

Как показывает следующий пример, несмотря на то, что операции параллельной композиции регулярных и ω -регулярных языков очень похожи, методы решения уравнений для регулярных языков не могут быть напрямую применены при решении уравнений для ω -регулярных языков. Рассмотрим ω -регулярные языки $C = ((i_1 + i_2)(u_1 + u_2))^*(i_1u_1)^\omega + (i_2u_2)^\omega$ и $S = (i_1 + i_2)^*i_1^\omega$ (где верхний индекс ω означает бесконечную конкатенацию слова) и их множества конечных префиксов $Init(C) = ((i_1 + i_2)(u_1 + u_2))^*(i_1u_1)^* + (i_2u_2)^*$ и $Init(S) = (i_1 + i_2)^*i_1^* = (i_1 + i_2)^*$. Наибольшим решением уравнения $Init(C) \diamond X = Init(S)$ является регулярный язык $Sol = (u_1 + u_2)^*$. Как обычно, определим предел регулярного языка L как ω -регулярный язык, содержащий каждое бесконечное слово, множество конечных префиксов которого содержится в L . Взяв предел регулярного языка Sol , получим $\lim(Sol) = (u_1 + u_2)^\omega$. Однако ω -язык $(u_1 + u_2)^\omega$ не является решением уравнения $C \diamond X = S$, так как $(u_1 + u_2)^\omega$ содержит слово u_2^ω , расширение которого на алфавит I содержит слово $(i_2u_2)^\omega$, а значит, пересечение $C \cap (\lim(Sol))_{\uparrow I}$ будет содержать слово $(i_2u_2)^\omega$, ограничением которого на алфавит I будет слово i_2^ω , не содержащееся в S . Однако можно показать, что формула наибольшего решения для ω -регулярных языков имеет такой же вид, как и при решении уравнения для регулярных языков, т. е. наибольшее решение уравнения $C \diamond X = S$ есть ω -язык $C \diamond \overline{S}$. В нашем примере наибольшим решением уравнения является ω -регулярный язык $(u_1 + u_2)^\omega \setminus u_2^\omega$.

Бушков В. Г. выражает благодарность фонду Бортника за финансовую поддержку по проекту 8858, Евтушенко Н. В. выражает благодарность РФФИ за финансовую поддержку по проекту 06-08-89500.

ЛИТЕРАТУРА

1. Buffalov S., El-Fakih K., Yevtushenko N., et al. Progressive solutions for a parallel automata equation // FORTE'03. Berlin: Springer, 2003. P. 367–382.
2. Yevtushenko N. V., Villa T., Brayton R. K., et al. Sequential synthesis by language equation solving // International Workshop on Logic Synthesis. June, 2000.
3. Глушков В. М. Синтез цифровых автоматов. М.: Физматгиз, 1962. 476 с.
4. Mukund M. Finite-state automata on infinite inputs // The 6th National Seminar on Theoretical Computer Science. Banasthali, Rajasthan, India, 1996. V. 2.

УДК 519.651

БЛИЗОСТЬ К КЛАССУ МОНОМИАЛЬНЫХ АППРОКСИМАЦИЙ ПРИВЕДЕННОГО ПРЕДСТАВЛЕНИЯ БУЛЕВОЙ ФУНКЦИИ В ЗАВИСИМОСТИ ОТ ВЫБОРА БАЗИСА, В КОТОРОМ ОНО ЗАДАНО

А. В. Иванов

Пусть $\mathbb{F}_2$ — поле из двух элементов с единицей e , $\mathbb{F}_{2^n}$ — его расширение степени $n \in \mathbb{N}$, $\text{tr}_1^n(\alpha) = \sum_{k=0}^{n-1} \alpha^{2^k}$ — функция след из $\mathbb{F}_{2^n}$ в $\mathbb{F}_2$. Для целых t_1, t_2 через (t_1, t_2) будем обозначать их неотрицательный наибольший общий делитель.

Основные результаты работы получены с использованием представления булевых функций от n переменных в виде многочленов над полем $\mathbb{F}_{2^n}$, принимающих значения в поле $\mathbb{F}_2$ (так называемого «приведенного представления»). Описание механизма получения подобного представления можно найти в [1].

