k_a+1. Заметим, что носителю спектра S_{f_1} принадлежат следующие наборы: все наборы веса 2 с единицами в компонентах i и s, $i = s-k_a,\dots,s-1$, а также набор веса 1 с единицей в компоненте s. Образуем функцию $f_2(x_1,\dots,x_s) = f_1(x_s,\dots,x_1)$ на F_2^s, переименовав все переменные в обратном порядке. Ясно, что функция f_2 будет обладать свойствами, аналогичными свойствам функции f_1. Носителю спектра S_{f_2} принадлежат в числе прочих следующие наборы: все наборы веса 2 с единицами в компонентах 1 и i, $i = 2,\dots,k_a+1$, а также набор веса 1 с единицей в компоненте 1. Заметим, что во всех наборах из S_{f_1} в первой компоненте ноль, а во всех наборах из S_{f_2} в первой компоненте единица. Поэтому множества S_{f_1} и S_{f_2} в F_2^s не пересекаются.

Рассмотрим функцию

$$f'(x_1,\dots,x_{s+1}) = (x_{s+1}+1)f_1(x_1,\dots,x_s) + x_{s+1}f_2(x_1,\dots,x_s)$$

на F_2^{s+1}. По лемме 14 для любого $u \in F_2^s$

$$W_{f'}(u0) = W_{f_1}(u) + W_{f_2}(u), \qquad W_f(u1) = W_{f_1}(u) - W_{f_2}(u).$$

Как было указано выше, множества S_{f_1} и S_{f_2} в F_2^s не пересекаются. Поэтому каждый набор u из S_{f_1} и S_{f_2} в F_2^s даст ровно два набора $(u,0)$ и $(u,1)$, входящие в носитель спектра $S_{f'}$ функции f' на F_2^{s+1}, причем значения ненулевых коэффициентов Уолша функции f' будут теми же самыми, что и значения ненулевых коэффициентов Уолша функций f_1 и f_2. Таким образом, мощность $S_{f'}$ равна 4^{h+1}, и функция f' также является платовидной функцией.

Из сказанного выше следует, что $S_{f'}$ принадлежат все наборы веса 2 с единицами в компонентах 1 и i, $i = 2,\dots,k_a+1$, все наборы веса 2 с единицами в компонентах i и s, $i = s-k_a,\dots,s-2,s-1,s+1$, а также наборы веса 1 с единицей в компонентах 1 и s. Легко видеть, что ранг вышеуказанной системы наборов равен $s+1$. Поэтому ранг функции f' на F_2^{s+1} равен $s+1$. В то же время для любого набора из $S_{f'}$ сумма значений 1-й и s-й компонент равна 1. Поэтому S_f принадлежит гиперплоскости $H = \{x \in F_2^{s+1} \mid x_1 + x_s = 1\}$, и аффинный ранг функции f' меньше, чем $s+1$, но он не меньше, чем ранг функции f' без единицы, и поэтому аффинный ранг функции f' равен s. Таким образом, требуемая функция построена.

Теорема 2. *Для любого натурального k_a, удовлетворяющего неравенствам $2h \leqslant k_a \leqslant 2^{h+1}-2$, существует платовидная функция с носителем спектра мощности 4^h и аффинным рангом k_a.*

Доказательство. Проведем доказательство индукцией по h. При $h = 1$ величина k_a может быть равна только 2. Такой функцией является, например, бент-функция x_1x_2 на F_2^2 (если мы не хотим считать бент-функцию платовидной функцией, то добавим к ней фиктивную переменную). Если утверждение теоремы верно для h, то его справедливость для $h + 1$ немедленно следует из леммы 30.

Следствие 1. *Аффинный ранг платовидной функции с носителем спектра мощности* 16 *может принимать только значения* 4, 5 *и* 6.

