arXiv:2303.14899v1 [math.MG] 27 Mar 2023

圆盘中格点多边形的分类与枚举†

刘秋月[1],张玉琴[2] 和蔡占元*

天津大学应用数学中心，中国天津，300072

摘要

1980年，V. I. Arnold 研究了给定面积的凸格多边形的分类问题。此后，许多作者研究了这一问题及其类似问题，其中包括 B´ar´any、Lagarias、Pach、Santos、Ziegler 和 Zong。最近，Zong 提出两个计算机程序，分别用于证明 Hadwiger 覆盖猜想和 Borsuk 分割问题；这些程序基于对包含在特定球中的凸格多面体进行枚举。为此，类似于 B´ar´any 和 Pach 关于体积的工作，以及 Liu 和 Zong 关于基数的工作，我们得到了给定圆盘中非等价凸格多边形数量的界。此外，我们还提出了一种枚举这些凸格多边形的算法。

关键词：格点多边形、分类、枚举

2010年 数学主题分类：52B20, 52C07

1 引言

$\mathbb{E}^d$ 中的凸格多胞体是整数格 $\mathbb{Z}^d$有限子集的凸包。另一种描述方式是将其定义为凸体与 $\mathbb{Z}^d$的交集；为方便起见，本文采用这一表述。按照惯例，令 P 表示一个 d维凸格多胞体，令 $|P|$ 表示 P的基数，令 $f_0(P)$表示 P的顶点数，令 $v(P)$表示 P的体积。关于多胞体和格多胞体的更多信息，可参见 [19] 和 [5]。

考虑两个 d维凸格多胞体，分别记为 P_1 和 P_2。如果存在一个保持 $\mathbb{Z}^d$的幺模变换 σ，使得 $\sigma(P_1) = P_2$，则称 P_1 和 P_2 幺模等价，记作 $P_1 \sim P_2$。容易看出，若 $P_1 \sim P_2$ 和 $P_2 \sim P_3$，则有 $P_1 \sim P_3$。此外，若 $P_1 \sim P_2$，则有

$$|P_1| = |P_2|,\ f_0(P_1) = f_0(P_2),\ v(P_1) = v(P_2).$$

在格多面体中，如果两个顶点是同一条边的端点，就称它们相邻。因此，如果 $P_1 \sim P_2$ 和 σ 是幺模变换，那么 σ 会保留顶点之间的邻接关系和非邻接关系。此外，如果幺模变换 σ 将 $v_1^{(i)}$ 映射到 $v_2^{(i)}$，其中 v_1^i 和 v_2^i 分别是 P_1 和 P_2 的顶点，那么由 $v_i^{(1)}$ 及其相邻顶点构成的凸包体积，与由 $v_i^{(2)}$ 及其相邻顶点构成的凸包体积相同。此外，当 $P_1 \sim P_2$时，对于 P_1的任意一条边 S， S 上的格点数与 σ上的相同（S）。

显然，根据等价关系∼，凸格多面体可以分为不同的类。通过三角剖分，很容易证明

$$d! \cdot v(P) \in \mathbb{Z} \tag{1}$$

†本研究得到国家自然科学基金委员会（NSFC12226006、NSFC11921001）和国家重点研发计划（2018-YFA0704701）的资助。

*通讯作者。电子邮箱：18976257573@163.com。

对任意 d维凸格多面体 P，均成立。令 $v(d,m)$表示具有 $v(P)=m/d!$的 d维凸格多面体 P的不同类的数量，其中 d 和 m 均为正整数。设 $f(d,m)$和 $g(d,m)$是正整数 d和 m的函数。本文中，$f(d,m)\ll g(d,m)$表示

$$f(d,m)\leqslant c_d\cdot g(d,m) \tag{2}$$

对所有正整数 m 以及固定的正整数 d均成立，其中 c_d 是一个仅取决于 d的常数。

1980年，Arnold [22] 研究了 $v(2,m)$ 的取值，并证明

$$m^{\frac{1}{3}}\ll\log v(2,m)\ll m^{\frac{1}{3}}\log m, \tag{3}$$

当 m充分大时成立。1991年，Lagarias 和 Ziegler [12] 证明，任何体积不超过 V 的格多面体，都幺模等价于一个包含在边长至多为 $n\cdot n!V$的格立方体内的格多面体，这意味着体积有界的格多胞体的等价类数量有限。1992年，B´ar´any 和 Pach [9] 将 Arnold 的上界改进为

$$\log v(2,m)\ll m^{\frac{1}{3}}. \tag{4}$$

此外，B´ar´any 和 Vershik [10] 得到了一个一般上界

$$\log v(d,m)\ll m^{\frac{d-1}{d+1}}, \tag{5}$$

对于任意固定的 d 以及充分大的 m均成立。

令 $\kappa(d,w)$ 表示具有$|P|=w$的 d维凸格多面体 P 的不同类的数量。2011年，Liu 和 Zong [8] 通过证明研究了给定基数的凸格多面体的分类问题

$$\begin{gathered} w^{\frac{1}{3}}\ll\log\kappa(2,w)\ll w^{\frac{1}{3}}, \\ \kappa(d,w)=\infty,\ if\ w\geqslant d+1\geqslant 4. \end{gathered} \tag{6}$$

本文还得到了 Arnold 关于中心对称格多边形问题的一些相关结果。

在 [11], I. Aliev、J. A. De Loera 和 Q. Louveaux 提出了六项关于半群 $Sg(A)=\{\mathbf{b}:A\mathbf{x}=\mathbf{b}\ x\in\mathbb{Z}^n,\mathbf{x}\geqslant\mathbf{0}\}$ 的 k- 可行性研究成果，其中 A 是一个整 $d\times n$ 矩阵，并研究了相关的多面体几何。事实上，k-可行性问题是对具有 k 格点的多面体进行分类这一问题的特殊情形（针对形式为 $\{\mathbf{x}:A\mathbf{x}=\mathbf{b},\mathbf{x}\geqslant\mathbf{0}\}$ 的参数多面体）。

除了上述关于类数的结果外，还有几位作者着重研究了在特定条件下枚举 d 维凸格多面体。S. Rabinowitz [20] 枚举了所有内部格点不超过一个的凸格多边形代表元。M. Blanco 和 F. Santos [16] 证明了三维中宽度大于一且格点数固定的多面体具有有限性，并明确枚举了格点数不超过 11 的情形 [17,18]。2021年，B. Gabriele [2] 开发了一种算法，用于完整枚举体积不超过 m 的 d 维凸格多面体代表元。此外，J.A. De Loera 在 [13], 讨论了枚举有理凸多面体内部所有格点的算法和软件，而在 [14], 中，他综述了计算多面体内部格点数的问题及其应用。

从上述研究可以看出，关于凸格多面体的分类与枚举，仅在凸格多面体自身结构相关的条件下进行过探讨，例如内部、体积、基数、宽度等。然而，据我们所知，很少有研究关注受限于给定

区域的凸格多面体的分类与枚举，即由给定区域内的格点构成的凸格多面体。这是一个至关重要且有价值的研究领域，原因如下。

1957年，Hadwiger [7] 提出了一项猜想：每个 n维凸体都可以由其内部的2^n 个平移覆盖。该猜想被称为Hadwiger猜想，目前对所有 $n \geqslant 3$而言仍未解决。1933年，Borsuk [15] 提出了一项猜想：每个有界的 n维集合都可以划分为$n+1$ 个直径更小的子集，这被称为Borsuk猜想。2010年，Zong [4] 提出了一个四步定量方案，以解决Hadwiger猜想。2021年，Zong [3] 基于一种新颖的重新表述，开发了一个计算机证明程序来处理Borsuk猜想。Zong的这两个方案都依赖于枚举包含在特定球 P 中的凸格多面体。

此外，对在给定区域内枚举凸格多面体所有代表元的算法进行复杂度分析，有助于确定这一枚举问题是否为NP困难或NP完全。这可能会促成新的基于格的NP困难或NP完全问题的发现，对格密码学领域具有重要意义。

本文聚焦于二维情形下的凸格多面体，即凸格多边形。基于上述动机，我们在第2节研究以原点为中心、半径为 R 的给定闭圆盘内凸格多边形的不同类的数量，记为 B_R。具体而言，设 $\kappa(R)$ 表示 B_R 中凸格多边形的不同类的数量，并证明

$$R^{2/3} \ll \log \kappa(R) \ll R^{2/3}.$$

Thi该结果与 B´ar´any 和 Pach [9]，以及 Liu 和 Zong [8] 的结果类似 .

