2013 Теоретические основы прикладной дискретной математики №2(20)

DOI 10.17223/20710410/20/2

УДК 510.52

НИЖНЯЯ И ВЕРХНЯЯ ОЦЕНКИ ПОРЯДКА АФФИННОСТИ ПРЕОБРАЗОВАНИЙ ПРОСТРАНСТВ БУЛЕВЫХ ВЕКТОРОВ

С. П. Горшков*, А. В. Двинянинов**

*Институт криптографии, связи и информатики, г. Москва, Россия

**Лаборатория ТВП, г. Москва, Россия

E-mail: spg54@bk.ru

Находятся нижняя и верхняя оценки порядка аффинности множества всех преобразований n-мерного пространства булевых векторов. Результаты работы могут быть использованы при оценке сложности одного метода решения систем булевых уравнений.

Ключевые слова: *преобразование пространства булевых векторов, аффинное отображение, сложность решения систем булевых уравнений.*

Будем использовать следующие обозначения:
$\mathbb{N}$ — множество натуральных чисел;
V_n — n-мерное пространство булевых векторов, $n \in \mathbb{N}$;
Φ_n — множество всех отображений $V_n \to V_n$;
$0_n^{\downarrow} = (\underbrace{0, \ldots, 0}_{n})^T$;
$\lfloor c \rfloor$ — целая часть числа c,
если действительные функции $g(n), h(n)$ определены для всех натуральных $n \in \mathbb{N}$ и существует такое $n_0 \in \mathbb{N}$, что для всех $n \geqslant n_0$ выполняется $g(n) < h(n)$, то будем записывать

$$g(n) \tilde{<} h(n).$$

Всякое отображение $F \in \Phi_n$ записывается системой координатных булевых функций $F = \{(f_1(x_1, \ldots, x_n), \ldots, f_n(x_1, \ldots, x_n)\}$.

Отображение F называется *линейным* (*аффинным*), если все его координатные функции линейны (аффинны).

Введём ещё некоторые определения, которые заимствованы из [1, с. 163–164].

Отображение $F \in \Phi_n$ *аффинно* на множестве M, где $M \subseteq V_n$, если найдётся аффинное отображение $A \in \Phi_n$, такое, что $F(\alpha) = A(\alpha)$ при любом $\alpha \in M$. Тогда отображение A назовём *линеаризующим F на множестве M*.

Пусть $M_1, \ldots, M_r$ — разбиение множества V_n, $A_1, \ldots, A_r$ — отображения, линеаризующие F на множествах $M_1, \ldots, M_r$ соответственно. При этом r назовём *порядком разбиения* множества V_n, линеаризующего F. *Порядком аффинности отображения F* (обозначим его $\operatorname{ard} F$) назовём наименьший из порядков разбиений множества V_n, линеаризующих F.

Прикладное значение введённых определений состоит в следующем. Предположим, что необходимо решить систему булевых уравнений вида

$$\begin{cases} f_1(x_1, \ldots, x_n) = \gamma_1, \\ \ldots \\ f_n(x_1, \ldots, x_n) = \gamma_n, \end{cases} \tag{1}$$

где $\{f_1, \ldots, f_n\}$ — координатные функции отображения F. Систему (1) будем записывать также в виде

$$F(x) = \gamma, \tag{2}$$

где $x = (x_1, \ldots, x_n)$, $\gamma = \begin{pmatrix} \gamma_1 \\ \ldots \\ \gamma_n \end{pmatrix}$.

Пусть $A_1, \ldots, A_{\operatorname{ard} F}$ — отображения, линеаризующие F. Тогда для решения (1) (или (2)) достаточно решить следующее множество линейных булевых систем уравнений:

$$A_i(x) = \gamma, \quad i = 1, \ldots, \operatorname{ard} F,$$

и полученные решения проверить по исходной системе (2). Ясно, что общее число решаемых линейных систем уравнений равно $\operatorname{ard} F$.

Дальнейшие определения введены авторами данной работы.

Пусть

$$\operatorname{ard} \Phi_n = \max_{F \in \Phi_n} \operatorname{ard} F.$$

Величину $\operatorname{ard} \Phi_n$ назовём *порядком аффинности* Φ_n. Параметр $\operatorname{ard} \Phi_n$ оценивает сверху число решаемых линейных систем при любой системе (2).

