

MSC 11J68

ОПТИМИЗАЦИЯ ГРАНИЦ ОТКЛОНЕНИЙ ДЛЯ ДВУМЕРНЫХ МНОЖЕСТВ ОГРАНИЧЕННОГО ОСТАТКА

А.А. Абросимова, Д.А. Блинов

Владимирский государственный университет им. А.Г. и Н.Г. Столетовых,
пр. Строителей, 11, Владимир, 600024, Россия,
e-mail: AlbinaAbrosimowa@yandex.ru, mr.DmBlinov@mail.ru

Аннотация. Рассматривается оптимизация границ отклонений для двумерных множеств ограниченного остатка, построенных на основе выпуклых гексагональных разверток.

Ключевые слова: развертка тора, множества ограниченного остатка, границы отклонений, метрики трехмерного пространства, оптимизация границ.

Введение. В работе [1] были построены двумерные множества ограниченного остатка или ВР-множества на основе выпуклых гексагональных разверток тора (рис. 1).

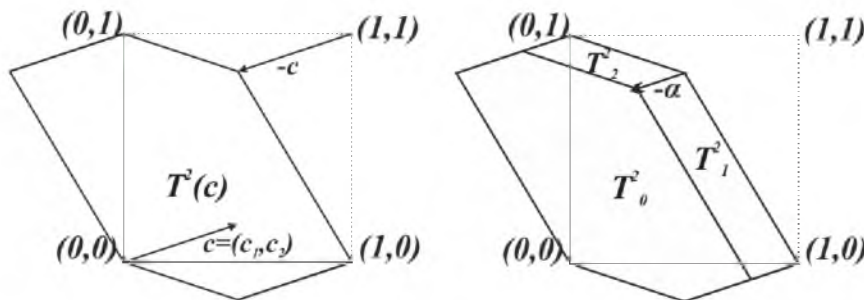


Рис. 1.

Форма развертки задается параметром $c = (c_1, c_2)$. Для каждой области $T_k^2, k = 0, 1, 2$, изображенной на рис. 1, введем считающие функции

$$r_k(i) = \#\{j : S_\alpha^j(0) \in T_k^2, 0 \leq j < i\}, \quad (1)$$

как количество попаданий точек в каждую из областей T_k^2 , и отклонения считающих функций

$$\delta_k(i) = r_k(i) - is_k$$

от ожидаемой величины is_k , где s_k — площади областей T_k^2 , и они соответственно равны $s_0 = 1 - \alpha_1 - \alpha_2 = \alpha_0, s_1 = \alpha_1, s_2 = \alpha_2$.



В работе [1] также была доказана теорема о точных границах остаточных членов этих множеств. В работе [2] было проведено обобщение на случай невыпуклых шестиугольников (рис. 2), а также доказана следующая теорема.

Теорема 1. Пусть дан сдвиг тора S_α на вектор α , и α — иррациональный, т.е. числа $\alpha_1, \alpha_2, 1$ линейно независимы над \mathbb{Z} , пусть тор \mathbb{T}^2 разбит на области \mathbb{T}_k^2 : $\mathbb{T}^2 = \mathbb{T}_0^2 \sqcup \mathbb{T}_1^2 \sqcup \mathbb{T}_2^2$. Тогда для отклонений выполняются точные неравенства:

$$\begin{aligned} 0 \leq \delta_0(i, 0) \leq 2 - c_1 - c_2 & \quad \text{для } c_i \geq 0, c_1 + c_2 \leq 1; \\ 1 - c_1 - c_2 \leq \delta_0(i, 0) \leq 1 & \quad \text{для } c_1 + c_2 > 1; \\ -1 \leq \delta_1(i, 0) \leq c_1; \\ -1 \leq \delta_2(i, 0) \leq c_2. \end{aligned} \tag{2}$$