在第3节，我们介绍一种算法，用于枚举 B_R 中凸格多边形的代表元，并求得当 $R=2$ 为 3 和 4 时不同类的数量。值得注意的是，在二维情形下，该算法也适用于圆盘以外的其他区域。此外，该算法有助于 [3] 中的计算机证明。

在第4节，我们分析第3节所介绍算法得出的实验结果。基于观察结果，我们提出两个开放问题，旨在加深对 B_R 中代表元数量的理解。

在第5节中，我们分析算法的复杂度。这有助于确定：关于 R，在 B_R 中寻找所有非等价凸格多边形的问题是 NP困难还是 NP完全；以及关于 n，在 αB^n 中寻找所有非等价凸格多胞体的问题是 NP困难还是 NP完全，其中 B^n 是以原点为中心、位于 $\mathbb{E}^n$中的 n 维单位球。

2 凸格多边形的分类 c

回顾一下， $\kappa(R)$表示 B_R中凸格多边形的所有不同类的数量。本节的主要任务是证明以下定理。

定理 2.1。 当 R 足够大时，有

$$c_1 R^{2/3} \leqslant \log \kappa(R) \leqslant c_2 R^{2/3}, \tag{7}$$

对某个适当的 c_1， $c_2 > 0$。也就是说，有

$$R^{2/3} \ll \log \kappa(R) \ll R^{2/3}. \tag{8}$$

在证明定理 2.1 之前，我们先按照 [8]，中的做法，构造凸格多边形 M_τ 和 $Q_i, i = 1, \cdots, 2^{|V_\tau|-1}$。这一构造的思路最初源自 Arnold [22]。

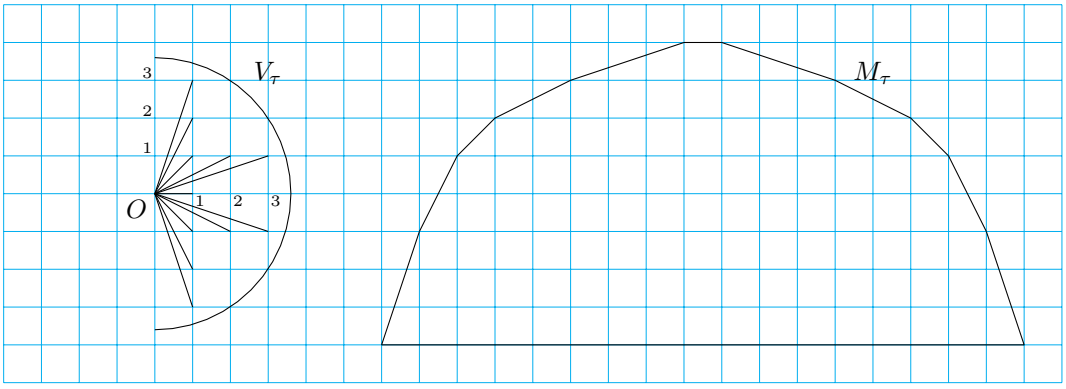

图 2.1： V_τ 和 M_τ的示例

设 τ 为一个较大的数，令 V_τ 表示半圆 $\{(x,y)：\ x^2+y^2\leqslant\tau^2,\ x>0\}$ 中所有本原整数向量组成的集合。设 M_τ 为一个凸格多边形，其有向边是 V_τ 和 $-\sum_{v\in V_\tau}v$ 中的所有整数向量，如图 2.1 所示。

众所周知，在数论中

$$|V_\tau|=\frac{3}{\pi}\tau^2+O(\tau\log\tau). \tag{9}$$

我们将凸格多边形 M_τ 的一些性质列举如下:

1. 它有 $|V_\tau|+1$ 个顶点。

2. 除直径外， M_τ 的每条边上除了顶点外不含其他格点。

3. 设 r 为包含在 M_τ 中的半圆的最大半径， r' 为包含 M_τ的半圆的最小半径。由（9）可推得

$$\tau^3\ll r\leqslant r'\ll\tau^3.$$

现在我们考虑凸格多边形 $2M_\tau$。令 $S_1, S_2, \cdots, S_{|V_\tau|}$按顺时针顺序为 $2M_\tau$的短边。根据性质 2，对于每个 i， S_i 包含三个格点，分别记为 $\mathbf{q}_i^0$、$\mathbf{q}_i^1$和 $\mathbf{q}_i^2$。于是我们有 $\mathbf{q}_1^0=(0,0)$、$\mathbf{q}_i^0=\mathbf{q}_{i-1}^2$ 以及 $\mathbf{q}_{|V_\tau|}^2=2\sum_{\mathbf{v}\in V_\tau}\mathbf{v}$。对于每个 $\mathbf{u}=(i_1,i_2,...,i_{|V_\tau|-1})\in\{1,2\}^{|V_\tau|-1}$，我们得到一个凸格多边形

$$Q_{\mathbf{u}}=\mathrm{conv}\{\mathbf{q}_1^0,\mathbf{q}_1^{i_1},\mathbf{q}_2^{i_2},\cdots,\mathbf{q}_{|V_\tau|-1}^{i_{|V_\tau|-1}},\mathbf{q}_{|V_\tau|}^2\}.$$

显然，当 $\mathbf{u}$、$\mathbf{v}\in\{1,2\}^{|V_\tau|-1}$ 且 $\mathbf{u}\neq\mathbf{v}$ 时， $Q_{\mathbf{u}}$ 和 $Q_{\mathbf{v}}$ 互不相同。令 $\mathcal{Q}$ 为这些多边形的集合 $Q_{\mathbf{u}}$，$\mathbf{u}\in\{1,2\}^{|V_\tau|-1}$。显然， $|\mathcal{Q}|=2^{|V_\tau|-1}$，并且我们有以下定理。

定理 2.2. 对于任意 $Q_{\mathbf{u}}\in\mathcal{Q}$，至多存在另一个与 $Q_{\mathbf{u}}$ 幺模等价的 $Q_{\mathbf{v}}\in\mathcal{Q}$。

证明. 根据 $2M_\tau$ 的构造，我们有

$$2M_\tau\subseteq\{(x,y):x\geqslant0,y\geqslant0\}. \tag{10}$$

给定任意 $Q_{\mathbf{u}}\in\mathcal{Q}$，假设存在一个与$Q_{\mathbf{u}}$幺模等价的凸格多边形 $Q_{\mathbf{v}}\in\mathcal{Q}$，也就是说，存在一个幺模变换 σ，使得 $\sigma(Q_{\mathbf{u}})=Q_{\mathbf{v}}$。现在考虑 $Q_{\mathbf{u}}$ 作为

一个矩阵，其列为多边形 $Q_{\mathbf{u}}$中格点的坐标，并对 $Q_{\mathbf{v}}$作同样处理。然后，变换 σ 可写为:

$$\sigma(Q_{\mathbf{u}}) \coloneqq AQ_{\mathbf{u}} + b = Q_{\mathbf{v}},$$

其中 A 是一个幺模矩阵， b 是一个整数向量。

设 $q_{\mathbf{u}}^{(1)} = (0,0)$、 $q_{\mathbf{u}}^{(2)}$、 $\cdots$、 $q^{(|V_\tau|+1)_{\mathbf{u}}}$是按顺时针顺序排列的 $Q_{\mathbf{u}}$的顶点，并以同样的方式记 $Q_{\mathbf{v}}$的顶点。根据 $Q_{\mathbf{u}}$和 $Q_{\mathbf{v}}$的定义， $q^{(|V_\tau|+1)_{\mathbf{u}}} = q^{(|V_\tau|+1)_{\mathbf{v}}} = (n,0)$。显然，对于 $Q_{\mathbf{u}}$ 和 $Q_{\mathbf{v}}$，任一短边上的格点数都严格少于直径上的格点数。因此， σ 将 $Q_{\mathbf{u}}$ 的直径映射为 $Q_{\mathbf{v}}$的直径。所以，讨论可分为以下两种情况。