Пусть $\varphi(x_0, x_1, \dots, x_{n-1})$ — булева функция от n переменных, $(\varepsilon_0, \varepsilon_1, \dots, \varepsilon_{n-1})$ — базис векторного пространства $(\mathbb{F}_{2^n})_{\mathbb{F}_2}$. Как следует из результатов работы [1], существует многочлен $\Phi(x)$ над полем $\mathbb{F}_{2^n}$ такой, что для каждого $x \in \mathbb{F}_{2^n}$ выполнено $\text{tr}_1^n(\Phi(x)) = \varphi(x_0, x_1, \dots, x_{n-1})$, где $x = \sum_{j=0}^{n-1} x_j \cdot \varepsilon_j$. Для каждой линейной булевой функции ее приведенное представление имеет вид $\text{tr}_1^n(\alpha x)$ для некоторого $\alpha \in \mathbb{F}_{2^n}$.

Нас будет интересовать удаленность (в смысле расстояния Хемминга между векторами значений) булевой функции от некоторого множества функций — класса приближений. В качестве показателя близости приближающей функции $G(x) : \mathbb{F}_{2^n} \rightarrow \mathbb{F}_2$ к исходной функции $F(x)$ будем использовать величину $\Delta(F, G) = \sum_{x \in \mathbb{F}_{2^n}} (-1)^{F(x)+G(x)}$.

Если функция $G(x)$ линейная, то $\Delta(F, G)$ есть соответствующий коэффициент Уолша — Адамара функции $F(x)$ (см., например, [2]). Для коэффициентов Уолша — Адамара произвольной функции справедлива оценка

$$\max \{ |\Delta(F, \text{tr}_1^n(\alpha x))| : \alpha \in \mathbb{F}_{2^n} \} \geq 2^{\frac{n}{2}}. \quad (1)$$

Функции, для которых неравенство (1) обращается в равенство, существуют только для четных значений n и носят название бент-функций.

Функция принадлежит классу мономиальных функций, если ее приведенное представление имеет вид $L_\alpha^{(\delta)}(x) = \text{tr}_1^n(\alpha \cdot x^\delta)$ для некоторых $\alpha \in \mathbb{F}_{2^n}$, $\delta \in \mathbb{N}$ ([1, 3]). Из оценки (1) следует справедливость неравенства

$$\max \{ |\Delta(F, L_\alpha^{(\delta)})| : \delta \in \mathbb{N}, (\delta, 2^n - 1) = 1, \alpha \in \mathbb{F}_{2^n} \} \geq 2^{\frac{n}{2}}. \quad (2)$$

Функции, для которых достигается оценка (2), называют гипербент-функциями [1, 3]. Класс бент-функций инвариантен относительно невырожденной линейной замены переменных (см., например, [2]). В этом смысле основной результат данной работы демонстрирует отличие свойств бент- и гипербент-функций.

Рассмотрим вопрос о том, как влияет выбор базиса, в котором строится приведенное представление булевой функции, на его (представления) свойство «быть гипербент-функцией». Для $d \in \overline{1, 2^n - 2}$ через π_d обозначим отображение на $\mathbb{F}_{2^n}$ такое, что для любого $x \in \mathbb{F}_{2^n}$ выполнено $\pi_d(x) = x^d$. Для различных $d', d'' \in \overline{1, 2^n - 2}$, каждое из которых взаимно просто с $2^n - 1$, отображения $\pi_{d'}$ и $\pi_{d''}$ задают различные подстановки на $\mathbb{F}_{2^n}$. Кроме того, для любых $d', d'' \in \overline{1, 2^n - 2}$ выполнено $\pi_{d'}\pi_{d''} = \pi_{d'd'' \bmod (2^n - 1)}$. Положим $\mathcal{D} = \{\pi_d \mid (d, 2^n - 1) = 1\}$ и заметим, что это множество с операцией умножения является абелевой группой. Зафиксируем базис $(\mathbb{F}_{2^n})_{\mathbb{F}_2}$. Пусть отображение T ставит в соответствие каждому элементу $\mathbb{F}_{2^n}$ строку координат его разложения по данному базису, задавая биективное соответствие между $\mathbb{F}_{2^n}$ и $(\mathbb{F}_2)^n$. Через χ обозначим индуцируемый отображением T изоморфизм групп $S(\mathbb{F}_{2^n} \setminus \{0\})$ и $S((\mathbb{F}_2)^n \setminus \{\vec{0}\})$.

Лемма 1. Пусть $n > 4$, τ — нечетная подстановка на множестве $\mathbb{F}_{2^n} \setminus \{0\}$, такая, что τ^2 не принадлежит $\chi^{-1}(\text{GL}(n, 2))$. Тогда τ в объединении с $\chi^{-1}(\text{GL}(n, 2))$ в их действии на $\mathbb{F}_{2^n} \setminus \{0\}$ порождает группу $S(\mathbb{F}_{2^n} \setminus \{0\})$.