Теорема 1. При $n \geqslant 2$ для порядка аффинности справедлива нижняя оценка

$$\operatorname{ard} \Phi_n > \frac{2^n}{n^2}.$$

Доказательство. Нетрудно показать, что число аффинных отображений $V_n \to V_n$ равно $2^{n(n+1)}$. Пусть

$$A_1, \ldots, A_{2^{n(n+1)}} \tag{3}$$

— все аффинные отображения из Φ_n. Обозначим символом u порядок аффинности $\operatorname{ard} \Phi_n$. Тогда для каждого $F \in \Phi_n$ найдутся разбиение V_n на блоки $M_1, \ldots, M_k$, $k \leqslant u$, и аффинные отображения $A_{i_1}, \ldots, A_{i_k}$, такие, что A_{i_j} линеаризует F на M_j, $j \in \{1, \ldots, k\}$. Если считать, что некоторые блоки M_l могут быть пустыми, то можно полагать, что все линеаризующие наборы $A_{i_1}, \ldots, A_{i_k}$ состоят из u элементов.

Оценим сверху число h всех отображений из Φ_n, которые могут быть линеаризованы наборами из не более чем u аффинных отображений:

$$h \leqslant \binom{2^{n(n+1)}}{u} \cdot u^{2^n}. \tag{4}$$

Первый сомножитель в (4) — число вариантов, которыми можем выбрать $A_{i_1}, \ldots, A_{i_u}$ из всех аффинных отображений (3). Если набор $A_{i_1}, \ldots, A_{i_u}$ задан, то он линеаризует не более чем u^{2^n} отображений $F \in \Phi_n$, поскольку каждый элемент $F(\alpha)$, $\alpha \in V_n$, может принимать не более u значений.

Нетрудно видеть, что

$$h < 2^{un(n+1)} \cdot u^{2^n}. \tag{5}$$

Логарифмируя обе части неравенства (5) по основанию 2, получим

$$\log_2 h < un(n+1) + 2^n \cdot \log_2 u. \tag{6}$$

Предположим, что выполнено неравенство

$$\operatorname{ard}\Phi_n \leqslant \frac{2^n}{n^2}.$$

Тогда из (6) следует, что

$$\log_2 h < 2^n\left(n + \frac{n(n+1)}{n^2} - 2\log_2 n\right). \tag{7}$$

При $n \geqslant 2$ из неравенства (7) следует

$$\log_2 h < n \cdot 2^n. \tag{8}$$

Поскольку u — порядок аффинности Φ_n, то $h = |\Phi_n| = 2^{n\cdot 2^n}$,

$$\log_2 h = n \cdot 2^n. \tag{9}$$

Из полученного противоречия (8) и (9) вытекает, что $\operatorname{ard}\Phi_n > \dfrac{2^n}{n^2}$. ■

Найдём верхнюю оценку для $\operatorname{ard}\Phi_n$. Получение этой оценки предварим несколькими достаточно простыми утверждениями.

Легко показать, что справедлива следующая лемма.

Лемма 1. Пусть $\{(\beta^{(1)}, \delta^{(1)}), \ldots, (\beta^{(m)}, \delta^{(m)})\}$ — пары векторов из V_n, причём $m \leqslant n$, а векторы $\{\beta^{(1)}, \ldots, \beta^{(m)}\}$ линейно независимы. Тогда найдётся линейное отображение $L \in \Phi_n$, такое, что

$$L(\beta^{(i)}) = \delta^{(i)}, \quad i = 1, \ldots, m.$$

Лемма 2. Пусть $M \subseteq V_n$, $|M| \geqslant 2^k$, где $k \in \{0, \ldots, n-1\}$, все векторы в M ненулевые. Тогда в M найдётся $k+1$ линейно независимых векторов.