情形 1。 $\sigma(q_{\mathbf{u}}^{(1)}) = q_{\mathbf{v}}^{(1)}$， $\sigma(q^{(|V_\tau|+1)_{\mathbf{u}}}) = q^{(|V_\tau|+1)_{\mathbf{v}}}$。由于幺模变换保持凸格多边形顶点之间的邻接关系，因此对所有 $i \in \{1, \cdots, |V_\tau|+1\}$，都有 $\sigma(q_{\mathbf{u}}^{(i)}) = q_{\mathbf{v}}^{(i)}$。显然， $b = (0,0)$ 和 A 可写成以下形式:

$$A = \begin{bmatrix} -1 & a \\ 0 & 1 \end{bmatrix} \ or \ \begin{bmatrix} -1 & a \\ 0 & -1 \end{bmatrix},$$

其中 a 是 $\mathbf{n}$ 个整数。由（10）可知， $Q_{\mathbf{u}}, Q_{\mathbf{v}} \subseteq \{(x,y) : x \geqslant 0, y \geqslant 0\}$，因此 A 只能是

$$A = \begin{bmatrix} -1 & a \\ 0 & 1 \end{bmatrix}.$$

如果存在一个 $i \in \{2, \cdots, |V_\tau|\}$ 使得 $q_{\mathbf{u}}^{(i)} = q_{\mathbf{v}}^{(i)}$，那么 $A = I_2$，其中 I_2是单位矩阵。否则 $q_{\mathbf{u}}^{(2)} \neq q_{\mathbf{v}}^{(2)}$（事实上，此时对所有 $i \in \{2, \cdots, |V_\tau|\}$都有 $q_{\mathbf{u}}^{(i)} \neq q_{\mathbf{v}}^{(i)}$），这意味着 $q_{\mathbf{u}}^{(2)}$和 $q_{\mathbf{v}}^{(2)}$的纵坐标不同（当 $\tau \geqslant \sqrt{5}$时）。这是因为 $q_{\mathbf{u}}^{(2)}$和 $q_{\mathbf{v}}^{(2)}$只能是短边 S_1 上的格点 $\mathfrak{q}_1^1$ 或 $\mathfrak{q}_1^2$，且该短边属于 $2M_\tau$。但对于任意整数点 $z \in \mathbb{Z}^2$， Az 和 z 的纵坐标相同， $q_{\mathbf{u}}^{(2)}$和 σ的纵坐标也相同（$q_{\mathbf{u}}^{(2)}$） $= q_{\mathbf{v}}^{(2)}$，这导致矛盾。因此在这种情况下，我们有 $A = I_2$和 $Q_{\mathbf{v}} = I_2 Q_{\mathbf{u}} = Q_{\mathbf{u}}$。

情况 2. $\sigma(q_{\mathbf{u}}^{(1)}) = q^{(|V_\tau|+1)_{\mathbf{v}}}$， $\sigma(q^{(|V_\tau|+1)_{\mathbf{u}}}) = q_{\mathbf{v}}^{(1)}$. 不难看出

$$A = \begin{bmatrix} -1 & a \\ 0 & 1 \end{bmatrix} \ or \ \begin{bmatrix} -1 & a \\ 0 & -1 \end{bmatrix}, \ b = \begin{bmatrix} n \\ 0 \end{bmatrix},$$

其中 a 是一个整数。与情况 1 类似， A 只能是

$$A = \begin{bmatrix} -1 & a \\ 0 & 1 \end{bmatrix}.$$

Let

$$Q'_{\mathbf{u}} \coloneqq \begin{bmatrix} -1 & 0 \\ 0 & 1 \end{bmatrix} Q_{\mathbf{u}} + \begin{bmatrix} n \\ 0 \end{bmatrix} \coloneqq \sigma'(Q_{\mathbf{u}}), \tag{11}$$

我们有

$$Q_{\mathbf{v}} = \begin{bmatrix} -1 & a \\ 0 & 1 \end{bmatrix} Q_{\mathbf{u}} + \begin{bmatrix} n \\ 0 \end{bmatrix} = \begin{bmatrix} 1 & a \\ 0 & 1 \end{bmatrix} Q'_{\mathbf{u}} \coloneqq A' Q'_{\mathbf{u}}. \tag{12}$$

显然， σ' 11 $Q_{\mathbf{u}}$ n $q_{\mathbf{u}}^{\prime(1)}$ = 中的 ( ) 关于 Y 轴翻转，并向右 σ' $q^{(|V_\tau|+1}$ = $0,0$ $q_{\mathbf{u}}^{\prime(i)}$ i $Q'_{\mathbf{u}}$
平移 个单位。设 ()$_{\mathbf{u}}$ ( ) 和 是按顺时针顺序排列的第 个顶点，则

$$q_{\mathbf{u}}^{\prime(i)} = \sigma'(q_{\mathbf{u}}^{(|V_\tau|+2-i)}), \quad i \in \{1, \cdots, |V_\tau|+1\}. \tag{13}$$

特别地 $q'^{(|V_\tau|+1}{}_{)\mathbf{u}} = \sigma'(q_{\mathbf{u}}^{(1)}) = (n, 0)$。

根据 (12)，我们知道 A' 将 $Q'_{\mathbf{u}}$ 的顶点 (0, 0) 映射到 $Q_{\mathbf{v}}$的顶点 (0, 0)。此外，A'将顶点 $(n, 0)$ 映射到顶点 $(n, 0)$。因此，与情形 1 类似，我们有 $A' = I_2$ 和 $\tau \geqslant \sqrt{5}$。所以在这种情况下，我们有 $a = 0$,

$$A = \begin{bmatrix} -1 & 0 \\ 0 & 1 \end{bmatrix} \text{ and } Q_{\mathbf{v}} = \begin{bmatrix} -1 & 0 \\ 0 & 1 \end{bmatrix} Q_{\mathbf{u}} + \begin{bmatrix} n \\ 0 \end{bmatrix}.$$

定理得证。 □

为进一步简化定理 2.1 的证明，我们陈述如下引理。

引理 2.3。给定一个足够大的 R 及其对应的闭圆盘 B_R，设 $\tau \geqslant \sqrt{2}$, d 为 $2M_\tau$的直径长度。如果

$$d \leqslant \sqrt{2}R, \tag{14}$$

那么，将 $d/2$ 向左平移 B_R 个单位后，$2M_\tau$ 可以被覆盖。

证明。给定任意 $\tau \geqslant \sqrt{2}$，可以构造一个凸格多边形 $2M_\tau$。设 d 为 $2M_\tau$的直径长度，并令 G_τ表示区域 $\{(x, y) : x^2 + y^2 \leqslant \tau^2, x > 0, y > 0\}$中的所有本原整数向量组成的集合。$G_\tau$中的向量关于直线 $y = x$对称。令$2G_\tau := \{2\mathbf{v} : \mathbf{v} \in G_\tau\}$，则我们有

$$\sum_{\mathbf{v} \in 2G_\tau} = (\ell_\tau, \ell_\tau), \tag{15}$$

其中 ℓ_τ 是正整数。

从 $2M_\tau$ 的最高点 B 到 X 轴的距离，可通过将 $2G_\tau$ 中各向量的纵坐标相加得到，即 ℓ_τ。根据（(15)），有 $\ell_\tau < d/2$。因此，$2M_\tau$ 可以被一个长为 d、宽为 $d/2$ （为正整数）的格点矩形 T_τ 覆盖，该矩形的长边与多边形 $2M_\tau$ 的直径重合，如图 2.2 左侧所示。

