

которого асимптотически минимальна, а мощность решётки удовлетворяет неравенству

$$|\mathbb{N}_m^2| > 2^{n-2 \log_2 n(1+\varepsilon_n)},$$

где $\varepsilon_n \rightarrow 0$ при $n \rightarrow \infty$.

Рассмотренные свойства вложений обобщаются на произвольные метрические пространства, хотя выше для простоты сформулированы для графов с обычной метрикой.

Найдены также оптимальные кодирования решёток, определяемые их 2-интервальными вложениями, специальный случай которых для малых значений параметров рассмотрен в [3].

ЛИТЕРАТУРА

1. Евдокимов А. А. Метрические свойства вложений и коды, сохраняющие расстояния // Труды Института математики СО РАН. Новосибирск: Наука, 1988. Т. 10. С. 116–132.
2. Евдокимов А. А. Локально изометрические вложения графов и свойство продолжения метрики // Сиб. журн. исслед. операций. 1994. Т. 1. № 1. С. 5–12.
3. Евдокимов А. А. Вложения графов в n -мерный булев куб и интервальное кодирование табло // Вестник Томского государственного университета. Приложение. 2006. № 17. С. 15–19.

УДК 519.7

КОЛИЧЕСТВО БЕНТ-ФУНКЦИЙ НА МИНИМАЛЬНОМ РАССТОЯНИИ ОТ КВАДРАТИЧНОЙ БЕНТ-ФУНКЦИИ¹

Н. А. Коломеец

Бент-функции — это булевы функции, максимально удаленные от класса аффинных функций. Впервые бент-функции были рассмотрены О. Ротхаусом [1]. Бент-функции имеют огромное число приложений: в криптографии, теории кодирования, теории информации. Тем не менее для них до сих пор существует много нерешенных проблем. Одна из наиболее важных проблем — описание всех бент-функций, в частности нахождение конструкций для бент-функций.

В работе рассматривается получение бент-функций на минимальном расстоянии от квадратичной бент-функции. В [2] показано, что две бент-функции от $2k$ переменных находятся на минимальном расстоянии тогда и только тогда, когда они отличаются на аффинном подпространстве размерности k и обе функции на нем аффинны. В данной работе описываются все бент-функции на минимальном расстоянии от квадратичной бент-функции $(x_1x_{k+1} \oplus x_2x_{k+2} \oplus \dots \oplus x_kx_{2k})$, а также подсчитывается число бент-функций на минимальном расстоянии от произвольной квадратичной бент-функции.

Пусть A — произвольная матрица; через $a_{(i)}$ будем обозначать её i -й столбец. Будем описывать линейные подпространства с помощью базисов Гаусса — Жордана. Отметим, что в наших обозначениях базисные векторы являются *столбцами* базисной матрицы.

Определение 1. Пусть G — матрица с k столбцами, образованная векторами $u_{(1)}, \dots, u_{(k)}$ длины n . Через $l(u_{(i)})$ обозначим $\min\{j : u_{(i)j} \neq 0\}$. Матрица G является *базисом Гаусса — Жордана* подпространства размерности k в пространстве размерности n , если выполняются следующие условия:

¹Работа выполнена при финансовой поддержке РФФИ (проект № 11-01-00997) и ФЦП «Научные и научно-педагогические кадры инновационной России» на 2009–2013 гг. (гос. контракт № 02.740.11.0362).

- 1) если $i_1 < i_2$, то $l(u_{(i_1)}) < l(u_{(i_2)})$;
- 2) если $i_1 \neq i_2$, то $u_{(i_1)l(u_{(i_2)})} = 0$.

В этом случае через $l(G)$ обозначим множество $\{l(u_{(1)}), \dots, l(u_{(k)})\}$. Все строки матрицы G с номерами из множества $l(G)$ будем называть *ведущими строками*. Все остальные строки будем называть *неведущими*. Через L_G обозначим подпространство с базисом $u_{(1)}, \dots, u_{(k)}$. Заметим, что столбцы матрицы G действительно являются базисными векторами пространства L_G , а матрицу G^T называют также *редуцированной ступенчатой матрицей*.

Известно, что любое линейное подпространство имеет ровно один базис Гаусса — Жордана.

Введем определение *допустимого* базиса Гаусса — Жордана. Пусть базис Гаусса — Жордана G для подпространства размерности k в пространстве размерности $2k$ имеет следующий вид:

$$\left(\begin{array}{c|c} A & 0 \\ \hline Z & Y \end{array} \right),$$

где матрица A размера $k \times t$ не содержит нулевых столбцов, а матрица Y имеет размер $k \times (k - t)$. Заметим, что матрицы A и Y являются базисами Гаусса — Жордана. Пусть $L_Y = L_A^\perp$. Удалим из матрицы A все строки с номерами из $l(Y)$. Пусть все оставшиеся строки образуют матрицу A' . Аналогичные действия проделаем и с матрицей Z : удалим все строки с номерами из $l(Y)$ и образуем из оставшихся строк матрицу Z' . Заметим, что все удаленные из матрицы Z строки являются нулевыми, так как G является базисом Гаусса — Жордана. Таким образом, получили матрицы A' и Z' размера $t \times t$. Базис Гаусса — Жордана G назовем *допустимым*, если $t \leq 1$ или элементы матрицы Z' при $t \geq 2$ являются решениями следующей системы уравнений с матрицей размера $(t(t - 1)/2) \times t^2$:

