arXiv:2302.06974v2 [math.GR] 4 Jun 2023

后代数 Baumslag–Solitar 群中的二次方程

Richard Mandel 和 Alexander Ushakov

Abstract. 对于有限生成群 G， G 上的丢番图问题是一个算法问题：判断给定的方程 $W(z_1, z_2, \ldots, z_k) = 1$（可能限于某个固定的方程子类）在 G中是否有解。在本文中，我们研究后代数 Baumslag–Solitar 群 BS(1, n)上 $\mathcal{C}$ 二次方程这一类丢番图问题的算法复杂度。我们证明，当 $n \neq \pm 1$时，该问题是 NP 完全的，并确定了 $\mathcal{C}$的各种子类（可定向、不可定向等）的算法复杂度。

1. Introduction

群上的方程研究至少可以追溯到1911年，当时 Max Dehn 提出了字问题和共轭问题。不过，该领域的主要研究工作稍晚才开始；尤其是，Roger Lyndon 于1960年明确描述了自由群上任意单变量方程的解（见 [12]），而直到20世纪80年代才取得一般性的可判定性结果。具体而言，Makanin [16]和 Razborov [19] 证明，判定自由群上的一般方程组是否有解的问题是可判定的。这个问题——判定给定的群上方程 G 是否有解——称为 G 的丢番图问题，本文记作 DP(G)。自 Makanin 和 Razborov 以来，已有许多研究结果确立了各种群类和方程类的丢番图问题的可判定性，并在某些情况下确定了其算法复杂度（例如，见 [8], [2], [14], [13], [15]）。关于这一主题的综述（侧重于可解群），见 [20]。

一类引起广泛关注的群上的方程是二次方程：其中每个变量 x 出现两次（分别以 x 或 x^{-1}的形式出现）。20世纪80年代初，Culler [4] 和 Schupp [21] 注意到，这类方程与紧曲面的理论具有密切联系（例如通过其相应的范坎彭图）。这一几何观点带来了许多有趣的结果，尤其是在自由群上的二次方程领域。例如，Grigorchuk 和 Kurchanov 在 [7], 中给出了对解集的描述，而 Kharlampovich、Lysenok、Myasnikov 和 Touikan [10]则证明了丢番图问题是 NP 完全的。在本文中，我们结合几何方法与计算方法，研究后代数 Baumslag–Solitar 群 BS(1, n) 上二次方程的算法复杂度。

第一作者部分获得巴斯克政府资助项目 IT1483-22 以及西班牙政府资助项目 PID2019-107444GA-I00 和 PID2020-117281GB-I00 的支持。2020年数学主题分类。主要分类：20F16、20F10、68W30。关键词与短语：亚幂零群、鲍姆斯拉格-索利塔群、二次方程、复杂性、NP完全性。

1.1. 鲍姆斯拉格-索利塔群。鲍姆斯拉格-索利塔群是由表示 BS$(m,n) = \langle a, t \mid t^{-1}a^m t = a^n \rangle$ 给出的单关系群。它们最早由 Gilbert Baumslag 和 Donald Solitar 于 1962 [1], 研究，此后被证明是反例和意外性质的丰富来源。特别是，这些群提供了已知的首批单关系非霍普夫群实例（即具有一个同构的真商[a]的群），并持续推动着大量富有成果的研究。众所周知，对于所有 n，群 BS(1, n) 都是后代数的；同时，它们也是唯一的可解鲍姆斯拉格–索利塔群。值得注意的是，当 $|n| \geq 2$时，BS(1, n) 的一阶理论是不可判定的；对于任何不是几乎阿贝尔的有限生成的几乎可解群，情况都是如此（这是 G. A. Noskov 在 [18]中证明的）。因此，确定后代数 Baumslag–Solitar 群（它们甚至不是几乎幂零群）上哪些类别的方程和不等式是可判定的，似乎是一项有趣且重要的工作。

Kharlampovich、Lopez 和 Miasnikov 最近证明，BS(1, n) 中二次方程的丢番图问题是可判定的（见 [9]）。近来，人们还研究了后代数 Baumslag–Solitar 群中的许多其他算法问题，包括离散优化问题和判定问题。例如，M. Lohrey 在 [11], 中证明背包问题是 NP 完全的，而同一篇论文中还证明，指数方程组[b] 的丢番图问题是不可判定的。Ciobanu、Holt 和 Rees 在 [3], 中证明了所有虚拟地为双曲群直积的群（例如 BS($n, \pm n$)）的丢番图问题具有可判定性；在[5] 中，作者则证明，BS(1, n) 上某些方程族的解集构成 EDT0L 语言。

1.2. 主要结果与概要。本文证明以下结果 .

定理 1.1. 当 $|n| \neq 1$ 时，BS(1, n) 上二次方程的丢番图问题是 NP 困难的；否则可在多项式时间内判定。

定理 1.2. 设 $m, n \in \mathbb{Z}$ 满足 $|m| \neq |n|$。那么，BS(m,n) 上二次方程的丢番图问题是 NP 困难的。

定理 1.3. 如果 BS(1, n) 上的二次方程 $W = 1$ 有解，那么它有一个大小为 $O(|W|^3)$ 的解。

我们还对可定向（其中每个变量都同时以 x 和 x^{-1} 的形式出现）和不可定向（其中至少有一个变量只以 x 或只以 x^{-1} 的形式出现）二次方程子类的丢番图问题的算法复杂度进行了完整分类。由于 BS(1, n) 的字问题可在多项式时间内求解（利用 Britton 引理很容易证明这一点），定理 1.3 提供了一个以解本身为形式的 NP 证书。因此，定理 1.1 是定理 1.2 和定理 1.3 的直接推论。不过，在第 5 节中，我们使用另一种我们认为更方便的证书完成了定理 1.1 的证明。这些结果见推论 5.3、5.6 和 5.8。