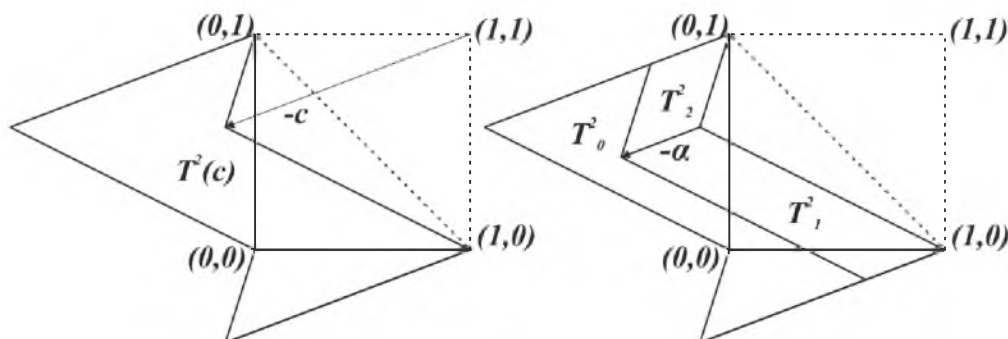


Рис. 2.

В настоящей работе приведен общий метод построения двумерных множеств ограниченного остатка на основе гексагональных разверток и получены точные границы отклонений для этих множеств. Для приложений необходимо чтобы границы всех отклонений $\delta_k(i)$ одновременно были бы как можно меньше, например, для построения сбалансированных слов, которые в свою очередь широко используются в криптографии. Поэтому в работе получена оптимизация границ отклонений.

1. Двумерные множества ограниченного остатка. Для построения двумерных множеств ограниченного остатка выберем точку $c = (c_1, c_2)$, такую что $c = (c_1, c_2) \in C = C_{con} \cup C_{ncon1} \cup C_{ncon2}$, где область C изображена на рис. 3.

Отложим вектор $-c$ от точек с координатами $(0, 1), (1, 1), (1, 0)$ и соединим полученные точки. Построенный шестиугольник $T^2(c)$ будет иметь вершины с координатами $(0, 0), (1 - c_1, -c_2), (1, 0), (-c_1, -c_2), (0, 1), (-c_1, 1 - c_2)$. Причем, шестиугольник $T^2(c)$ будет выпуклым, если точка $c \in C_{con}$, и невыпуклым, если $c \in C_{ncon} = C_{ncon1} \cup C_{ncon2}$.

Рассмотрим два случая.

1. В случае $c \in C_{con} \cup C_{ncon1}$ отложим вектор $-\alpha = (-\alpha_1, -\alpha_2)$, где $\alpha = tc$, от точек $(0, 1), (-c_1, 1 - c_2), (1, 0)$ и получим разбиение шестиугольника $T^2(c)$ на множества ограниченного остатка $T_k^2, k = 0, 1, 2$. Выбор параметра t зависит от выбора области, которой принадлежит точка c . Если $c \in C_{con}$, то параметр t будет изменяться в границах



от 0 до 1, если $c \in C_{ncon1}$, то $0 \leq t \leq (c_1 + c_2)^{-1}$. В этом случае относительно границ отклонений доказана теорема 1.

2. В случае $c \in C_{ncon2}$ вместо вектора α будем использовать вектор $\tilde{\alpha} = (\tilde{\alpha}_1, \tilde{\alpha}_2 = t\tilde{c})$, $\tilde{c} \equiv c \pmod{\mathbb{Z}^2}$, где \mathbb{Z}^2 – квадратная решетка, заданная базисом с векторами $e_1 = (1, 0)$, $e_2 = (0, 1)$. Если $c_1 > 0, c_2 < 0$, то $\tilde{c} = e_2 - c = (-c_1, 1 - c_2)$ и $0 \leq t \leq (c_1 + c_2)/c_1$, если же $c_1 < 0, c_2 > 0$, то $\tilde{c} = e_1 - c = (1 - c_1, -c_2)$ и $0 \leq t \leq (1 - c_2)/(1 - c_1 - c_2)$.