Доказательство. Предположим противное, что максимальная (точнее, одна из максимальных) система линейно независимых векторов состоит из $t < k+1$ векторов. Пусть это векторы $\varphi^{(1)}, \ldots, \varphi^{(t)}$. Символом M' обозначим линейное пространство векторов с базисом $\varphi^{(1)}, \ldots, \varphi^{(t)}$, $M'' = M' \setminus \{0_n^{\downarrow}\}$. Ясно, что $M'' \supseteq M$, то есть $|M''| \geqslant 2^k$. С другой стороны, $|M''| = 2^t - 1 \leqslant 2^k - 1 < 2^k$. Из полученного противоречия вытекает справедливость леммы. ■

Теорема 2. При $n \geqslant 2$ для порядка аффинности справедлива следующая верхняя оценка:

$$\operatorname{ard}\Phi_n \leqslant \frac{2^n}{n} \sum_{i=1}^{n-1} 2^{-i} \cdot \frac{n}{n-i}.$$

Доказательство. Пусть F — произвольное, но фиксированное отображение из Φ_n. Линеаризовывать отображение F будем следующим образом: все ненулевые векторы V_n разобьём на непересекающиеся группы линейно независимых векторов (число этих групп обозначим r). Выделим одну группу (пусть это будут векторы $\{\alpha_1^{(1)}, \ldots, \alpha_n^{(1)}\}$) и линеаризуем значение F на этих векторах некоторым аффинным преобразованием так, чтобы одновременно линеаризовалось значение $F(0_n^{\downarrow})$.

Согласно доказательству леммы 1, можем подобрать такое линейное отображение $L \in \Phi_n$, что $L(\alpha_i^{(1)}) = F(\alpha_i^{(1)}) \oplus F(0_n^{\downarrow})$, $i = 1, \ldots, n$. Тогда аффинное отображение

$L(x^{\downarrow}) \oplus F(0_n^{\downarrow})$ линеаризует F на векторах $\{\alpha_1^{(1)}, \ldots, \alpha_n^{(1)}, 0_n^{\downarrow}\}$. На каждой из остальных $r-1$ групп векторов, согласно лемме 1, отображение F можем линеаризовать соответствующим линейным отображением. Из этих рассуждений вытекает, что $\operatorname{ard} \Phi_n \leqslant r$.

Оценим значение r. Рассмотрим множество ненулевых векторов $V_n \setminus \{0_n^{\downarrow}\}$, при этом если $n \geqslant 1$, то $\left|V_n \setminus \{0_n^{\downarrow}\}\right| = 2^n - 1 \geqslant 2^{n-1}$. Согласно лемме 2, из множества $V_n \setminus \{0_n^{\downarrow}\}$ можем выбрать n линейно независимых векторов $\alpha_1^{(1)}, \ldots, \alpha_n^{(1)}$. Если для оставшегося множества $M' = V_n \setminus \{\alpha_1^{(1)}, \ldots, \alpha_n^{(1)}, 0_n^{\downarrow}\}$ будет выполняться $|M'| \geqslant 2^{n-1}$, то выберем ещё n линейно независимых векторов $\alpha_1^{(2)}, \ldots, \alpha_n^{(2)}$, и так далее, пока для оставшегося множества $M'' = V_n \setminus (\{\alpha_1^{(1)}, \ldots, \alpha_n^{(1)}, 0_n^{\downarrow}\} \cup \{\alpha_1^{(2)}, \ldots, \alpha_n^{(2)}\} \cup \ldots \cup \{\alpha_1^{(r_{n-1})}, \ldots, \alpha_n^{(r_{n-1})}\})$ не будет впервые выполняться $|M''| < 2^{n-1}$. Таким образом сформируем r_{n-1} групп линейно независимых векторов из n векторов, причём r_{n-1} такое, что

$$r_{n-1} = \frac{2^n - 1 - (2^{n-1} - q_{n-1})}{n} = \frac{2^{n-1} - 1 + q_{n-1}}{n},$$

где $q_{n-1} = n$, если $(2^{n-1} - 1)/n$ — целое; и $q_{n-1} \in \{1, \ldots, n-1\}$ таково, что $(2^{n-1} - 1 + {}+q_{n-1})/n$ целое, если $(2^{n-1} - 1)/n$ — дробное.

Далее формируем группы из $n-1$ линейно независимых векторов. Таких групп сформируем

$$r_{n-2} = \frac{2^{n-1} - q_{n-1} - (2^{n-2} - q_{n-2})}{n-1} = \frac{2^{n-2} - q_{n-1} + q_{n-2}}{n-1},$$

где $q_{n-2} \in \{1, \ldots, n-1\}$, и так далее.

Нетрудно видеть, что можно сформировать

$$r_i = \frac{2^{i+1} - q_{i+1} - (2^i - q_i)}{i+1} = \frac{2^i - q_{i+1} + q_i}{i+1}$$

групп из $i+1$ линейно независимых векторов, где $q_i \in \{1, \ldots, i+1\}$, $i \in 0, \ldots, n-2$.