第2节介绍背景材料，并给出关于 BS(1, n) 的一些一般性结果；第4节则证明定理 1.2（即推论 4.5）。下文中，DP 始终指 BS(1, n) 上二次方程类的丢番图问题，或（明确说明时）其某个子类的丢番图问题。

[a]当 m、n 的素因子集合不同时，BS(m,n) 是非 Hopf 群，例如 BS(2, 3)。[b]形如 $g_1^{x_{i_1}} \cdots g_k^{x_{i_k}}$ 的方程，其解在 $\mathbb{N}^k$ 中寻找。

容易看出，BS(1, 1) $\cong \mathbb{Z}\times\mathbb{Z}$ 上的二次方程是平凡的（即等价于字问题，且只可能有平凡解），因此我们始终假设 $n \neq 1$。事实上，在第3节之后，我们假设 $|n| \neq 1$；该节证明了 BS(1, -1) 上的二次丢番图问题可在多项式时间内判定。为证明定理 1.2，我们给出了从 3-划分问题——一个众所周知的 NP 完全问题——到 DP(BS(m, n)) 的归约。对于 3-划分归约和复杂度上界，我们都需要一些关于以下形式方程的丢番图问题的结果

$$q_1\alpha^{x_1} + \cdots + q_k\alpha^{x_k} = q,$$

其中有 q_i、q、$\alpha \in \mathbb{Q}$ 和未知数 x_i。这些结果陈述于第4.1节，证明见 [17]。我们假定读者具备复杂性理论和 NP 完全性的基础知识，相关内容见 [6]。

2. 预备知识

2.1. 群上的二次方程。令 $F = F(Z)$ 表示由生成元 $Z = \{z_1, z_2, \ldots, z_k\}$ 生成的自由群。对于群 G，以变量 z_1、.....、z_k 为变量的群 G 上的方程是形如 $W = 1$ 的表达式，其中 $W \in F * G$（为方便起见，我们假设所有 z_i 都出现在 W 中）。若 $W = c_0 z_{i_1} c_1 z_{i_2} \cdots z_{i_l} c_l$，其中 $c_j \in G$，则称 $\{c_0, \ldots, c_l\}$ 中非单位元的元素为 W 的常数（或系数）。有时我们写作 $W(\bar{z})$、$W(z_1, \ldots, z_k)$ 或 $W(z_1, \ldots, z_k; c_1, \ldots, c_s)$，以强调 W 中的变量集和常数集。

方程 $W(z_1, \ldots, z_k) = 1$ over G 的解是一个元组 $\bar{g} = (g_1, \ldots, g_k) \in G^k$，使得映射 $z_i \mapsto g_i$ 可扩展为一个同态

$$\varphi : F * G \to G$$

该同态在 G 上为恒等映射，并且满足 $\varphi(W) = 1$。我们也用 $W(g_1, \ldots, g_k)$ 或 $W(\bar{g})$ 表示 $W(z_1, \ldots, z_k)$ 在 φ 下的像。若方程 $W = 1$ 中每个变量都恰好出现两次（作为 z_i 或 z_i^{-1}），则称其为二次的。

2.2. DP实例或解的大小。DP(BS(1, n)) 的一个实例就是 $W \in F(\bar{z}) * \text{BS}(1, n)$ 的一个元素，用生成元 z_i、a 和 t 上的自由约化字给出；输入大小定义为字长 $|W|$（我们不要求 W 具有任何标准形）。解 $(g_1, \ldots, g_k)$ 的大小定义为 $\sum_{i=1}^{k} |g_i|$，其中 $|\cdot|$ 现在表示 $G = \text{BS}(1, n)$ 中的（测地）字长。对于生成元 $\{a, t\}$ 上的字 w，记号 $\sigma_a(w)$ $\sigma_t(w)$ 分别表示 w 的 a 指数和 t 指数。

2.3. 方程等价性。若存在自同构 $\phi \in \text{Aut}(F * G)$，使得 ϕ 在 G 上为恒等映射，且 $\phi(W) = V$，则称两个方程 $W = 1$、$V = 1$ 等价。根据紧曲面分类，有一个众所周知的结论：任意关于 G 的二次方程，都等价于以下三种标准形式之一；实现这一等价的自同构 ϕ 可在时间 $O(|W|^2)$ 内计算（参见例如 [7]或 [10]）：

$$W(\bar{z}) = \prod_{j=1}^{k} z_j^{-1} c_j z_j = 1 \qquad k \geq 1, \tag{1}$$

$$W(\bar{x}, \bar{y}, \bar{z}) = \prod_{i=1}^{g} [x_i, y_i] \prod_{j=1}^{k} z_j^{-1} c_j z_j = 1 \qquad g \geq 1, k \geq 0, \tag{2}$$

$$W(\bar{x}, \bar{z}) = \prod_{i=1}^{g} x_i^2 \prod_{j=1}^{k} z_j^{-1} c_j z_j = 1 \qquad g \geq 1, k \geq 0. \tag{3}$$

数值 g 是方程的亏格，而 g 和 k （常数的数量）都是不变量。这些标准形式分别称为球面型（或亏格为 0 的可定向形式）、亏格为 g的可定向形式，以及亏格为 g的不可定向形式。根据其标准形式，方程称为球面型、亏格为 $g \geq 1$ 的可定向形式或不可定向形式。与紧曲面的情形类似，若方程 $W = 1$ 中的每个变量都以 z_i 和z_i^{-1}两种形式出现，则该方程是可定向的（亏格可以为 0，即球面型）；否则，它是不可定向的。假设 G 是有限生成的，可以证明标准形式 $\phi(W) = 1$ 的字长不大于原始字长 $|W|$ （更多细节见 [7]）。因此，我们只需考虑这些标准形式的方程。

2.4. BS(1, n) 的基本事实与引理。

2.4.1. 半直积表示。令 $\varphi\colon \mathbb{Z} \to \mathrm{Aut}(\mathbb{Z}[\frac{1}{n}])$ 为将 1 映射到 $x \mapsto \frac{x}{n}$ 的同态。我们将用到以下众所周知的事实：

$$\mathbb{Z}[\tfrac{1}{n}] \rtimes_{\varphi} \mathbb{Z} \cong \mathbf{BS}(1, n)$$