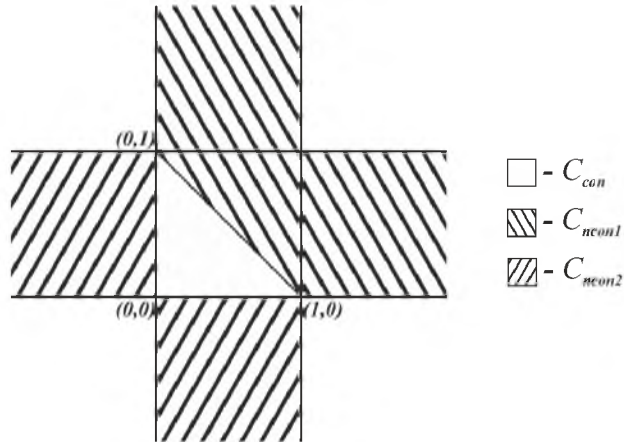


Рис. 3.

В случае 2 справедлива теорема аналогичная теореме 1.

Теорема 2. Пусть дан сдвиг тора $S_{\tilde{\alpha}}$ на вектор $\tilde{\alpha}$, и $\tilde{\alpha}$ – иррациональное число и пусть тор \mathbb{T}^2 разбит на области \mathbb{T}_k^2 : $\mathbb{T}^2 = \mathbb{T}_0^2 \sqcup \mathbb{T}_1^2 \sqcup \mathbb{T}_2^2$. Тогда для отклонений выполняются точные неравенства:

$$0 \leq \delta_0(i) \leq 1 - c_2, \quad -c_1 \leq \delta_1(i) \leq 1, \quad c_1 + c_2 - 2 \leq \delta_2(i) \leq 0 \tag{3}$$

для $c \in C_{ncon2}, c_1 > 0, c_2 < 0$;

$$0 \leq \delta_0(i) \leq 1 - c_1, \quad c_1 + c_2 - 2 \leq \delta_1(i) \leq 0, \quad -c_2 \leq \delta_2(i) \leq 1. \tag{4}$$

для $c \in C_{ncon2}, c_1 < 0, c_2 > 0$.

2. Оптимизация границ отклонений. Геометрическая интерпретация неравенств (1), (2), (3) заключается в том, что границы отклонений определяются границами шестиугольника $T^2(c)$, которые в свою очередь зависят от выбора параметра $c = (c_1, c_2)$ из области S . Для приложений необходимо, чтобы границы всех трех отклонений $\delta_k(i), k = 0, 1, 2$, были как можно меньше. Но, если уменьшать границы хотя бы одного из отклонений, то неминуемо будут расширяться границы других отклонений, поэтому для оптимизации границ отклонений $\delta_k(i)$ необходим параметр, связывающий все три отклонения. В связи с этим будем рассматривать отклонения $\delta_k(i)$ как координаты трехмерного вектора $x = (x_1, x_2, x_3)$, соответственно

$$\delta_1(i) = x_1, \quad \delta_2(i) = x_2, \quad \delta_0(i) = x_3. \tag{5}$$



В качестве величины, связывающей все три отклонения будем рассматривать метрику трехмерного пространства, которую зададим в виде

$$d_\theta(x) = (|x_1|^\theta + |x_2|^\theta + |x_3|^\theta)^{\frac{1}{\theta}}, \quad (6)$$

где $1 \leq \theta \leq \infty$, а $|\cdot|$ обозначает абсолютную величину.

Наиболее интересными для приложений являются случаи $\theta = 1, 2, \infty$.

1. Если взять $\theta = 1$, выражение (6) для метрики трехмерного пространства примет вид

$$d_1(x) = |x_1| + |x_2| + |x_3|. \quad (7)$$

Эта метрика используется в кристаллографии при изучении роста кристаллов.

2. При $\theta = 2$, получим привычную нам евклидову метрику

$$d_2(x) = \sqrt{|x_1|^2 + |x_2|^2 + |x_3|^2}. \quad (8)$$

3. При $\theta = \infty$, получим

$$d_\infty(x) = \max(|x_1|, |x_2|, |x_3|). \quad (9)$$

Рассмотрим суммарное векторное отклонение

$$\delta(i) = i\alpha + r_1(i)e_1 + r_2(i)e_2$$

для отклонений $\delta_k(i)$, $k = 0, 1, 2$, определенное в [2], где e_1, e_2 — векторы базиса квадратной решетки \mathbb{Z}^2 , а $r_1(i), r_2(i)$ — считающие функции, определенные в (1).

