

ЛИТЕРАТУРА

1. Kuribayashi A. and Komiya K. On Weierstrass Points of non-hyperelliptic compact Riemann surfaces of genus three // Hiroshima Math J. 1977. No. 7. P. 743–768.
2. Stichtenoth H. Algebraic Function Fields and Codes. Berlin; Heidelberg; New York: Springer Verlag, 1993.

УДК 519.174

КОДИРОВАНИЕ КОНЕЧНОЙ ЦЕЛОЧИСЛЕННОЙ РЕШЕТКИ
В КЛАССЕ ОТОБРАЖЕНИЙ ОГРАНИЧЕННОГО ИСКАЖЕНИЯ¹

А. А. Евдокимов

Пусть ε и δ — натуральные числа из области определения метрик ρ_G и ρ_H , заданных на множествах вершин $V(G)$ и $V(H)$ графов G и H , а $S_k(v)$ — шар с центром в точке $v \in V(G)$ и радиусом k . Скажем, что отображение $f : G \rightarrow H$, действующее из $V(G)$ в $V(H)$, обладает свойством $\langle \varepsilon, \delta \rangle$ -ограниченного искажения, если

$$f(S_\delta(v)) \subseteq (S_\varepsilon(f(v)))$$

для любой вершины $v \in V(G)$.

Скажем, что отображение $f : G \rightarrow H$ сохраняет $\langle \varepsilon, \delta \rangle$ -отделимость, если

$$\text{Im } f \cap S_\varepsilon(f(v)) \subseteq f(S_\delta(v)).$$

Вложение $f : G \rightarrow H$ графа G в H называем $\langle \varepsilon, \delta \rangle$ -вложением, если f обладает свойством $\langle \varepsilon, \delta \rangle$ -ограниченного искажения и сохраняет $\langle \varepsilon, \delta \rangle$ -отделимость.

В отличие от аналогичных определений в [1–3], здесь выбраны $\langle \varepsilon, \delta \rangle$ -язык и окрестности (шары), чтобы подчеркнуть общность с определениями классической математики. При «малых» значениях параметров $\langle \varepsilon, \delta \rangle$ -вложение означает, что оно связные части не разрывает, а «далёкие» не становятся «близкими». Первое является дискретным аналогом непрерывного отображения, а вместе со вторым свойством — аналогом гомеоморфного вложения.

Пусть $N_m = \{0, 1, \dots, m-1\}$ и $N_m^2 = N_m \times N_m$ — двумерная целочисленная решетка размера $m \times m$ с расстоянием

$$\rho_{N^2}(u, v) = |x_1 - x_2| + |y_1 - y_2|$$

между ее вершинами (узлами решетки) $u = (x_1, y_1)$ и $v = (x_2, y_2)$.

В [3] описана конструкция $\langle 3, 2 \rangle$ -вложения целочисленной решетки N_{14}^2 (плоского решётчатого табло) в булев гиперкуб I^{10} и показано, что наибольший размер решетки N_m^2 для любого $\langle 3, 2 \rangle$ -вложения $f : N_m^2 \rightarrow I^{10}$ равен 14×14 ; $\langle 3, 2 \rangle$ -вложение сохраняет все расстояния, не превосходящие 3, а вершины, находящиеся на расстоянии больше 1, не могут оказаться на расстоянии 0 или 1. Таким образом, изометричное 3×3 окно в классе обратимых кодирований двоичными словами длины 10 возможно для квадратного табло из 196 ячеек размера 1×1 .

Теорема 1. Существует и эффективно строится конструкция $\langle 4, 3 \rangle$ -вложения $f : N_m^2 \rightarrow I^n$ целочисленной решётки размера $m \times m$ в булев куб I^n , избыточность

¹Работа поддержана проектами РФФИ № 09-01-00070 и 11-01-00997 и программой фундаментальных исследований Отделения математических наук РАН.

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).