通过由下式定义的同构 ψ

$$(yn^{-\epsilon}, b) \mapsto t^{\epsilon} a^{y} t^{-\epsilon} t^{b}. \tag{4}$$

注意

$$\psi(\mathbb{Z}[\tfrac{1}{n}]) = \{t^{\epsilon} a^{y} t^{\epsilon} \mid \epsilon, y \in \mathbb{Z}\} = \langle\langle a \rangle\rangle,$$

且 $\psi^{-1}(g)$ 的第二个分量等于 $\sigma_t(g)$。在方便时，BS(1, n) 的一个元素可以直接写作其在 $\mathbb{Z}[\frac{1}{n}] \rtimes \mathbb{Z}$ 中对应的元素，而不再另行说明。

下面的引理给出了与 (4) 对应的标准形，以及一些有用的界。引理 2.2 和引理 2.3 分别给出了关于 $|W|$ 的半直积表示以及与 $\mathbb{Z}[\frac{1}{n}] \rtimes \mathbb{Z}$ 中给定元素对应的字 W 的长度的有用界。

引理 2.1. 对于每个元素 $g \in$ BS(1, n)，都存在 $\epsilon \in \mathbb{Z}_{\geq 0}$ 和 $y, z \in \mathbb{Z}$，使得

$$g = t^{\epsilon} a^{y} t^{-\epsilon} t^{z}. \tag{5}$$

此外，如果 W 是表示 g的生成元 $\{a, t\}$ 上的一个词，那么

$$|y| < |W||n|^{|W|} \quad and \quad \epsilon, |z| \leq |W|.$$

证明。显然，通过连续执行形如 $t^{-1}a \to a^n t^{-1}$ 和 $at \to ta^n$的变换，可以将任意词化为标准形 (5)。特别地，每当将一个正 t-字母一直移到左侧（或将一个负 t-字母移到右侧）时，a的指数绝对值就会乘以一个小于或等于 $|n|$的因子。这表明 y 的界成立；由于 t-字母的数量不会增加， ϵ、 $|z|$ 的界也随即成立。□

引理 2.2. 设 W 是生成元 $\{a,t\}$ 上的一个词，并设 $(\alpha,\beta)\in \mathbb{Z}[\frac{1}{n}]\rtimes\mathbb{Z}$ 满足： $W=(\alpha,\beta)$ 属于 BS(1, n)。那么

(a.) $|\alpha|<|n|^{|W|}$

(b.) $|\beta|\le |W|$

(c.) $n^{|W|}\alpha\in\mathbb{Z}$。

证明。我们可以将 W 写成 $t^{\epsilon_0}a^{\delta_0}t^{\epsilon_1}a^{\delta_1}\cdots t^{\epsilon_k}a^{\delta_k}$，其中 $\epsilon_i,\delta_i\in\{-1,0,1\}$ 和 $\sum_{i=0}^{k}|\epsilon_i|+|\delta_i|=|W|$。因此

$$(\alpha,\beta)=\prod_{i=0}^{k}(0,\epsilon_i)(\delta_i,0)=\prod_{i=0}^{k}(\delta_i n^{-\epsilon_i},\epsilon_i)=\left(\sum_{i=0}^{k}\delta_i n^{-\sum_{j=0}^{i-1}\epsilon_j},\sum_{i=0}^{k}\epsilon_i\right),$$

由此立即得出 (b) 和 (c)。从等式右边可见，

$$|\alpha|\le\sum_{i=0}^{k}|\delta_i||n|^{\sum_{j=0}^{i-1}|\epsilon_j|}\le 1+|n|+\cdots+|n|^{k-1}<|n|^{|W|},$$

这就证明了 (a)。 □

引理 2.3. 假设 $|n|>1$。设 $g\in$ BS(1, n)，并假设在半直积记号下， $g=(\alpha n^u,y)$，其中 $\alpha,y,u\in\mathbb{Z}$。那么 g 可以写成生成元 $\{a,t\}$ 上长度小于

$$2|n|(1+\log_{|n|}|\alpha|)+2|u|+|y|.$$

证明。假设 $\alpha\neq 0$ （否则结论显然），并令 $L=\log_{|n|}|\alpha|$。那么 g 可写为

$$\begin{aligned}w(a,t)=t^{-u}\left(\prod_{i=0}^{\lfloor L\rfloor}t^{-i}a^{\epsilon_i d_i}t^{i}\right)t^u t^y &= t^{-u}(a^{\epsilon_0 d_0}t^{-1}a^{\epsilon_1 d_1}t^{-1}\cdots t^{-1}a^{\epsilon_{\lfloor L\rfloor}d_{\lfloor L\rfloor}}t^{\lfloor L\rfloor})t^u t^y\\ &= t^{-u}a^{\epsilon_0 d_0}t^{-1}a^{\epsilon_1 d_1}t^{-1}\cdots t^{-1}a^{\epsilon_{\lfloor L\rfloor}d_{\lfloor L\rfloor}}t^{\lfloor L\rfloor+u}t^y,\end{aligned}$$

其中， $d_{\lfloor L\rfloor}\cdots d_1 d_0$ 是 $|\alpha|$ 的以$|n|$ 为底的展开，且 $\epsilon_i\in\{\pm 1\}$。因此，我们有

$$\begin{aligned}|w|\le 2|u|+2L+d_0+\cdots+d_{\lfloor L\rfloor}+|y| &< 2L+|n|(L+1)+2|u|+|y|\\ &< 2|n|(L+1)+2|u|+|y|\\ &= 2|n|(1+\log_{|n|}|\alpha|)+2|u|+|y|.\end{aligned}$$