Доказательство. Верхняя оценка $k_a \leqslant 6$ доказана в теореме 1. Нижняя оценка $k_a \geqslant 4$ очевидна. Существование функций с $k_a = 4, 5, 6$ следует из теоремы 2. Заметим, что примеры таких функций даны в [5].

Тривиальной верхней оценкой аффинного ранга k_a платовидной функции с носителем спектра мощности 4^h является $k_a \leqslant 4^h - 1$. Приведем несколько улучшенную оценку.

Теорема 3. *Пусть f является платовидной функцией, $|S_f| = 4^h$. Тогда для аффинного ранга k_a носителя спектра S_f справедлива оценка*

$$k_a \leqslant 2^{2h-1} - 2^{h-1} + h.$$

Будем следовать путем, аналогичным доказательству теоремы 1. Согласно лемме 8 $|T^+|, |T^-| \in \{2^{2h-1} + 2^{h-1}, 2^{2h-1} - 2^{h-1}\}$. Без ограничения общности можно считать, что $|T^+| = 2^{2h-1} + 2^{h-1}$, $|T^-| = 2^{2h-1} - 2^{h-1}$. Предположим, что аффинный ранг носителя спектра S_f равен k_a и аффинный ранг T^- равен k^-. Очевидно, что $k^- \leqslant 2^{2h-1} - 2^{h-1} - 1$. Легко видеть, что с помощью некоторого аффинного отображения в F_2^n можно вложить наименьший класс смежности, содержащий носитель спектра S_f, в $F_2^{k_a} \otimes (0, \ldots, 0)$, где $(0, \ldots, 0)$ — набор из $n - k_a$ нулей, так, чтобы некоторые $k^- + 1$ наборов из T^- перешли в наборы $(0, 0, 0, \ldots, 0)$, $(1, 0, 0, \ldots, 0)$, $(0, 1, 0, \ldots, 0)$, $\ldots$, $(0, 0, \ldots, 0, 1, 0, \ldots, 0)$, где в последнем наборе единица стоит на k^--м месте. Получившаяся в результате отображения булева функция будет платовидной с тем же набором значений, принимаемых коэффициентами Уолша, и теми же значениями k_a и k^-. По лемме 3 переменные с $(k_a + 1)$-й по n-ю у получившейся функции будут фиктивными. Отбрасывая их и деля все коэффициенты Уолша на 2^{n-k_a}, мы по леммам 2 и 3 получим платовидную функцию, заданную на $F_2^{k_a}$, с носителем спектра той же мощности 2^h. Таким образом, без потери общности мы в оставшейся части этого раздела будем рассматривать именно такой носитель спектра.

Образуем матрицу M размера $4^h \times k_a$. В строках M будем записывать слева направо наборы из S_f. В первых $2^{2h-1} + 2^{h-1}$ строках M запишем наборы из T^+, а в последних $2^{2h-1} - 2^{h-1}$ строках M запишем наборы из T^-. Левые k^- столбцов M назовем левой частью M, оставшиеся $k_a - k^-$ столбцов назовем правой частью M. Из того, что $|T^-| = 2^{2h-1} - 2^{h-1}$, следует оценка $k^- \leqslant 2^{2h-1} - 2^{h-1} - 1$.

Обозначим через δ_j столбцы из правой части M, а через y_j соответствующие этим столбцам переменные. Обозначим через δ_j^+ подстолбцы, содержащие верхние $2^{2h-1} + 2^{h-1}$ элементов столбцов δ_j соответственно.

Лемма 31. *Для любого множества $\delta_{j_1}, \ldots, \delta_{j_s}$, $1 \leqslant s \leqslant k_a - k^-$, различных столбцов из правой части M выполняется равенство*

$$\mathrm{wt}(\delta_{j_1}^+ + \ldots + \delta_{j_s}^+) = 2^h.$$

Доказательство. Положим $H = \{F_2^{k_a} \mid y_{j_1} + \ldots + y_{j_s} = 0\}$. Гиперплоскость H содержит все $2^{2h-1} - 2^{h-1}$ наборов из T^-, поэтому по лемме 8 гиперплоскость H должна содержать $2^{2h-1} - 2^{h-1}$ или $2^{2h-1} + 2^{h-1}$ наборов из T^+. Но если H содержит $2^{2h-1} + 2^{h-1}$ наборов из T^+, то H содержит S_f. Это невозможно, поскольку k_a есть размерность наименьшего класса смежности, содержащего S_f. Поэтому H содержит $4^h - 2^h$ наборов из S_f и $F_2^n \setminus H$ содержит в точности 2^h наборов из S_f.