假设 $2M_\tau$ 的直径中点为 C，我们将点 C 向左移动 $d/2$ 个单位，使其平移至原点。矩形 T_τ 和凸格多边形 $2M_\tau$ 也作相同的平移，如图 2.2 右侧所示。平移后，矩形的顶点 A（见图 2.2 右侧）与原点之间的距离为 $\frac{\sqrt{2}}{2}d$。要使矩形 T_τ 被 B_R 覆盖，d 只需满足

$$\frac{\sqrt{2}}{2}d \leqslant R,$$

也就是说

$$d \leqslant \sqrt{2}R. \tag{16}$$

因此，当 $d \leqslant \sqrt{2}R$, $2M_\tau$ 向左平移 $d/2$ 个单位后，可被 B_R 覆盖 s. □

现在我们可以证明定理 2.1 了。

定理 *2.1* 的证明。设 R 为一个充分大的数，设 B_R 为上文定义的闭圆盘。首先，我们证明上界。根据 B´ar´any 和 Pach [9], 的结果，以及显然的事实：包含在 B_R 中的每个凸格多边形的面积都不超过 πR^2，我们有

$$\log \kappa(R) \leqslant \log \sum_{i=1}^{\lfloor 2\pi R^2 \rfloor} v(2, i) \leqslant c_2 R^{2/3}, \tag{17}$$

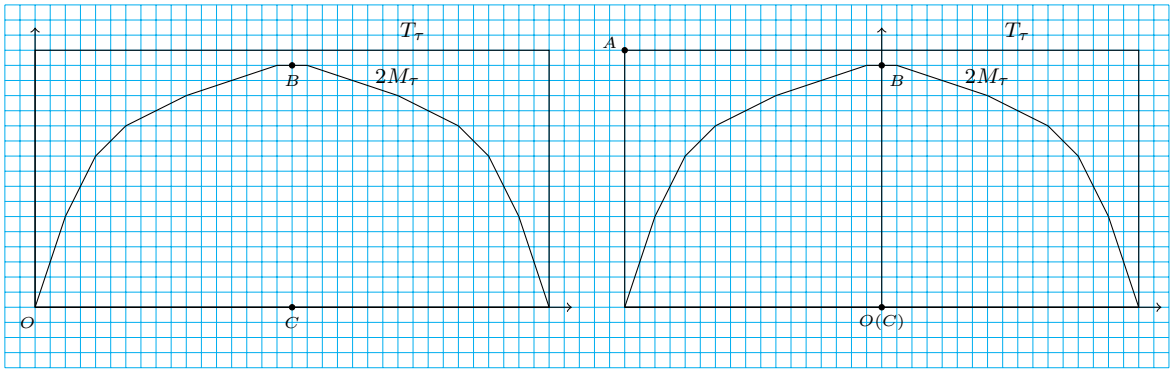

图 2.2：左：平移前的 $2M_\tau$ 和 T_τ；右：平移后的 $2M_\tau$ 和 T_τ

其中 c_2为某个常数。

接下来，我们证明下界。设 d 为 $2M_\tau$的直径长度。对于任意 $\tau \geqslant \sqrt{5}$，容易看出

$$d \leqslant 2\,|V_\tau| \cdot \tau.$$

由 (9) 可知，对于任意常数 $c > 1$,

$$d \leqslant c\frac{6}{\pi}\tau^3$$

当 τ i 足够大时成立。因此，存在一个足够大的 τ'，使得当 $\tau > \tau'$时，我们有

$$d \leqslant \sqrt{2}\frac{6}{\pi}\tau^3. \tag{18}$$

给定一个足够大的 R，满足

$$\tau^* \coloneqq \left(\frac{\pi}{6}R\right)^{1/3} > \tau', \tag{19}$$

于是我们有

$$d \leqslant \sqrt{2}\frac{6}{\pi}\tau^{*3} = \sqrt{2}R. \tag{20}$$

由引理 2.3 可推得，经过一次整数平移后， $2M_\tau^*$ 可被 B_R 覆盖。将平移后的多边形记为$2M_{\tau^*}^{'}$，于是有 $2M_{\tau^*}^{'} \subseteq B_R$。

现在，我们按照上述过程构造$2M_{\tau^*}^{'}$中凸格多边形的集合，记为 $\mathcal{Q}$。显然， $\mathcal{Q}$ 中的每个多边形都包含于 B_R中。因此，由定理 2.2 可得

$$\kappa(R) \geqslant \frac{|\mathcal{Q}|}{2} = 2^{|V_{\tau^*}|-2}. \tag{21}$$

由 (9)、(19) 和 (21)，我们得到

$$\log \kappa(R) \geqslant |V_{\tau^*}| - 2 \geqslant \frac{3}{\pi}\tau^{*2} = \frac{3}{\pi}(\frac{\pi}{6}R)^{2/3} = \frac{1}{2}(\frac{6}{\pi})^{1/3}R^{2/3}, \tag{22}$$

对于任意充分大的 R。 □

注 2.4. 若 R 足够大，则由 (17) 给出的常数 c_2 不会太大，也就是说，$\log \kappa(R)$ <11$(2\pi R)^{2/3}$。

根据定理 2.1 和注 2.4 的证明，我们可以得到

$$\frac{1}{2}(\frac{6}{\pi})^{1/3} \leqslant \liminf_{R} R^{-2/3}\log\kappa(R) \leqslant \limsup_{R} R^{-2/3}\log\kappa(R) \leqslant 11(2\pi)^{2/3}, \tag{23}$$

这自然引出了以下问题。

问题 1. 判断

$$\lim_{R\to\infty} R^{-2/3}\log\kappa(R) \tag{24}$$

是否存在。若极限存在，求出 *(24)* 的极限。

此外，根据 $2M_{\tau^*}^{'}$ 中 $\mathcal{Q}$ 的先前构造，对于 B_R 中凸格多边形顶点数的最大值，记为 M，我们有

$$M \geqslant 2|V_{\tau^*}|.$$

也就是说，由 (9) 和 (19) 可得

$$M \geqslant \frac{6}{\pi}(\tau^*)^2 = \frac{6}{\pi}(\frac{\pi}{6}R)^{2/3} = (\frac{6}{\pi})^{1/3}R^{2/3}. \tag{25}$$

根据 [22], 中的结果，我们知道

$$M \leqslant 16(2\pi R^2)^{1/3} = 16(2\pi)^{1/3}R^{2/3}. \tag{26}$$

3 圆盘中凸格多边形的枚举

本节中，我们介绍一种算法，用于找出给定圆盘中凸格多边形的所有代表元，然后计算不同类的数量。这里我们按基数对凸格多边形进行分类。我们的思路与 G. Brown 和 A. M. Kasprzyk [6]的思路类似。我们改进并扩展了 [6], 中的算法，并将其用于解决我们的问题。

定义 3.1. [6] 设 P为一个凸格多边形，且 $v \in \mathrm{vert}(P)$ 为 P的一个顶点。如果多边形$P_v := \mathrm{conv}((P \cap \mathbb{Z}^2)\setminus\{v\})$ 满足 $\dim P_v = \dim P$，则称 P_v是由 P经过削角得到的。给定一个多边形 Q，如果存在一列削角操作 $Q = P^{(0)} \subset \cdots \subset P_{(n)} = P$，其中 $P^{(i-1)} = P_{v_i}^{(i)}$对某个 $v_i \in \mathrm{vert}(P^{(i)})$ $0 < i \leqslant n$成立，则称 Q 可以由 P通过连续削角 得到。