□

由引理 2.2 和引理 2.3（及其证明）可知，我们可以高效地（即在关于 $|W|$的多项式时间和空间内）将以 $\{a,t\}$ 上的字编码的常数转换为$\mathbb{Z}[\frac{1}{n}] \rtimes \mathbb{Z}$ 中的元素（反之亦然）。因此，从 NP 完全性的角度来看，采用这两种格式中的哪一种来编码输入并无区别。不过，解的大小始终按 $\{a,t\}$上的字的长度来衡量。

2.4.2. 换位子宽度与词宽度。回顾一下，群 G 的换位子宽度是满足以下条件的最小数 $l \in \mathbb{N}$: 导出子群 G' 中的每个元素 g 都可以表示为群 G 中至多 l 个换位子的乘积。类似地，若 $W(z_1,\dots,z_k)$ 是字母 z_i 上的一个群词，则词子群 $S = \langle\{W(g_1,\dots,g_k)|g_i \in G\}\rangle$ 的词宽度（或简称宽度）定义为满足以下条件的最小数 l： 其中任意元素 $g \in S$ 都可以表示为至多 l 个形如 $W(g_1,\dots,g_k)$ 的字的乘积。

引理 2.4. 群词 $w = w(a,t)$ 表示导出子群 $\mathrm{BS}(1,n)'$ 中的一个元素，当且仅当

$$\sigma_t(w) = 0 \quad and \quad \sigma_a(w) \ is \ a \ multiple \ of \ n-1. \tag{6}$$

证明。 w 属于 $\mathrm{BS}(1,n)'$ ，当且仅当它在阿贝尔化 $\mathrm{BS}(1,n)^{\mathrm{ab}} = \langle a,t \mid [a,t]=1, a^{n-1}=1\rangle \cong \mathbb{Z}_{n-1}\times\mathbb{Z}$ 中为平凡元；这又当且仅当条件 (6) 得到满足。□

引理 2.5。$\mathrm{BS}(1,n)$ 的换位子宽度为 1。

证明。设 $w \in BS(1,n)'$。由引理 2.1 和引理 2.4 可得

$$w = t^p a^{k(n-1)} t^{-p}$$

对某些 $p \in \mathbb{Z}_{\geq 0}$ 和 $k \in \mathbb{Z}$，并且容易验证右端等于 $[t, a^{-k}t^{-p}]$ （事实上，对于任意阿贝尔群扩张循环群，都可以更一般地证明这一结果）。□

考虑词子群 $S = \langle x^2 \mid x \in \mathrm{BS}(1,n)\rangle$。作为词子群， S 是 $\mathrm{BS}(1,n)$ 的正规子群，并且容易验证它包含导出子群（这对任意群都成立）。特别地，商群 $\mathrm{BS}(1,n)/S$ 同构于有限阿贝尔群 $\langle a,t \mid a^2,\ a^{n-1},\ t^2,\ [a,t]\rangle$ 以及

$$w = w(a,t) \in S \quad \Leftrightarrow \quad \gcd(2,n-1) \mid \sigma_a(w) \quad \wedge \quad 2 \mid \sigma_t(w). \tag{7}$$

引理 2.6. S 的词宽度为 2。

证明. 任取一个 $s = (\alpha, 2b) \in S$。不妨设 $\alpha \in \mathbb{Z}$ （否则用 t 的适当次幂共轭 s ）。对于 p, $q \in \mathbb{Z}$ ，定义

$$x = (p,0) \quad \text{and} \quad y = \begin{cases} (qn^b, b) \text{ if } b \geq 0, \\ (q,b) \text{ if } b < 0, \end{cases}$$

使得

$$x^2y^2 = (2p + (1+n^{|b|})q, 2b).$$

如果 n是偶数，那么 $\gcd(2, 1+n^{|b|}) = 1$，因此我们可以选择 p和 q，使得 $x^2y^2 = (\alpha, 2b) = s$。如果 n 是奇数，那么 $\gcd(2, 1+n^{|b|}) = 2$。由 (7) 可知， $\sigma_a(s)$ 是偶数，因此 α 是偶数，并且如上所述，我们可以选择 p、 q ，从而得到 $x^2y^2 = s$。□

2.5. 3-划分问题与划分问题。对于由 $3k$ 个 $S = \{a_1, \ldots, a_{3k}\}$整数组成的多重集，令

$$L_S = \frac{1}{k} \sum_{i=1}^{3k} a_i.$$

3-划分问题（我们有时使用缩写 3PART）是这样一个判定问题：给定一个 $S = \{a_1, \ldots, a_{3k}\}$，其中包含 $L_S/4 < a_i < L_S/2$，能否将其划分为k 个三元组，且每个三元组的和都等于 L_S。众所周知，该问题是强 NP 完全的，这意味着即使 S 中的整数有上界，且该上界是输入大小的多项式，问题仍然是 NP 完全的；等价地说，即使输入采用一元编码表示，问题仍然是 NP 完全的。注意，由于限制条件 $L_S/4 < a_i < L_S/2$，我们可以假设 S 只包含正整数。

划分问题（或称 PARTITION）是一个相关问题，要求判定给定的正整数多重集S 能否划分为两个子集 S_1 和 S_2，使得 S_1 中各数之和等于 S_2中各数之和。若数字以二进制编码给出，该问题是 NP 完全的；若以一元编码给出，则可在多项式时间内判定（即弱 NP 完全）。有关这些问题的详尽论述，请参阅 [6]。

我们注意到，3PART 的强 NP 困难性对于证明 DP(BS(1, n)) 对 $|n| > 1$ 是 NP 困难的至关重要，因为 DP(BS(1, n)) 的实例以生成元上的字给出，即采用一元编码。另一方面，PARTITION 在一元输入下可在多项式时间内判定这一事实，将用于证明 DP(BS(1, -1)) $\in$ P。

2.6. Bézout 系数界。在第 5 节中，我们使用以下引理。

引理 2.7. 对任意整数 $\beta_1, \ldots, \beta_k$（其中至少一个不为零），存在 Bézout 系数 s_i，使得

$$\sum_{i=1}^{k} s_i \beta_i = \gcd(\beta_1, \ldots, \beta_k), \tag{8}$$

满足 $|s_i| < |\beta_1| + \cdots + |\beta_k|$.