Назовем

$$\Delta_\theta(c) = \sup_{i \in \mathbb{N}} d_\theta(\delta(i)) \quad (10)$$

верхней границей векторного отклонения $\delta(i)$ в метрике $d_\theta(x)$ при фиксированном c . Тогда

$$\Delta_\theta = \inf_{c \in X} \Delta_\theta(c) \quad (11)$$

нижняя граница $\Delta_\theta(c)$ берется по всем c из некоторой области X .

Рассмотрим оптимизацию границ отклонений во всех трех метриках (7), (8), (9) для случая, когда развертка тора представляет собой выпуклый шестиугольник (рис. 1), то есть $c \in C_{con}$, где

$$C_{con} = \{c = (c_1, c_2) \in \mathbb{R}^2; c_i \geq 0, c_1 + c_2 \leq 1\}. \quad (12)$$

Для нижней границы $\Delta_\theta(c)$ по всем c из области C_{con} справедлива следующая теорема.

Теорема 3. Пусть отклонения δ_k , $k = 0, 1, 2$ задают трехмерный вектор x , и пусть его длина $d_\theta(x)$ определена в (6). Тогда, если $c \in C_{con}$, где C_{con} определена в (12), для Δ_θ справедливы следующие равенства:

$$\Delta_1 = 2, \quad (13)$$



$$\Delta_2 = \sqrt{3/2}, \tag{14}$$

$$\Delta_\infty = 1. \tag{15}$$

где Δ_θ определены в (10). Равенства (12) и (14) достигаются при $c_1 + c_2 = 1$, равенство (13) – при $c = (1/2, 1/2)$.

□ Приведем общую схему доказательства для всех трех равенств (12), (13), (14). Определим верхнюю границу $\Delta_\theta(c)$, определенную в (9), векторного отклонения $\delta(i)$, и, изменяя параметр c , постараемся сделать ее как можно меньше. Так как все три метрики (7), (8), (9) выпуклые, то для определения $\Delta_\theta(c)$, достаточно найти длины $d(\delta(i))$ векторного отклонения $\delta(i)$ для всех вершин шестиугольника $T^2(c)$, а затем выбрать наибольшее значение.

Для $\theta = 1$, получим набор значений, представленный в таблице 1.

	Координаты вершины	Значение $d(\delta(i))$
1.	(0, 0)	0
2.	(1 - c ₁ , -c ₂)	2(1 - c ₁)
3.	(1, 0)	2
4.	(1 - c ₁ , 1 - c ₂)	4 - 2(c ₁ + c ₂)
5.	(0, 1)	2
6.	(-c ₁ , 1 - c ₂)	2(1 - c ₂)

Таблица 1.

Тогда $\Delta_1(c) = 4 - 2(c_1 + c_2)$ и при $c_1 + c_2 = 1$ получим нижнюю границу $\Delta_1 = 2$. Равенство (12) доказано.

Для $\theta = 2$, получим значения, представленные в таблице 2.

	Координаты вершины	Значение $d(\delta(i))$
1.	(0, 0)	0
2.	(1 - c ₁ , -c ₂)	$(2(1 - 2c_1 - c_2 + c_1c_2 + c_1^2 + c_2^2))^{\frac{1}{2}}$
3.	(1, 0)	$\sqrt{2}$
4.	(1 - c ₁ , 1 - c ₂)	$(2(3 - 3c_1 - 3c_2 + c_1c_2 + c_1^2 + c_2^2))^{\frac{1}{2}}$
5.	(0, 1)	$\sqrt{2}$
6.	(-c ₁ , 1 - c ₂)	$(2(1 - c_1 - 2c_2 + c_1c_2 + c_1^2 + c_2^2))^{\frac{1}{2}}$

Таблица 2.

Тогда $\Delta_2(c) = (2(3 - 3c_1 - 3c_2 + c_1c_2 + c_1^2 + c_2^2))^{\frac{1}{2}}$, и $\Delta_2(1/2, 1/2) = \sqrt{3/2}$. Равенство (13) доказано.