В целом получаем

$$\begin{aligned}
r = r_{n-1} + r_{n-2} + \ldots + r_0 &= \frac{2^{n-1} - 1 + q_{n-1}}{n} + \frac{2^{n-2} - q_{n-1} + q_{n-2}}{n-1} + r_{n-3} + \ldots + r_0 = \\
&= \frac{1}{n-1}\left(\frac{n-1}{n}(2^{n-1} - 1 + q_{n-1}) + 2^{n-2} - q_{n-1} + q_{n-2}\right) + r_{n-3} + \ldots + r_0 = \\
&= \frac{1}{n-1}\left(2^{n-1} - \frac{2^{n-1}}{n} + 2^{n-2} + q_{n-2} - \left(\frac{q_{n-1}}{n} + \frac{n-1}{n}\right)\right) + r_{n-3} + \ldots + r_0 \leqslant \\
&\leqslant \frac{2^{n-1}}{n-1} + \frac{2^{n-2} - 1 + q_{n-2}}{n-1} + r_{n-3} + r_{n-4} + \ldots + r_0 = \\
&= \frac{2^{n-1}}{n-1} + \left(\frac{2^{n-2} - 1 + q_{n-2}}{n-1} + \frac{2^{n-3} - q_{n-2} + q_{n-3}}{n-2}\right) + r_{n-4} + \ldots + r_0 \leqslant \\
&\leqslant \frac{2^{n-1}}{n-1} + \frac{2^{n-2}}{n-2} + \left(\frac{2^{n-3} - 1 + q_{n-3}}{n-2} + \frac{2^{n-4} - q_{n-3} + q_{n-4}}{n-3}\right) + r_{n-5} + \ldots + r_0 \leqslant \\
&\leqslant \frac{2^{n-1}}{n-1} + \frac{2^{n-2}}{n-2} + \ldots + \frac{2^2}{2} + \left(\frac{2^1 - 1 + q_1}{2} + \frac{2^0 - q_1 + q_0}{1}\right) = \\
&= \frac{2^{n-1}}{n-1} + \frac{2^{n-2}}{n-2} + \ldots + \frac{2^2}{2} + \frac{2^1}{1} = \frac{2^n}{n}\left(2^{-1}\frac{n}{n-1} + 2^{-2}\frac{n}{n-2} + \ldots + 2^{-(n-1)}\frac{n}{1}\right).
\end{aligned}$$

Теорема доказана. ■

Лемма 3. Справедливо соотношение

$$\lim_{n\to\infty}\sum_{i=1}^{n-1}2^{-i}\frac{n}{n-i}=1.$$

Доказательство. Оцениваемую сумму разобьём на две подсуммы:

$$\sum_{i=1}^{n-1}2^{-i}\frac{n}{n-i}=\sum_{i=1}^{\lfloor 3\log_2 n\rfloor}2^{-i}\frac{n}{n-i}+\sum_{i=\lfloor 3\log_2 n\rfloor+1}^{n-1}2^{-i}\frac{n}{n-i}. \tag{10}$$

Первую сумму в левой части (10) обозначим S_1, вторую — S_2. Нетрудно видеть, что

$$\sum_{i=1}^{\lfloor 3\log_2 n\rfloor}2^{-i}<S_1<\frac{n}{n-\lfloor 3\log_2 n\rfloor}\sum_{i=1}^{\lfloor 3\log_2 n\rfloor}2^{-i}. \tag{11}$$

Верхняя и нижняя оценки в (11) при $n\to\infty$ стремятся к 1.

Для S_2 верны оценки $0<S_2<n\cdot 2^{-\lfloor 3\log_2 n\rfloor}\leqslant n^{-1}$, то есть $\lim\limits_{n\to\infty}S_2=0$. Отсюда и из (11) следует справедливость леммы. ■

Следствие 1. Для порядка аффинности Φ_n выполняется следующее асимптотическое неравенство:

$$\operatorname{ard}\Phi_n\tilde{<}1{,}01\cdot\frac{2^n}{n}.$$

Справедливость следствия 1 непосредственно вытекает из теоремы 2 и леммы 3.

ЛИТЕРАТУРА

1. *Фомичёв В. М.* Дискретная математика и криптология. М.: Диалог-МИФИ, 2003. 397 с.