证明。我们不妨设 $\gcd(\beta_1, \ldots, \beta_k) = 1$, $\beta_1 > \beta_2 > \ldots > \beta_k \geq 1$ 和 $k > 1$。注意，对于任意 $c \in \mathbb{Z}$, $s_1, \ldots, s_{k-1}, s_k \in \mathbb{Z}$ 满足 (8) 当且仅当 $s_1, \ldots, s_{k-1} + c\beta_k, s_k - c\beta_{k-1}$ 满足 (8)。因此，我们不妨设 $|s_k| < \beta_{k-1}$。类似地，对于 $i = 2, \ldots, k$，我们不妨设$|s_i| < \beta_{i-1}$。现在可以直接验证

$$|s_1| = \frac{1}{\beta_1} \left| 1 - \sum_{i=2}^{k} s_i \beta_i \right| \leq \frac{1}{\beta_1} \left(1 + \sum_{i=2}^{k} |s_i| \beta_i \right) < \frac{1}{\beta_1} + \sum_{i=2}^{k} |s_i| < \beta_1 + \cdots + \beta_k,$$

完成证明。 □

3. A polynomial-time algorithm for DP(BS(1, -1))

这里，我们简要介绍 DP(BS(1, -1)) $= \langle a, t \mid t^{-1}at = a^{-1} \rangle \simeq \mathbb{Z} \ltimes \mathbb{Z}$ 的特殊情形，并证明该问题可在多项式时间内判定。

注意，BS(1, −1) 的每个元素都可以唯一地表示为 $a^m t^k$，并且以下公式成立：

$$(a^y t^x)^{-1} \cdot a^m t^k \cdot (a^y t^x) = \begin{cases} a^{-m} t^k & \text{if } x \text{ is odd and } k \text{ is even,} \\ a^{2y-m} t^k & \text{if } x \text{ is odd and } k \text{ is odd,} \\ a^m t^k & \text{if } x \text{ is even and } k \text{ is even,} \\ a^{m-2y} t^k & \text{if } x \text{ is even and } k \text{ is odd.} \end{cases} \tag{9}$$

由此公式立即可得以下命题。

命题 3.1. 球面方程 $W = \prod z_i^{-1} a^{m_i} t^{k_i} z_i = 1$ 有解，当且仅当 $\sum k_i = 0$ 且下列条件之一成立。

- $\{|m_1|, \ldots, |m_k|\}$ 是划分问题的一个肯定实例。
- 某个 k_i 为奇数，且 $\sum m_i$ 为偶数。

命题 3.2. 可定向方程 $W = \prod [x_j, y_j] \prod z_i^{-1} a^{m_i} t^{k_i} z_i = 1$ 有解，当且仅当 $\sum k_i = 0$ 且 $\sum m_i$ 为偶数。

证明。该结论可直接由下式得出

$$\mathbf{BS}(1,-1)' = \{\, [x,y] \mid x, y \in \mathbf{BS}(1,-1) \,\} = \left\{\, a^{2i} \;\middle|\; i \in \mathbb{Z} \,\right\}.$$

□

命题 3.3. 不可定向方程 $W = x^2 \prod z_i^{-1} a^{m_i} t^{k_i} z_i = 1$ 有解，当且仅当满足以下任一条件

- $\sum k_i \equiv_4 2$ 且 $\{|m_1|, \ldots, |m_k|\}$ 是划分问题的一个正实例。
- $\sum k_i \equiv_4 2$ 且某个 k_i 为奇数，而 $\sum m_i$ 为偶数。
- $\sum k_i \equiv_4 0$ 且 $\sum m_i$ 为偶数。

证明. 该结论可直接由 (9) 以及

$$\left\{\, x^2 \;\middle|\; x \in \mathbf{BS}(1,-1) \,\right\} = \left\{\, t^{4j+2} \;\middle|\; j \in \mathbb{Z} \,\right\} \cup \left\{\, a^{2i} t^{4j} \;\middle|\; i, j \in \mathbb{Z} \,\right\}.$$

□

命题 3.4. 不可定向方程 $W = x_1^2 \cdots x_n^2 \prod z_i^{-1} a^{m_i} t^{k_i} z_i = 1$（其中 $n \geq 2$）有解，当且仅当 $\sum k_i$ 和 $\sum m_i$ 均为偶数。

*Pr*噢。该陈述可由下式直接推出：

$$\left\langle \left\{\, w^2 \;\middle|\; w \in \mathbf{BS}(1,-1) \,\right\} \right\rangle = \left\{\, x^2 y^2 \;\middle|\; x, y \in \mathbf{BS}(1,-1) \,\right\} = \left\{\, a^{2i} t^{2j} \;\middle|\; i, j \in \mathbb{Z} \,\right\}.$$

□

定理 3.5. 关于 BS(1, −1) 上二次方程的丢番图问题可在多项式时间内判定。此外，如果 BS(1, −1) 上的一个二次方程有解，那么它有一个大小为 $O(|W|)$ 的解。

证明。计算 $\sum k_i$ 和 $\sum m_i$ 需要线性时间。此外，对于以一元编码给出的数 $\{m_1, \ldots, m_k\}$，其划分问题可在多项式时间内求解。因此，命题 3.1、3.2、3.3 和 3.4 为该问题提供了一种高效的解法，而解的界可从它们各自的证明中轻易推出。□

既然已证明定理 1.3 对 BS(1, ±1) 成立，以下我们假设 $|n| > 1$。

4. Complexity lower bounds for quadratic equations over BS(1, n)

本节证明，对于所有满足 $|m| \neq |n|$ 的 m, n，BS(m, n) 上的二次丢番图问题具有 NP 困难性，从而证明定理 1.2（作者将在一篇后续论文中证明，对于幺模鲍姆斯拉格–索利塔群 BS($n, \pm n$)，同样的结果也成立）。此外，我们还证明了一个特殊情形具有 NP 困难性：当 $|n| > 1$ 时，BS(1, n) 上亏格 1 的非定向方程。