下面的引理保证，圆盘中的所有凸格多边形都可以通过连续削去顶点得到。该引理与 [6] 的结果相似。为完整起见，我们在此重述其证明。

引理 3.2. 设 P 是一个凸格多边形， Q 是包含在 P 中的一个凸格多边形。那么，Q 可以通过连续削角从 P 得到。

证明。 如果 $P = Q$，那么结论成立。如果 $Q \subsetneq P,$，则必定存在顶点 $v \in$，使得 $\mathrm{vert}(P)$ 满足 $v \notin Q$。从 P 中削去 v，便可得到满足 $Q \subset P_v$ 的多边形 P_v。如果 $Q = P_v$，那么结论成立。否则，如果 $P_v \neq Q$，我们可以继续削去 P 的顶点，并令 Q 包含在新的多边形中。

根据上述定义，我们知道

$$\left|P^{(i-1)} \cap \mathbb{Z}^2\right| = \left|P^{(i)} \cap \mathbb{Z}^2\right| - 1, \quad 0 < i \leqslant n.$$

由于经过这一削切过程得到的多边形总是包含 Q，因此这些多边形的格点数有一个下界，即$\left|Q \cap \mathbb{Z}^2\right|$。所以，削切过程会在有限步后终止，而最后一步得到的多边形将是 Q。

□

现在，我们将 B_R 内最大的凸格多边形记为 N_R，即：

$$N_R := \mathrm{conv}(B_R \cap \mathbb{Z}^2). \tag{27}$$

令 $\mathcal{P}^k$ $(3 \leqslant k \leqslant |N_R|)$ 表示圆盘 B_R 中含有 k 个格点的凸格多边形的代表元族。下面的引理将说明，为了达到我们的目的，无须找出圆盘中的所有凸格多边形。

引理 3.3. 假设对于某个 $k\,(4 \leqslant k \leqslant |N_R|)$，$\mathcal{P}^k := \{P_1, \cdots P_{n_k}\}$ 非空。那么，对于任意包含在 B_R 中且含有 $k-1$ 个格点的凸格多边形 Q，存在 $P_i \in \mathcal{P}^k$ 以及一个顶点 $v \in$ 顶点(P_i)，使得 Q 与 $\mathrm{conv}((P_i \cap \mathbb{Z}^2) \backslash \{v\})$ 幺模等价。

证明。设 $\mathcal{P}^k \neq \emptyset$ 和 Q 是一个包含在 B_R 中且含有 $k-1$ 个格点的凸格多边形。那么，存在一列削角 $Q = P^{(0)} \subset \cdots \subset P^{(n)} = N_R$，其中 $P^{(i-1)} = P^{(i)}_{v_i}$，且对于某个 $v_i \in$，有顶点$(P^{(i)})$ $0 < i \leqslant n$。

在上述一系列削角操作中，显然 $P_{(1)}$ 包含 k 个格点，且 $P^{(1)} \subset B_R$。因此，根据 $\mathcal{P}^k$ 的定义，存在 $P_i \in \mathcal{P}^k$，使得 P_i 与 $P^{(1)}$ 幺模等价。如果 $v \in$ vert(P_i) 是 $v_1 \in P^{(1)}$ 在 P_i 与 $P^{(1)}$ 之间的幺模变换下的像，那么 Q 与 conv$((P_i \cap \mathbb{Z}^2) \backslash \{v\})$ 幺模等价，这正是我们所需要的。

□

引理 3.2 和 3.3 展示了我们算法的主要思路。从 $n = |N_R|$ 开始，依次对 $\mathcal{P}^n$ 中每个凸格多边形的每个顶点进行削角，从而得到由含有 $n-1$ 个格点的凸格多边形构成的集合。然后，从这个结果集合中移除等价的凸格多边形，即可得到 $\mathcal{P}^{n-1}$。最后，$\mathcal{P}^3 \cup \cdots \cup \mathcal{P}^{|N_R|}$ 正是我们算法的目标。

现在我们详细描述该算法的过程。我们用坐标表示一个格点，并用包含在凸格多边形内的所有格点的坐标序列表示一个凸格多边形。

我们的算法由三个主要部分组成：主算法、用于判断两个多边形上的幺模不变量的取值是否相等的算法（记作 COMPinv），以及用于判断两个多边形之间是否存在幺模变换的算法（记作 EQ）。

设 P 是一个凸格多边形。COMPinv 算法中使用的幺模不变量如下：

1. P 的顶点数，记作 $f_0(P)$。
2. P 边界上的格点数，记作 bound(P)。
3. P 的面积，记作 area(P)。
4. 令 $s_i(P)$ $i = 1, \cdots, f_0(P)$ 表示 P 的第 i 条边上的格点数。将 $\{s_i(P)\}$ 按升序排列所得的序列是第四个不变量，记作 sides(P)。
5. 令 $tr_i(P)$ $i = 1, \cdots, f_0(P)$ 表示由 P 的第 i 个顶点的相邻顶点构成的相邻三角形的面积，如图3.3所示。将 $\{tr_i(P)\}$ 按升序排列所得的序列是第五个不变量，记作 tr(P)。

前三个不变量称为一级不变量，后两个称为二级不变量。在 COMPinv 算法中，第一步是验证一级不变量；只有当一级不变量的值相等时，才进一步检查二级不变量。

注3.4. 通过实验已证明，上述不变量在半径较小时是有效的。此外，上述每个不变量都可以推广到 n 维情形。

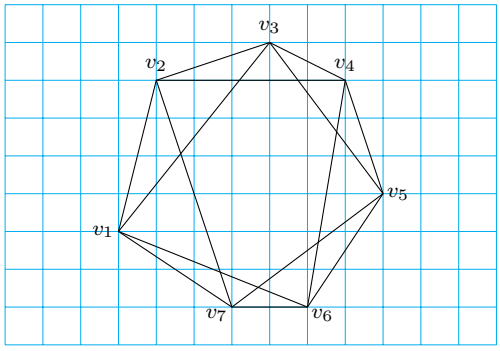

图3.3：顶点与相邻三角形

主算法、COMPinv 算法和 EQ 算法的具体流程分别见算法 1、算法 2 和算法 3。

在算法 1 中，函数 CALinv 将一个多边形作为输入，并输出该多边形上的不变量值。令 INVAR$[P_v]$ 表示 P_v上的不变量值，并令 $\mathcal{P}_{inv}^{n-1}$:= {INVAR$[P]$ ： $P \in \mathcal{P}^{n-1}$}，其中 $n = 4$、 $\cdots$、 $|N_R| + 1$。

算法 2 将两个多边形作为输入。如果发现这两个多边形上的所有不变量值都相等，COMPinv 算法输出 1；否则输出 0。显然，当 COMPinv 算法输出 0 时，这两个多边形一定不幺模等价。在算法 2 中，使用 MATLAB 命令 convhull 获取给定凸格多边形边界上的所有顶点或格点。需要注意的是，如果输入点的凸包不是二维的，命令 convhull 会报错；在算法 1 中，我们通过捕获这一特定错误来检查给定凸格多边形的维数。

算法 3 将两个多边形作为输入，并判断它们之间是否存在幺模变换。若存在这样的变换，EQ 算法输出 1，否则输出 0。由于幺模变换不会改变 $tr_i(P)$，我们可以根据相邻三角形的面积确定任意顶点可能的像。然后，我们可以求出幺模矩阵。具体过程如下。设 $v_i^{(1)}, i = 1, \cdots, n_1$ 表示 P_1 的顶点，其中每个 $v_i^{(1)}$ 与其相邻顶点构成的三角形，在所有这类相邻三角形中具有最小面积 s_1 。接着，我们固定 $v_1^{(1)}$ 并将其移至原点。若 $v_i^{(2)}, i = 1, \cdots, n_2$ 是 P_2 的顶点，且其相邻三角形的面积等于 s_1，我们依次将它们移至原点。 P_1 和 P_2 分别进行同样的平移。设 a、b 为平移后顶点 $v_1^{(1)}$ 相邻的边向量，设 c_i、d_i 为平移后顶点 $v_i^{(2)}, i = 1, \cdots, n_2$ 相邻的边向量，其中，格多面体中顶点 x 的相邻边向量是一个向量 v $\in \mathbb{Z}^n$ ，满足 v $=$ y $-$ x，其中 y 是某个顶点，且 conv(x, y) 是一条边。然后，对于每个 i，我们检查边向量 a、b 与边向量 c_i、d_i 之间是否存在幺模矩阵。若不存在，则这两个凸格多边形不幺模等价。若存在，我们检查该幺模矩阵是否将 P_1 的顶点映射到 P_2 中对应的顶点。若是，则这两个多边形幺模等价；否则，它们不幺模等价。