В случае $\theta = \infty$, получим



	Координаты вершины	Значение $d_\infty(\delta(i))$
1.	(0, 0)	0
2.	(1 - c_1 , - c_2)	1 - c_1
3.	(1, 0)	1
4.	(1 - c_1 , 1 - c_2)	2 - c_1 - c_2
5.	(0, 1)	1
6.	(- c_1 , 1 - c_2)	1 - c_2

Таблица 3.

Тогда $\Delta_\infty(c) = 2 - c_1 - c_2$, и при $c_1 + c_2 = 1$ получим значение нижней границы $\Delta_\infty = 1$. ■

Рассмотрим теперь случай $c \in C_{ncon2}$. Имеет место следующая теорема.

Теорема 4. Пусть отклонения $\delta_k, k = 0, 1, 2$ задают трехмерный вектор x , и пусть его длина $d_\theta(x)$ определена в (6). Тогда, если $c \in C_{ncon2}$ (рис. 3), для Δ_θ справедливы следующие равенства:

$$\Delta_1 = 2, \quad (16)$$

$$\Delta_2 = \sqrt{2}, \quad (17)$$

$$\Delta_\infty = 1. \quad (18)$$

где Δ_θ определены в (10).

□ Доказательство аналогично доказательству теоремы 3. Все верхние границы отклонений $\Delta_\theta(c)$ такие же как и в случае выпуклого шестиугольника, единственное отличие заключается в том, что все нижние значения Δ_θ достигаются в двух точках (1, 0) и (0, 1). ■

Более сложной является задача в случае $c \in C_{ncon1}$.

Теорема 5. Пусть отклонения $\delta_k, k = 0, 1, 2$ задают трехмерный вектор x , и пусть его длина $d_\theta(x)$ определена в (6). Тогда, если $c \in C_{ncon1}$ (рис. 3), для Δ_θ справедливы следующие равенства:

$$\Delta_1 = 0, \quad (19)$$

$$\Delta_2 = \sqrt{2/3}, \quad (20)$$

$$\begin{aligned} \Delta_\infty &= 1/2, \quad \text{для } c \in C_1 \text{ и } c \in C_2; \\ \Delta_\infty &= 2/3, \quad \text{для } c \in C_3. \end{aligned} \quad (21)$$

где Δ_θ определены в (10).

□ Наиболее простым является доказательство равенства (18). Пользуясь таблицей 1 и сравнивая полученные в ней значения, можно заключить, что в области C_1 (рис. 4) $\Delta_1(c) = 2(1 - c_2)$ и в этой области $\Delta_1 = 0$ при $c_2 = 1$.

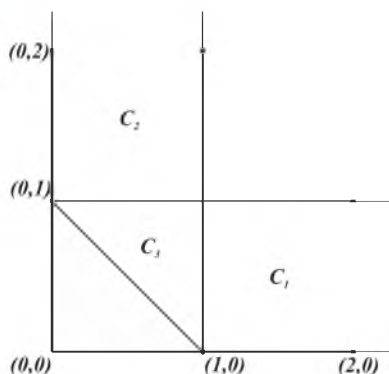


Рис. 4.

Область C_2 симметрична области C_1 и для нее $\Delta_1(c) = 2(1 - c_1)$ и $\Delta_1 = 0$ при $c_1 = 1$. Для области C_3 , получим $\Delta_1(c) = 4 - 2(c_1 - c_2)$ и $\Delta_1 = 0$ в точке $(1, 1)$.

Теперь пользуясь результатами таблицы 2 для метрики d_2 получим, что если $c_1 + 2c_2 < 2$ и $2c_1 + c_2 < 2$ (рис. 5), то $\Delta_2(c) = (2(3 - 3c_1 - 3c_2 + c_1c_2 + c_1^2 + c_2^2))^{\frac{1}{2}}$ и $\Delta_2 = \sqrt{2/3}$ в точке $(2/3, 2/3)$. В этой же точке достигаются нижние границы $\Delta_2(c)$ для двух других случаев.