4.1. 带指数的代数方程。

带指数的代数方程是如下形式的方程

$$q_1\alpha^{x_1} + \cdots + q_k\alpha^{x_k} = q, \tag{10}$$

其中 $\alpha \in \mathbb{R}$ 是代数的，q_i、q、$\in \mathbb{Q}$（α）以及未知数 x_i，并要求其具有整数解。文献 [17] 证明，对于任意固定的 $\alpha \notin \{-1, 0, 1\}$，方程（10）的丢番图问题，即判定（10）是否有解的问题，是 NP 完全的。为了建立解的大小的上界（以证明定理 1.3）并实现从 3PART $\leq$ 到 DP 的归约，我们需要以下关于带指数的代数方程的结果（其中 α、q_1、.....、q_k、$q \in \mathbb{Q}$）。定理 4.1 以及命题 4.2 和命题 4.3 的证明见 [17]；这里我们仅给出命题 4.3 的证明，因为其中涉及一个一般性过程，该过程也用于证明不可定向情形下的 NP 困难性。

定理 4.1。设 $q_1, \ldots, q_k \in \mathbb{Z}$, $\alpha \in \mathbb{Q}$，并假设方程

$$q_1\alpha^{x_1} + \cdots + q_k\alpha^{x_k} = 0 \tag{11}$$

有整数解。那么它有一个满足以下条件的解 $x_1, \ldots, x_k \in \mathbb{Z}$

$$0 \;\leq\; x_1, \ldots, x_k \;\leq\; \sum_{i=1}^{k} \left| \log_{|\alpha|}(|q_i| + 1) \right|. \tag{12}$$

证明。该陈述由 [17, 定理 3.5] 和 [17, 命题 3.11]得出 □

命题 4.2（[17, 命题 2.3]）。给定 $s \in \mathbb{N}$，存在 $c \in \mathbb{N}$，使得对于任意$\alpha \in \mathbb{Q} \setminus \{-1, 0, 1\}$ 以及满足 $p_{i+1} - p_i \geq c$的整数 $0 \leq p_1 < p_2 < \cdots < p_s$，方程

$$\alpha^{x_1} + \cdots + \alpha^{x_s} = \alpha^{p_1} + \cdots + \alpha^{p_s} \tag{13}$$

有唯一的整数解 $x_i = p_i$（相差一个排列）。此外，c 是 $O(\log s)$，并且可以根据 s高效计算。

命题 4.3。固定 $\alpha \in \mathbb{Q} \setminus \{-1, 0, 1\}$。设 $S = \{a_1, \ldots, a_{3k}\}$ 是一个 3PART 实例，其中 $L = \frac{1}{k}\sum a_i$ 是子集的预期和，且 $L/4 < a_i < L/2$ 对 $i = 1$、2、. . ., $3k$成立（我们可以假设 $L \in \mathbb{N}$）。令 $c \in \mathbb{N}$ 为命题 4.2 保证存在的、对应于 $s = Lk$的数。定义数

$$q_y = 1 + \alpha^c + \alpha^{2c} + \cdots + \alpha^{(y-1)c} \qquad for \quad y \in \mathbb{N}$$
$$r = q_L\left(1 + \alpha^{2cL} + \alpha^{4cL} + \cdots + \alpha^{2(k-1)cL}\right)$$

以及方程

$$q_{a_1}\alpha^{x_1} + \cdots + q_{a_{3k}}\alpha^{x_{3k}} = r. \tag{14}$$

那么，当且仅当 (14) 有解时， S 是 3PART 的一个肯定实例。此外，(14) 的每个解都满足

$$0 \le x_1, \dots, x_{3k} \le 2ckL. \tag{15}$$

证明。假设 S 是 3PART 的一个肯定实例。必要时重新排列 a_i 和 x_i 的索引，我们可以假设对于 $i = 0$，1，.....，$k-1$，有 $\sum_{j=1}^{3} a_{3i+j} = L$。现在很容易验证

$$\begin{aligned} x_{3i+1} &= 2icL \\ x_{3i+2} &= c(2iL + a_{3i+1}) \\ x_{3i+3} &= c(2iL + a_{3i+1} + a_{3i+2}) \end{aligned}$$

对于 $i = 0$，1，.....，$k-1$，满足 (14) 和 (15)。

对于另一个方向，假设 x_1，.....，x_{3k} 是 (14) 的一个解。根据构造，(14) 的左边是 Lk 个 α的幂之和，而右边是 Lk 个互不相同的 α^c的幂之和。特别地，右边的和包含若干连续的 α^c的幂所构成的块，这些块之间在 $\alpha^{(2i-1)c(L-1)}$ 与 α^{2icL}、 $i = 1$、.....、$k-1$处有间隔。命题 4.2 表明，左边由相同的、互不相同的 α的幂组成，证明可通过仔细比较这些幂得出。首先，显然对于恰好一个 x_{i_1}，必有 $x_{i_1} = 0$，且 $q_{a_{i_1}} \alpha^{x_{i_1}} = 1 + \alpha^c + \ldots + \alpha^{c(a_{i_1}-1)}$ 。根据假设， $a_{i_1} < L$，因此 (14) 的右边包含 $\alpha^{ca_{i_1}}$，所以对于某个（唯一的） x_{i_2}，必有 $x_{i_2} = ca_{i_1}$。类似地， $q_{a_{i_1}} \alpha^{x_{i_1}} + q_{a_{i_2}} \alpha^{x_{i_2}}$的最高次项是 $\alpha^{c(a_{i_1}+a_{i_2}-1)}$），并且由于$c(a_{i_1}+a_{i_2}) < cL$，我们必须在左边取 α^c的下一个连续幂。因此，必有 $x_{i_3} = c(a_{i_1} + a_{i_2})$。最后， $q_{a_{i_1}} \alpha^{x_{i_1}} + q_{a_{i_2}} \alpha^{x_{i_2}} + q_{a_{i_3}} \alpha^{x_{i_3}}$的最高次幂是$\alpha^{c(a_{i_1}+a_{i_2}+a_{i_3}-1)}$），它必须是第一组连续的 α^c幂中的最后一项（因为对于任意 a_l，都有 $cL < c($ $a_{i_1}+a_{i_2}+a_{i_3}+a_l)$）。这意味着 $c(a_{i_1}+a_{i_2}+a_{i_3}) = cL$，且下一个最大的 x_i 等于 $2cL$。显然，可以继续这一过程，证明 S是一个肯定实例，并且 x_1，.....，x_{3k}满足 (15)。□