Лемма 32. *Правая часть матрицы M содержит не более $h + 1$ столбцов.*

Доказательство. Пусть правая часть матрицы M содержит m столбцов $\delta_1, \ldots, \delta_m$. Для $c_1, \ldots, c_m \in \{0, 1\}$ положим $\delta^+(c_1, \ldots, c_m) = c_1\delta_1^+ \cdots + c_m\delta_m^+$. Рассмотрим сумму

$$S = \sum_{c_1,\ldots,c_m \in \{0,1\}} \mathrm{wt}(\delta^+(c_1, \ldots, c_m)).$$

Каждое слагаемое в S, кроме слагаемого, соответствующего нулевому набору, равно 2^h по лемме 31. Обозначим через r число строк среди верхних $2^{2h-1} + 2^{h-1}$ строк матрицы M, содержащих хотя бы одну единицу в правой части матрицы M. Заметим, что если строка в верхней части матрицы M содержит хотя бы одну такую единицу, то в точности 2^{m-1} из $2^m - 1$ ненулевых наборов $\delta^+(c_1, \ldots, c_3)$ имеют единицу в этой строке. Поэтому $S = 2^h(2^m - 1) = r2^{m-1}$. Отсюда $r = 2^{h+1} - 2^{h-m+1}$. В силу целочисленности r справедливо неравенство $m \leqslant h + 1$, что и требовалось доказать.

Утверждение теоремы 3 немедленно следует из структуры матрицы M и леммы 32. При $h = 2$ оценка теоремы 3 не достигается. Осмелимся выдвинуть гипотезу.

Гипотеза. Для любого натурального h максимально возможный аффинный ранг платовидной функции с носителем спектра мощности 4^h равен $2^{h+1} - 2$.

Список литературы

1. Кузнецов Ю. В., О носителях платовидных функций. В сб.: *Материалы VIII Международного семинара «Дискретная математика и ее приложения».* МГУ, Москва, 2004, с. 424–426.
2. Логачев О. А., Сальников А. А., Ященко В. В., *Булевы функции в теории кодирования и криптографии.* МЦНМО, Москва, 2004.
3. Тарапников Ю. В., О корреляционно-иммунных и устойчивых булевых функциях. *Матем. вопросы кибернетики* (2002) **11**, 91–148.
4. Тарапников Ю. В., О платовидных устойчивых функциях. В сб.: *Материалы VIII Международного семинара «Дискретная математика и ее приложения».* МГУ, Москва, 2004, с. 431–435.
5. Carlet C., Charpin P., Cubic Boolean functions with highest resiliency. In: *Proc. 2004 IEEE Intern. Symposium on Inform. Theory,* 2004, p. 497.
6. Carlet C., Sarkar P., Spectral domain analysis of correlation immune and resilient Boolean functions. *Finite Fields Appl.* (2002) **8**, 120–130.
7. Kasami T., Tokura N., Azumi S., On the weight enumeration of weights less than $2.5d$ of Reed–Muller codes. *Information and Control* (1976) **30** (**4**), 380–395.
8. Pei D., Qin W., The correlation of a Boolean function with its variables. *Lecture Notes Computer Sci.* (2000) **1977**, 1–8.
9. Zheng Y., Zhang X.-M., Plateaued functions. *Lecture Notes Computer Sci.* (1999) **1726**, 284–300.

Статья поступила 27.01.2005.