注3.5。从上述讨论可以看出，算法1、2和3几乎都可以推广到高维情形。在二维情形中，顶点可以按逆时针或顺时针顺序排序，但这在高维情形中并不适用，这可能是推广过程中面临的主要挑战。因此，确定两个凸格多面体的顶点之间的对应关系将更加困难，这可能导致算法 3 在高维情形下的时间复杂度显著增加。

算法 1： 主算法

输入： N_R

输出： $\mathcal{P} = \mathcal{P}^3 \cup \cdots \cup \mathcal{P}^{|N_R|}$

集合 $n \leftarrow |N_R|$, $\mathcal{P}^{|N_R|} \leftarrow \{N_R\}$, $\mathcal{P}^i = \emptyset, i = 3, 4, ..., |N_R| - 1$;
不变量$[N_R]$ ←CALinv(N_R);
设置 $\mathcal{P}_{inv}^{|N_R|} \leftarrow \{$不变量$[N_R]\}$, $\mathcal{P}_{i\ nv}^{i} = \emptyset, i = 3, 4, ..., |N_R| - 1$;
当 $n \geqslant 4$ **时**
  对于 $P \in \mathcal{P}^n$
    对于 $v \in vert(P)$ **执行**
      $P_v \leftarrow (P \cap \mathbb{Z}^2) \backslash \{v\}$;
      如果 维数$(P_v) = 2$ **则**
        不变量$[P_v]$ ←CALinv(P_v);
        如果 $\mathcal{P}^{n-1}$ 为空**则**
          $\mathcal{P}^{n-1} \leftarrow \{P_v\}$;
          $\mathcal{P}_{inv}^{n-1} \leftarrow \{$不变量$[P_v]\}$
        else
          $j \leftarrow 1$, EQidx $\leftarrow 0$;
          当 $1 \leqslant j \leqslant |\mathcal{P}^{n-1}|$ **时执行**
            如果 COMPinv($\mathcal{P}_{inv}^{n-1}[j]$, 不变量$[P_v]$) $== 0$ **那么**
              $j \leftarrow j + 1$
            否则如果 EQ($\mathcal{P}^{n-1}[j], P_v$) $== 1$ **那么**
              EQidx $\leftarrow 1$;
              $j \leftarrow \left|\mathcal{P}^{n-1}\right| + 1$;
            else
              $j \leftarrow j + 1$;
            end
          end
          如果 EQidx $== 0$ **那么**
            $\mathcal{P}^{n-1} \leftarrow \mathcal{P}^{n-1} \cup \{P_v\}$;
            $\mathcal{P}_{inv}^{n-1} \leftarrow \mathcal{P}_{inv}^{n-1} \cup \{$不变量$[P_v]\}$
          end
        end
      end
    end
  end
  $n \leftarrow n - 1$
结束

算法 2： COMPinv 算法

输入： 两个凸格多边形 P_1 和 P_2的不变量值

输出： 一个逻辑变量，用于指示 P_1 和 P_2 上的不变量值是否相等

读取 $f_0(P_1)$、bound(P_1)、area(P_1)、 $f_0(P_2)$、bound(P_2) 和 area(P_2)；

读取 sides(P_1)、tr(P_1)、sides(P_2) 和 tr(P_2)；

第一层(P_1) $\leftarrow$ [$f_0(P_1)$，边界(P_1)，面积(P_1)]；第二层(P_1) $\leftarrow$ [边(P_1)，迹(P_1)]；

第一层(P_2) $\leftarrow$ [$f_0(P_2)$，边界(P_2)，面积(P_2)]；第二层(P_2) $\leftarrow$ [边(P_2)，迹(P_2)]；

如果 第一层(P_1) $\neq$ 第一层(P_2) **那么**

  输出： 0

否则如果 第二层(P_1) ==第二层(P_2) **那么**

  输出： 1

否则

  输出： 0

结束

算法 3： EQ 算法

输入： 两个凸格多边形 P_1 和 P_2

输出： 一个逻辑变量，指示 P_1之间是否存在幺模变换以及 P_2

调用 tr(P_1) 和 tr(P_2)，解出 $v_i^{(1)}$、 $i = 1$、$\cdots$、n_1 以及 $v_i^{(2)}$、 $i = 1$、$\cdots$、n_2；

AlterVert$_1$ $\leftarrow v_1^{(1)}$ ；

将 vert(P_1) 按逆时针方向排列，并令 AlterVert$_1$ 为 vert(P_1) 中的第一个顶点；

从 vert(P_1) 中删除 AlterVert$_1$，后，所得序列中的每个顶点仍记为 vert(P_1)；

对于 $i \leftarrow 1$ **到** n_2，**执行**

  改变顶点$_2$ $\leftarrow v_i^{(2)}$ ；

  将顶点(P_2)按逆时针顺序排列，并令改变顶点$_2$ 为顶点(P_2)中的第一个顶点；

  顶点(P_2)中的每个顶点减去改变顶点$_2$, 后，所得序列仍记为顶点(P_2)；

  点$_1^1$ $\leftarrow$顶点(P_1)[n_1]；点$_2^1$ $\leftarrow$顶点(P_1)[2]；

  点$_1^2$ $\leftarrow$顶点(P_2)[n_2]；点$_2^2$ $\leftarrow$ 顶点(P_2)[2]；

  unimomatrix$_1$ $\leftarrow$ 将点$_1^1$ 和点$_2^1$ 分别映射到点$_1^2$ 和点$_2^2$的幺模矩阵分别；

  unimomatrix$_2$ $\leftarrow$ 将点$_1^1$ 和点$_2^1$ 分别映射到点$_2^2$ 和点$_1^2$的幺模矩阵分别；

  顶点(P_2)$_F$ $\leftarrow$ 将顶点(P_2)首尾翻转，使AlterVert$_2$ 成为最后一个顶点；

  如果(unimomatrix$_1$ *is an integer matrix*)&(unimomatrix$_1$ *maps* 顶点(P_1) *to* 顶点(P_2))**那么**

    输出： 1

  否则如果 (unimomatrix$_2$ *is an integer matrix*)&(unimomatrix$_2$ *maps* 顶点(P_1) *to* 顶点(P_2)$_F$) **then**