4.2. DP(BS(m, n)) 的 NP 困难性，其中 $|m| \neq |n|$。固定 $m, n \in \mathbb{Z} \setminus \{0\}$，使得 $|m| \neq |n|$，并令 $\alpha = \frac{m}{n}$。设 $S = \{a_1, \dots, a_{3k}\}$ 是一个 3PART 实例，其中$L/4 < a_i < L/2$， L 是预期的和。按照命题 4.3 中的定义，设 $c \in \mathbb{N}$。构造与 S 对应的方程 (14)，其整数系数为 $q_{a_1}, \dots,$ $q_{a_{3k}}$，而 r 按命题 4.3 中的定义给出。将系数乘以 n^{4ckL}，得到

$$b = rn^{4ckL} \quad \text{and} \quad b_i = q_{a_i} n^{4ckL} \quad \text{for } i = 1, \dots, 3k.$$

最后，考虑球面方程

$$z_1^{-1} a^{b_1} z_1 \cdots z_{3k}^{-1} a^{b_{3k}} z_{3k} = a^b \tag{16}$$

在群 BS(m, n) 上。

命题 4.4. S 是 3PART 的一个肯定实例，当且仅当 (16) 有解。

证明. 若 S 是 3PART 的一个肯定实例，则根据命题 4.3，(14) 有一个解 $x_1, \dots, x_{3k} \in \mathbb{Z}$，满足 $0 \le x_1, \dots, x_{3k} \le 2ckL$。根据构造，对于所有的 x_i，都有 $\frac{b_i}{n^{x_i}} \in \mathbb{Z}$。因此，在 BS($m, n$) 中，我们有 $t^{-x_i} a^{b_i} t^{x_i} = a^{b_i (\frac{m}{n})^{x_i}}$，并且

$$\prod t^{-x_i} a^{b_i} t^{x_i} = \prod a^{b_i \left(\frac{m}{n}\right)^{x_i}} = a^{\sum b_i \left(\frac{m}{n}\right)^{x_i}} = a^b.$$

因此， $z_i = t^{x_i}$ 是方程 (16) 的一个解。

反过来，假设 (16) 有一个解 $z_1, \ldots, z_{3k} \in \mathrm{BS}(m,n)$。由于常数中不包含 t-字母，我们可以假设每个 $z_i = t^{x_i}$ 都满足某个 $x_i \in \mathbb{Z}$。应用 Britton 引理，很容易看出，带指数的代数方程

$$b_1(\tfrac{m}{n})^{x_1} + \cdots + b_{3k}(\tfrac{m}{n})^{x_{3k}} = b$$

mu成立。因此，根据命题 4.3，S 是 3PART 的肯定实例 . □

推论 4.5. 当 $|m| \neq |n|$ 时（即定理 1.2 成立），关于 $\mathrm{BS}(m,n)$ 的丢番图问题是强 NP 困难的。

4.3. 亏格 1 的不可定向方程的 NP 困难性。本节固定 $n \in \mathbb{Z}$，使得 $|n| > 1$。考虑 3-划分问题的一个实例 $S = \{a_1, \ldots, a_{3k}\}$，其中$L/2 < a_i < L/4$，其中 L 是预期的和。对于 $s \in \mathbb{N}$，定义

$$A(s) = \sum_{i=1}^{s} n^{ikL} \text{ and } A^* = \sum_{i=0}^{k-1} n^{ikL(L+1)} A(L),$$

并令 $M = k^2L(L+1)$。最后，考虑群 $\mathrm{BS}(1,n)$ 上以下亏格为 $g = 1$ 的不可定向方程:

$$W = x^2(y^{-1}t^{2M}y)a^{-A^*} \prod_{i=1}^{3k} z_i^{-1} a^{A(a_i)} z_i = 1. \tag{17}$$

命题 4.6. 方程 (17) 有解，当且仅当 S 是 3-划分问题的肯定实例。

证明。“⇐” 假设 S是一个正实例。如有必要，对 $a_1, \ldots, a_{3k}$重新编号，我们可以假设对每个 $j = 0, \ldots, k-1$，都有 $a_{3j+1} + a_{3j+2} + a_{3(j+1)} = L$。定义$\alpha_1, \ldots, \alpha_{3k} \in \mathbb{N}$如下:

$$\begin{array}{lll} \alpha_1 = 0 & \alpha_4 = (L+1) & \alpha_{3i+1} = i(L+1) \\ \alpha_2 = a_1 & \alpha_5 = (L+1) + a_4 & \alpha_{3i+2} = i(L+1) + a_{3i+1} \\ \alpha_3 = a_1 + a_2 & \alpha_6 = (L+1) + a_4 + a_5 & \alpha_{3i+3} = i(L+1) + a_{3i+1} + a_{3i+2}, \end{array}$$

对于 $i = 0, 1, \ldots, k-1$。那么，$x = t^{-M}$, $y = 1$和 $z_i = t^{kL\alpha_i}$是自由群 $F(a,t)$ 中方程 (17) 的一个解。