$$\begin{pmatrix} a'_{(2)}{}^T & a'_{(1)}{}^T & 0 & 0 & \dots & 0 \\ \dots & & & & & \\ a'_{(t)}{}^T & 0 & 0 & \dots & 0 & a'_{(1)}{}^T \\ \dots & & & & & \\ 0 & a'_{(3)}{}^T & a'_{(2)}{}^T & 0 & \dots & 0 \\ \dots & & & & & \\ 0 & a'_{(t)}{}^T & 0 & \dots & 0 & a'_{(2)}{}^T \\ \dots & & & & & \\ 0 & 0 & 0 & \dots & a'_{(t)}{}^T & a'_{(t-1)}{}^T \end{pmatrix} \cdot \begin{pmatrix} z'_{(1)} \\ z'_{(2)} \\ \vdots \\ z'_{(t)} \end{pmatrix} = 0.$$

Следующая теорема описывает все бент-функции на минимальном расстоянии от квадратичной бент-функции.

Теорема 1. Для бент-функции $f(x) = x_1x_{k+1} \oplus x_2x_{k+2} \oplus \dots \oplus x_kx_{2k}$ функция $f(x) \oplus \text{Ind}_L(x)$ является бент-функцией на минимальном расстоянии от $f(x)$ тогда и только тогда, когда множество L является линейным подпространством с допустимым базисом Гаусса — Жордана или сдвигом такого подпространства.

Теорема 2. Любая квадратичная бент-функция от $2k$ переменных имеет ровно $2^k(2^1 + 1) \cdot \dots \cdot (2^k + 1)$ бент-функций на минимальном расстоянии 2^k .

Заметим, что число бент-функций от $2k$ переменных на минимальном расстоянии от заданной бент-функции можно оценить сверху числом 2^{k^2+2k} (это оценка сверху числа всевозможных аффинных подпространств размерности k), а число бент-функций на минимальном расстоянии от квадратичной бент-функции асимптотически равно $C \cdot 2^{k(k+3)/2}$. Таким образом, число бент-функций на минимальном расстоянии от квадратичной бент-функции больше, чем корень из этой тривиальной верхней оценки.

ЛИТЕРАТУРА

1. Rothaus O. On bent functions // J. Combin. Theory. Ser. A. 1976. No. 20. P. 300–305.
2. Коломеец Н. А., Павлов А. В. Свойства бент-функций, находящихся на минимальном расстоянии друг от друга // Прикладная дискретная математика. 2009. № 4. С. 5–21.

УДК 519.7

О СТАТИСТИЧЕСКОЙ НЕЗАВИСИМОСТИ СУПЕРПОЗИЦИИ БУЛЕВЫХ ФУНКЦИЙ¹

О. Л. Колчева, И. А. Панкратова

Интерес к статистической независимости булевой функции от подмножества аргументов возникает в связи с построением статистических аналогов функции [1], которые, в свою очередь, используются в линейном криптоанализе [2, 3].

Будем говорить, что булева функция f статистически не зависит от подмножества U своих аргументов, если для любой её подфункции f' , полученной фиксированием значений всех переменных в U , имеет место $\Pr[f' = 1] = \Pr[f = 1]$; или, что то же самое, $w(f') = w(f)/2^{|U|}$, где $w(f)$ — вес функции f . В частности, для статистического аналога $\varphi(x, y, k) = 0$ функции шифрования $F(x, k)$, где x, k, y — переменные со значениями в множествах открытых текстов, ключей и шифртекстов соответственно, условие статистической независимости функции $\varphi_F(x, k) = \varphi(x, F(x, k), k)$ от переменных в x является необходимым для того, чтобы вероятность выполнения уравнения $\varphi_F = 0$ сохранялась при подстановке в это уравнение любого значения x при равновероятном выборе k [1].

Требование статистической независимости функции от конкретного подмножества аргументов более слабое, чем условие корреляционной иммунности [4]: функция является корреляционно-иммунной порядка m , если и только если она статистически не зависит от любого m -элементного подмножества своих аргументов.

В [1] сформулирован тест статистической независимости: функция $f(x, y)$, где x, y — переменные со значениями в $(\mathbb{Z}_2)^n$ и $(\mathbb{Z}_2)^m$ соответственно, статистически не зависит от булевых переменных в x , если и только если $\hat{f}(u, 0^m) = 0$ для любого ненулевого вектора $u \in (\mathbb{Z}_2)^n$. Здесь $\hat{f}$ — преобразование Уолша — Адамара функции f ; 0^m — m -компонентный нулевой вектор.

Сформулируем некоторые простейшие свойства статистической независимости.

- 1) Если функция имеет s линейных переменных, то она статистически не зависит от любого $(s - 1)$ -элементного подмножества своих аргументов.
- 2) Если функция статистически не зависит от U , то она статистически не зависит от любого подмножества U .

¹Работа выполнена в рамках реализации ФЦП «Научные и научно-педагогические кадры инновационной России» на 2009–2013 гг. (гос. контракт № П1010).