    输出： 1

  else

    输出： 0

  end

结束

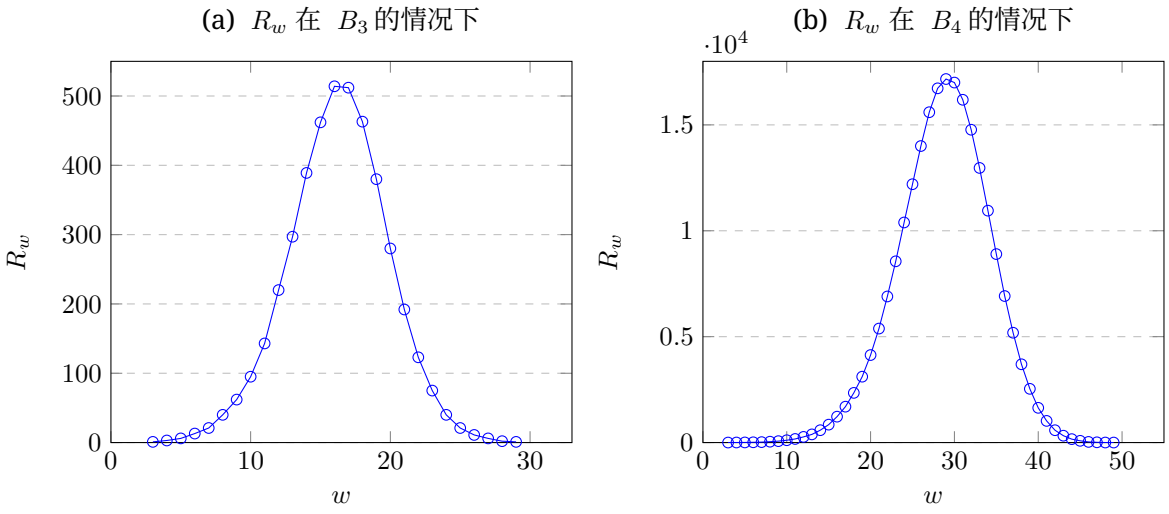

图 4.4: R_w 在 B_3 和 B_4的情况下的散点图

4 实验结果

我们使用上一节提出的算法，分别求出 B_2、B_3 和 B_4 中所有凸格多边形的代表元。表 4.1 和表 4.2 展示了在 B_2、B_3 和 B_4 中，具有不同基数的凸格多边形的不同类的数量。

设 R_w 为满足 $|P| = w$ 且包含于 B_R 中的所有代表元的数量，则在 $R = 2$ 的情况下，$\{R_w : R_w \neq 0\}$、3 和 4 的数据列于表 4.1 和表 4.2 中。表 4.1（仅在 B_3 的情况下）和表 4.2 中的数据绘制成散点图，即图 4.4(a) 和图 4.4(b) 。当 R 固定时，R_w 显然是 w 的函数。从这两幅图可以看出，当 $R = 3$ 和 4 时，随着 w 增加，R_w 先增大后减小。自然会问，R_w 的这一趋势是否对其他任何 R 都成立。更一般地，我们可以提出以下问题。

问题 2. 固定 R，并将 R_w 视为 w的函数，求一个近似函数，使其在 R 较大时能很好地拟合R_w 。

我们还可以提出问题 2 的对偶问题，如下所示，这有助于我们了解含有 w 个格点的代表元在不同半径的圆盘中的集中程度。这恰好就是问题 2 和问题 3 的值。

问题 3. 固定 w，并将 R_w 视为 R的函数，求一个近似函数，使其在 w 较大时能很好地拟合R_w 。

5 算法的复杂度分析

本节将给出算法 1、2 和 3 所执行的算术运算次数的上界。给定一个 R 及其对应的 B_R，令 W 为包含在 B_R 中的格点数，令 M 为包含在 B_R中的凸格点多边形的顶点数的最大值。由 (26) 和 [1], 可得

$$W \leqslant d_1 R^2, \quad M \leqslant d_2 R^{2/3}, \tag{28}$$

表 4.1：非　　等价凸格多边形的数量，其基数在 B_2 和 B_3中各不相同　　.

R (半径)=2			R (半径)=3				
w (基数)	R_w	总和为 R_w	w (基数)	R_w	w (基数)	R_w	总和为 R_w
3	1	75	3	1	17	512	4372
4	3		4	3	18	463	
5	6		5	6	19	380	
6	11		6	13	20	280	
7	15		7	21	21	192	
8	16		8	40	22	123	
9	12		9	62	23	75	
10	6		10	95	24	40	
11	3		11	143	25	21	
12	1		12	220	26	11	
13	1		13	297	27	6	
			14	389	28	2	
			15	462	29	1	
			16	514			

其中 d_1 和 d_2为适当的常数。令 N 为 B_R中所有凸格点多边形的不同类的数量。

首先，我们分析算法 1 中函数 CALinv 执行的算术运算次数。该函数用于计算包含在 B_R 中的凸格多边形上各个不变量的值，具体如下：

1. 如前所述，对于任意凸格多边形，我们使用 MATLAB 命令 convhull，并将该多边形内的所有格点作为输入，以获得该多边形的顶点和边界上的格点。根据 [21], , convhull 求解 n 个点的凸包所执行的算术运算次数为 $O(n\log\ n)$。对于 B_R中的任意凸格多边形，其中包含的格点数必定小于或等于 W。因此，获取 B_R 中的凸格多边形的顶点和边界上的格点所需的算术运算次数为 $O(W\log\ W)$。

2. 我们的算法中用于计算凸格多边形面积的方法如下：将多边形的一个顶点与其他顶点相连，对多边形进行三角剖分，然后通过计算每个小三角形的面积并将其相加，得到多边形 P 的面积。需要计算面积的小三角形数量最多为 $|\text{vert}(P)|-2$。因此，计算凸格多边形面积所需的算术运算次数为 $O(M)$。

3. 设 P 是 B_R 中的一个凸格多边形。计算向量 $(s_1(P)\ \cdots, s_{f_0(P)}(P))'$所需的算术运算次数为 $O(M)$, 其中 $f_0(P)$ 是 P 的顶点数。这是因为 P 至多有 M 条边。随后，按升序对该向量的所有分量进行排序，至多需要 $O(M\log\ M)$ 次算术运算。因此，计算给定多边形 P 的第四个不变量值，至多需要 $O(M\log\ M)$ 次算术运算。排序后的向量仍记为 $(s_1(P)\ \cdots, s_{f_0(P)}(P))'$。

4. 设 P 是 B_R 中的一个凸格多边形。计算向量 $(tr_1(P)\ \cdots, tr_{f_0(P)}(P))'$ 所需的算术运算次数为 $O(M)$, 因为 P 至多有 M 个相邻三角形。类似

表 4.2: B_4中不同基数的非等价凸格多边形的数量。

R (半径)=4							
w (基数)	R_w	w (基数)	R_w	w (基数)	R_w	w (基数)	R_w
3	1	15	846	27	15589	39	2537
4	3	16	1223	28	16726	40	1640
5	6	17	1695	29	17165	41	1023
6	13	18	2346	30	16998	42	583
7	21	19	3111	31	16185	43	324
8	41	20	4132	32	14771	44	162
9	67	21	5383	33	12967	45	83
10	110	22	6898	34	10950	46	31
11	170	23	8558	35	8899	47	12
12	268	24	10392	36	6918	48	2
13	386	25	12198	37	5186	49	1
14	584	26	14001	38	3696		
R之和 $_w$=224901							

于对第四个不变量的分析，考虑到排序的时间复杂度，计算给定多边形 P 上第五个不变量的值也至多需要 $O(M\log\ M)$ 次算术运算。排序后的向量仍记作 $(tr_1(P)\ \cdots, tr_{f_0(P)}(P))'$。

总之，计算凸格多边形上所有不变量的值所需的算术运算次数为 $O(W\log\ W)\ + O(M\log\ M)\ = O(W\log\ W)$，也就是说，函数 CALinv 需要 $O(W\log\ W)$ 次算术运算。

其次，算法 2 只比较不变量，而不计算它们。因此，算法 2 需要 $O(M)$ 次算术运算，因为如果将不变量的值组合起来构成一个新向量（$f_0(P)$，bound(P)，面积(P) $s_1(P)\ \cdots, s_{f_0(P)}(P)$ $tr_1(P)\ \cdots, tr_{f_0(P)}(P)$），那么该向量的长度不会超过 $2M + 3$。