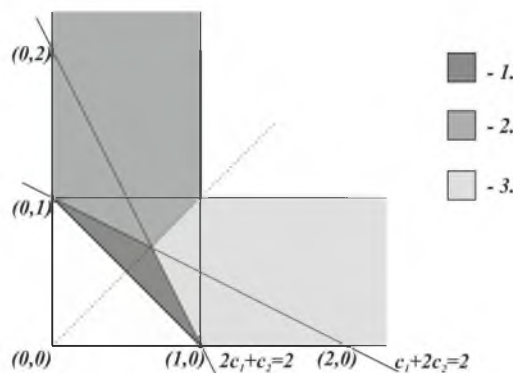


Рис. 5.

Если $c_1 + 2c_2 > 2$ и $c_2 > c_1$ то $\Delta_2(c) = (2(1 - 2c_1 - c_2 + c_1c_2 + c_1^2 + c_2^2))^{\frac{1}{2}}$ и $\Delta_2 = \sqrt{2/3}$. Если же $2c_1 + c_2 > 2$ и $c_1 > c_2$, то $\Delta_2(c) = (2(1 - c_1 - 2c_2 + c_1c_2 + c_1^2 + c_2^2))^{\frac{1}{2}}$ и $\Delta_2 = \sqrt{2/3}$. Таким образом, выражение (19) также доказано.

Осталось доказать равенство (21). Составим для этого новую таблицу

	Координаты вершины	Значение $ x_1 $	Значение $ x_2 $	Значение $ x_3 $
1.	$(0, 0)$	0	0	0
2.	$(1 - c_1, -c_2)$	$ 1 - c_1 $	$ -c_2 $	$ c_1 + c_2 - 1 $
3.	$(1, 0)$	1	0	1
4.	$(1 - c_1, 1 - c_2)$	$ 1 - c_1 $	$ 1 - c_2 $	$ c_1 + c_2 - 2 $
5.	$(0, 1)$	0	1	1
6.	$(-c_1, 1 - c_2)$	$ -c_1 $	$ 1 - c_2 $	$ c_1 + c_2 - 1 $

Таблица 4.



Чтобы найти верхнее значение $\Delta_{\infty}(c)$, достаточно сравнить значения в таблице 4. Рассмотрим пункт 2 таблицы 4, возможны 2 варианта:

1) $c_1 > 1$, $|1 - c_1| = c_1 - 1$, $|-c_2| = c_2$, $|c_1 + c_2 - 1| = c_1 + c_2 - 1$ — это соответствует области C_1 на рис. 4. В этой области максимальной является функция $c_1 + c_2 - 1$.

2) $c_1 < 1$, $|1 - c_1| = 1 - c_1$, $|-c_2| = c_2$, $|c_1 + c_2 - 1| = c_1 + c_2 - 1$ — это соответствует областям C_2 и C_3 на рис. 4. В этой области максимальной является функция c_2 .

Для пункта 6 проведем аналогичные рассуждения:

1) $c_2 > 1$, $|-c_1| = c_1$, $|1 - c_2| = c_2 - 1$, $|c_1 + c_2 - 1| = c_1 + c_2 - 1$ — это соответствует области C_2 на рис. 4. В этой области максимальной является функция $c_1 + c_2 - 1$.

2) $c_2 < 1$, $|-c_1| = c_1$, $|-c_2| = 1 - c_2$, $|c_1 + c_2 - 1| = c_1 + c_2 - 1$ — это соответствует областям C_1 и C_3 на рис. 4. В этой области максимальной является функция c_2 . Учитывая, что выше прямой $c_1 = c_2$ больше функция c_2 , а ниже c_1 , разделим область C_3 прямой $c_1 = c_2$.