Утверждение 1. Для $n > 4$ существует $d \in \overline{1, 2^n - 2}$, такое, что π_d в объединении с $\chi^{-1}(\text{GL}(n, 2))$ в их действии на $\mathbb{F}_{2^n} \setminus \{0\}$ порождает группу $S(\mathbb{F}_{2^n} \setminus \{0\})$.

Следствие 1. Для $n > 4$ группа $\mathcal{D}$ в объединении с $\chi^{-1}(\text{GL}(n, 2))$ в их действии на $\mathbb{F}_{2^n} \setminus \{0\}$ порождает группу $S(\mathbb{F}_{2^n} \setminus \{0\})$.

Теорема 1.

1) Для любой бент-функции от 4 переменных существуют базисы $(\varepsilon_0^{(1)}, \varepsilon_1^{(1)}, \varepsilon_2^{(1)}, \varepsilon_3^{(1)})$ и $(\varepsilon_0^{(2)}, \varepsilon_1^{(2)}, \varepsilon_2^{(2)}, \varepsilon_3^{(2)})$ векторного пространства $(\mathbb{F}_{2^4})_{\mathbb{F}_2}$, такие, что приведенное представление данной функции в первом базисе является, а во втором не является гипербент-функцией.

2) Для любого четного $n > 4$ существуют функции от n переменных, для каждой из которых можно найти два базиса векторного пространства $(\mathbb{F}_{2^n})_{\mathbb{F}_2}$, таких, что приведенное представление функции в первом базисе является, а во втором не является гипербент-функцией.

ЛИТЕРАТУРА

1. Кузьмин А. С., Марков В. Т., Нечаев А. А., Шишков А. Б. Приближение булевых функций мономиальными // Дискретная математика. 2006. Т. 18. № 1. С. 9–29.
2. Логачев О. А., Сальников А. А., Яценко В. В. Булевы функции в теории кодирования и криптологии. М.: МНЦМО, 2004. 470 с.
3. Youssef A. M., Gong G. Hyper-bent functions // Proceedings of Advances in Cryptology, EUROCRYPT'2001. Lect. Notes in Comp. Sci. New York: Springer Verlag, 2001. V. 2045. P. 406–419.

УДК 519.7

СВОЙСТВА БЕНТ-ФУНКЦИЙ, НАХОДЯЩИХСЯ НА МИНИМАЛЬНОМ РАССТОЯНИИ ДРУГ ОТ ДРУГА

Н. А. Коломеец, А. В. Павлов, А. А. Левин

Здесь и далее пусть n — четное натуральное число. Обозначим:

- E^n — множество двоичных векторов длины n ;
- $\mathcal{F}_n$ — множество всех булевых функций от n переменных;
- нелинейность — расстояние Хэмминга до класса аффинных функций;
- бент-функции — булевы функции от четного числа переменных, обладающие максимальной нелинейностью;
- $\mathfrak{B}_n$ — множество всех бент-функций от n переменных;
- $D(f, g) = \{x \in E^n \mid f(x) \neq g(x)\}$, где $f, g \in \mathcal{F}_n$;
- f аффинна на D , если для некоторых $w_0 \in E^n, c \in E$ и для любого $x \in D$ выполняется $f(x) = w_0 \cdot x \oplus c$, где $f \in \mathcal{F}_n, D \subseteq E^n$;
- $d(A)$ — минимальное расстояние между двумя функциями в классе $A \subseteq \mathcal{F}_n$;
- U — многообразие в E^n , т. е. $U = x_0 \oplus L$, где L — подпространство в $E^n, x_0 \in E^n$.

Имеет место нижняя оценка на расстояние между бент-функциями.

Теорема 1. Справедливо $d(\mathfrak{B}_n) \geq 2^{n/2}$.

Следующая теорема дает критерий расположения функций на расстоянии $2^{n/2}$.

Теорема 2. Пусть $f, g \in \mathcal{F}_n$, f — бент-функция, $|D(f, g)| = 2^{n/2}$. Тогда g — бент-функция тогда и только тогда, когда множество $D(f, g)$ — линейное многообразие размерности $n/2$ и f на нем аффинна.

Следствие 1. Минимальное расстояние в классе бент-функций равно $2^{n/2}$.

Определим следующие множества.