第三，我们分析算法 3，其目标是确定是否存在一个幺模变换将 P_1 映射到 P_2。由于函数 CALinv 已经计算出 tr(P_1) 和 tr(P_2)，我们可以直接访问它们。之后，按照前文所述的过程，我们固定 P_1 的一个顶点，记为 $v_1^{(1)}$；该顶点与其相邻顶点构成一个面积最小的相邻三角形 s_1。对于 P_2 中每个相邻三角形面积与 s_1 相同的顶点，它都有可能是 $v_1^{(1)}$ 的像。我们将 $v_1^{(1)}$ 及其可能的像平移至原点。然后，对 $v_1^{(1)}$ 的每个可能像，我们检验 $v_1^{(1)}$ 的相邻边向量与该可能像的相邻边向量之间是否存在幺模矩阵；此步骤需要 $O(1)$ 次算术运算。接下来，我们需要检查该幺模矩阵能否将 P_1 的其他顶点映射到 P_2 的顶点；这一过程需要 $O(M)$ 次算术运算。这是因为 P_1 和 P_2 至多有 M 个顶点。此外，$v_1^{(1)}$ 至多有 M 个可能的像。由此可得，算法 3 需要 $O(M \cdot M)\ = O(M^2)$ 次算术运算。

最后，我们分析主算法。在算法 1 第 4 行开始的循环（下文称为主循环）的第 i 次迭代中，$\mathcal{P}^{W-i}$ 由 $\mathcal{P}^{W-i+1}$ 得出，该过程可分为两部分。第一部分依次对 $\mathcal{P}^{W-i+1}$ 中每个多边形的每个顶点进行削角，得到一个凸格多边形集合，记为 G^{W-i}，其中每个多边形都包含 $W - i$ 个格点。然后，我们计算通过削角得到的每个多边形的不变量值。令

$$\left|\mathcal{P}^{W-i+1}\right| = n_i, \quad \left|G^{W-i}\right| = n'_{i+1},$$

那么很容易看出

$$n'_{i+1} \leqslant Mn_i. \tag{29}$$

此外 , 主循环第 i 次迭代期间的削角次数也至多为 Mn_i
。主循环第 i 次迭代的第二部分是判断 G^{W-i} 中任意两个多边形是否等价。通过这样做，并为每个等价类仅保留一个多边形，我们可以得到 $\mathcal{P}^{W-i}$。显然，最多需要进行 $C^2_{n'_{i+1}}$ 次判断，其中 $C^2_{n'_{i+1}}$ 是一个组合数。

现在我们分别分析这两个部分。在第一部分中，从一个凸格多边形中削去一个顶点，至多需要 $O(W)$ 次操作。这是因为凸格多边形是通过其所包含的所有格点的坐标序列来表示的。因此，在削去一个顶点之前，我们需要在多边形所包含的所有格点序列中搜索该顶点，这至多需要 W 次。回顾算法 1 中函数 CALinv 的算术运算次数为 $O(W\log\ W)$，第一部分执行的算术运算次数为

$$O(WMn_i + W\log W n'_{i+1}) = O((W + W\log W)Mn_i) = O(W\log WMn_i). \tag{30}$$

在第二部分中，我们需要比较 G^{W-i} 中每两个多边形的不变量值。之后，我们需要找出 G^{W-i} 中每两个多边形之间是否存在幺模变换。回想一下，算法 2 和算法 3 分别需要 $O(M)$ 和 $O(M^2)$ 次算术运算，因此第二部分执行的算术运算次数为

$$\begin{aligned} &O(C^2_{n'_{i+1}}(M^2+M)) \\ =&O(n'^2_{i+1}(M^2+M)) \\ =&O((M^2n_i^2)(M^2+M)) \\ =&O((M^2n_i^2)M^2) \\ =&O(M^4n_i^2). \end{aligned} \tag{31}$$

综上，主循环第 i 次迭代期间的算术运算总次数为

$$O(W\log WMn_i) + O(M^4n_i^2). \tag{32}$$

那么，主算法执行的算术运算次数为

$$\begin{aligned} &O\left[\sum_{i=3}^{W}\left(W\log WMn_i + M^4n_i^2\right)\right] \\ =&O(W\log WMN + M^4\sum_{i=3}^{W}n_i^2) \\ =&O(W\log WMN + M^4N^2) \\ =&O(M^4N^2). \end{aligned} \tag{33}$$

由 (17) 和 (28)，(33) 可写为

$$O(R^{8/3}2^{cR^{2/3}}). \tag{34}$$

由 (33) 可知，我们算法的复杂度是关于 M and$N$ 的多项式函数，且 N 的次数仅为二，相对较低。这表明我们的算法是有效的。然而，定理 2.1 和 (34) 表明，在 B_R 中寻找所有非等价凸格多边形的问题可能是 NP完全或 NP困难问题。

此外，设 B_R^n 为以 $\mathbb{E}^n$ 的原点为中心、半径为 R 的 n 维闭球。将上述枚举问题中的 B_R 替换为 B_R^n，即可得到一个更复杂的问题，该问题也可能是 NP 完全或 NP 困难问题。这类复杂度较高的基于格的问题或许能在格密码学领域发挥重要作用，值得进一步探索。

参考文献

[1] A. Balog 和 I. B´ar´any，《论圆盘内整数点的凸包》。离散与计算几何（新不伦瑞克，新泽西州，1989/1990），DIMACS 离散数学与理论计算机科学丛书，Amer. Math. Soc.，普罗维登斯，罗得岛州，第 6 卷（1991年），39–44 页。[2] B. Gabriele，《按体积枚举格多胞体》。离散与计算几何，65（2021年），1087–1122 页。[3] C. Zong，《博尔苏克分割猜想》。日本数学杂志，16（2021年），185–201 页。[4] C. Zong，《Hadwiger 覆盖猜想的定量研究纲领》。中国科学：数学，53（2010年），2551–2560 页。[5] G.M. Ziegler，《多胞体讲义》，施普林格出版社，纽约，1995年。[6] G. Brown 和 A. M. Kasprzyk，《小多边形与环面码》。符号计算杂志，51（2013年），55–62 页。[7] H. Hadwiger，《未解问题》第 20 题。初等数学，12（1957年），121 页。[8] H. Liu 和 C. Zong，《关于凸格多面体的分类》。先进几何，11（2011年），第 4 期，711–729 页。[9] I. B´ar´any 和 J. Pach，《关于凸格多边形的数量》。组合、概率与计算，1（1992年），295–302 页。[10] I. B´ar´any 和 A.M. Vershik，《关于凸格多胞体的数量》。几何与泛函分析，2（1992年），381–393 页。[11] I. Aliev、J. A. De Loera 和 Q. Louveaux，《含至少 k 个格点的参数多面体：其半群结构与 k-弗罗贝尼乌斯问题》，载于《组合学最新进展》，施普林格出版社，柏林，2016年，753–778 页。[12] J.C. Lagarias 和 G.M. Ziegler，《包含子格中固定数量内部点的格多胞体的界》。加拿大数学杂志，43（1991年），1022–1035 页。[13] J.A. De Loera、R. Hemmecke、J. Tauzer、R. Yoshida，《有理凸多面体中的有效格点计数》。符号计算杂志，38（2004年），1273–1302 页。[14] J.A De Loera，《多胞体格点计数的诸多方面》。数学学报，52（2005年），175–195 页。[15] K. Borsuk，《关于 n 维欧几里得球面的三个定理》。数学基础，20（1993年），177–190 页。[16] M. Blanco 和 F. Santos，《含少量格点的格三维多胞体》。SIAM 离散数学杂志，30（2016年），669–686 页。[17] M. Blanco 和 F. Santos，《含六个格点的格三维多胞体》。SIAM 离散数学杂志，30（2016年），687–717 页。[18] M. Blanco 和 F. Santos，《按格点数枚举格三维多胞体》。离散与计算几何，60（2018年），756–800 页。[19] P.M. Gruber，《凸几何与离散几何》，施普林格出版社，柏林，2007年。

[20] S. Rabinowitz, 《至多含一个内部格点的凸格多边形计数》。组合艺术，28（1989年），83–96 页。[21] S. Hert 和 S. Stefan, 《二维凸包与极点》。CGAL 用户与参考手册。CGAL 编辑委员会4（2012年）。[22] V.I. Arnold, 《整凸多边形的统计》（俄文），泛函分析及其应用，14（1980年），1–3 页。英文译本：泛函分析及其应用，14（1980年），79–81 页。