Теперь рассмотрим пункт 4 таблицы 4, получим следующие варианты

	Значение $ x_1 $	Значение $ x_2 $	Значение $ x_3 $	Максимальное значение
1.	$c_1 > 1, c_1 - 1$	$c_2 < 1, 1 - c_2$	$c_1 + c_2 > 2, c_1 + c_2 - 2$	$c_1 - 1$
2.	$c_1 > 1, c_1 - 1$	$c_2 < 1, 1 - c_2$	$c_1 + c_2 < 2, 2 - c_1 - c_2$	$1 - c_2$
3.	$c_1 < 1, 1 - c_1$	$c_2 > 1, c_2 - 1$	$c_1 + c_2 > 2, c_1 + c_2 - 2$	$c_2 - 1$
4.	$c_1 < 1, 1 - c_1$	$c_2 > 1, c_2 - 1$	$c_1 + c_2 < 2, 2 - c_1 - c_2$	$1 - c_1$
5.	$c_1 < 1, 1 - c_1$	$c_2 < 1, 1 - c_2$	$2 - c_1 - c_2$	$2 - c_1 - c_2$

Таблица 5.

Сравнивая выражения, найденные для пунктов 2, 4 и 6 таблицы 4, получим следующие результаты (рис. 6).

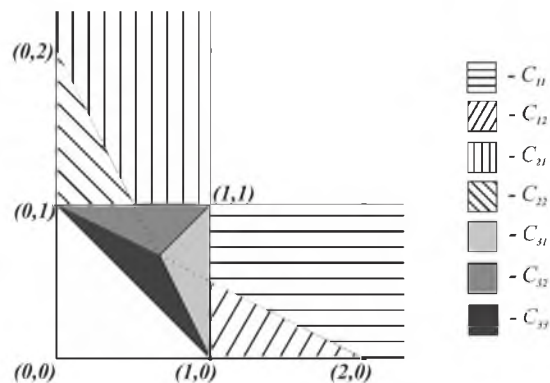


Рис. 6.

Для области C_{11} $\Delta_{\infty}(c) = c_1 + c_2 - 1$, и $\Delta_{\infty} = \frac{1}{2}$ достигается в точке $(1, 1/2)$. Для области C_{12} $\Delta_{\infty}(c) = 1 - c_2$, и $\Delta_{\infty} = 1/2$ достигается также в точке $(1, 1/2)$. Для области C_{21} $\Delta_{\infty}(c) = c_1 + c_2 - 1$ и $\Delta_{\infty} = 1/2$ достигается в точке $(1/2, 1)$. Для области C_{22} $\Delta_{\infty}(c) = 1 - c_1$ и $\Delta_{\infty} = 1/2$ достигается в точке $(1/2, 1)$. Для области C_{31} $\Delta_{\infty}(c) = c_1$, и ее $\Delta_{\infty} = 2/3$ достигается в точке $(2/3, 2/3)$. Для области C_{32} $\Delta_{\infty}(c) = c_2$, и $\Delta_{\infty} = 2/3$ достигается в точке $(2/3, 2/3)$.



Для области C_{33} $\Delta_{\infty}(c) = 2 - (c_1 + c_2)$, и ее $\Delta_{\infty} = 2/3$ в точке $(2/3, 2/3)$.

Таким образом, действительно для областей $C_1 = C_{11} \cup C_{12} \cup C_{13}$ и $C_2 = C_{21} \cup C_{22} \cup C_{23}$ получили $\Delta_{\infty} = 1/2$ и для области $C_3 = C_{31} \cup C_{32} \cup C_{33}$ $\Delta_{\infty} = 2/3$. ■

Литература

1. Абросимова А.А. Средние значения отклонений для распределения точек на торе // Научные ведомости БелГУ. Математика. Физика. Белгород: НИУ БелГУ. – 2012. – №.5(124); Вып.26. – С.5-11.
2. Абросимова А.А. Множества ограниченного остатка на двумерном торе // Чебышевский сборник. – 2011. – 12; Вып.4(40). – С.15-23.

BOUNDARIES OPTIMIZATION OF TWO-DIMENSIONAL BOUNDED REMAINDER SETS

A.A. Abrosimova, D.A. Blinov

Vladimir State University named A. and N. Stoletovs,
Stroiteley Av., 11, Vladimir, 600024, Russia, e-mail: AlbinaAbrosimowa@yandex.ru,
mr.DmBlinov@mail.ru

Abstract. Two-dimensional bounded remainder sets which are constructed by a hexagonal development of torus are under study. Optimization of boundaries for these sets are found.

Key words: bounded remainder sets, distribution of fractional parts, toric development, exchanged domains, three-dimensional metric.