“⇒” 假设 (17) 有一个解。首先，我们证明以下辅助命题。

引理 4.7。固定 $K, M, p_1, \ldots, p_K \in \mathbb{N}$和 $n \in \mathbb{Z}$，使得 M为偶数，$|n| > 1$, $p_1 < p_2 < \cdots < p_K < M/2$，以及 $p_{i+1} - p_i \geq K$。令 $0 \leq l \leq K$。考虑方程

$$X(n^M + 1) = (n^{p_1} + \cdots + n^{p_K}) - \sum_{i=1}^{l} \varepsilon_i n^{x_i} \tag{18}$$

未知数为 x_i、ε_i、X。满足以下条件的 (18) 的每个整数解

$$0 \leq x_1, \ldots, x_l < M \quad and \quad \varepsilon_i \in \{-1, 1\} \tag{*}$$

必然满足以下条件:

(i) $X = 0$, (ii) $\varepsilon_1 = \cdots = \varepsilon_l = 1$,

(iii) $l = K$ *and* $\{x_1, \ldots, x_l\} = \{p_1, \ldots, p_K\}$.

证明。令 l 为满足 (*) 的 (18) 的解所对应的最小数目。当 $l = 0$ 时不存在这样的解；而当 $l = K$ 时，显然有一个解 $X = 0, \varepsilon_i = 1, x_i = p_i$。因此，我们可以假设 $l \in \{1, 2, \ldots, K\}$。下面证明 $l = K$。

设 x_i、ε_i、X 是方程 (18) 的一个解，且满足 (*)。若 $\varepsilon_i n^{x_i} + \varepsilon_j n^{x_j} = 0$，那么消去 $\varepsilon_i n^{x_i}$ 和 $\varepsilon_j n^{x_j}$ 并重新排列各项后，我们可使 l 减少 2，这与最小性矛盾。因此，同一个幂不能以相反的符号出现两次。类似地，若对 n 个互不相同的指标 i_1、.....、i_n，有 $x_{i_1} = \cdots = x_{i_n} = s$，那么根据上述论证，$\varepsilon_{i_1} = \cdots = \varepsilon_{i_n}$，并且我们可以进行代换

$$\begin{aligned} &\varepsilon_{i_1} n^{x_{i_1}} + \cdots + \varepsilon_{i_n} n^{x_{i_n}} \to \varepsilon_{i_1} n^{s+1} && \text{若 } s < M-1, \\ &\varepsilon_{i_1} n^{x_{i_1}} + \cdots + \varepsilon_{i_n} n^{x_{i_n}} \to -\varepsilon_{i_1} && \text{若 } s = M-1, \end{aligned}$$

（因为 $n^M \equiv -1$（模 $n^M + 1$））， 从而使项数减少 $n - 1$。在这两种情况下， l 的最小性都被推翻，因此我们证明了每个幂至多出现 $n - 1$ 次，且符号始终相同。令 $I = \{i \mid \varepsilon_i = 1\}$、 $J = \{i \mid \varepsilon_i = -1\}$，这意味着

$$\sum_{i \in I} n^{x_i}, \sum_{i \in J} n^{x_i} < \sum_{\delta=1}^{K} (n-1) n^{M-\delta}, \tag{19}$$

并且，数 $\sum_{i \in I} n^{x_i}$ 和 $\sum_{i \in J} n^{x_i}$ 的底数为 n 的表示（底数可以为负）中的数位之和分别为 $|I|$ 和 $|J|$。注意到 (18) 蕴含同余式

$$\sum_{i \in I} n^{x_i} \equiv n^{p_1} + \cdots + n^{p_K} + \sum_{i \in J} n^{x_i} \pmod{n^M + 1}. \tag{20}$$

关于 $p_1, \ldots, p_K$ 的假设确保了 $p_K < M - K$；结合 (19)，可知 (20) 两边都介于 0 和 $n^M + 1$ 之间。因此，该同余式实际上是一个等式，从而证明了 $X = 0$。现在我们可以考虑方程

$$\sum_{i \in I} n^{x_i} = n^{p_1} + \cdots + n^{p_K} + \sum_{i \in J} n^{x_i}. \tag{21}$$

显然， $|J| < K$，因为 $|I| + |J| \le K$ 和 I 必须非空。用底数为 n 表示时，数 $n^{p_1} + \cdots + n^{p_K}$ 可表示为 K 个 1，中间以若干串 $K - 1$ 个 0 隔开。容易看出，将少于 K 个 n 的幂加到这个数上，不可能使其数位之和减小（至少需要 $(n-1)$ 个 K 的幂才能做到这一点）。因此，等式右边的底数为 n 的数位之和至少为 K，从而证明了 $|I| = K, J = \emptyset$ 和 $l = K$。底数为 n 表示的唯一性意味着，唯一的解是（相差一个指标的排列） $x_i = p_i$，证明完毕。□

为完成命题 4.6 的证明，设 x, y, z_i 是方程 (17) 的一个解。不难看出，可以作出以下假设:

对某个 $v_1 \in \mathbb{Z}[\frac{1}{n}]$， • $x = (v_1, -M)$;
对某个 $v_2 \in \mathbb{Z}[\frac{1}{n}]$， • $y = (v_2, 0)$;
• $z_i = t^{u_i} = (0, u_i)$ 对每个 $i = 1, \ldots, 3k$ 均成立。

因此，我们有

$$\begin{aligned} x^2y^{-1}t^{2M}y &= (v_1(1+n^M), -2M)(v_2(n^{-2M}-1), 2M) \\ &= (v_1(1+n^M) + v_2(1-n^{2M}), 0) = ((v_1 + v_2(1-n^M))(1+n^M)), 0). \end{aligned}$$

令 $X = v_1 + v_2(1-n^M)$，由此我们得到方程

$$\begin{aligned} X(1+n^M) &= A^* - \sum_{i=1}^{3k} n^{u_i} A(a_i) \\ &= \sum_{i=0}^{k-1} n^{ikL(L+1)}(n^{kL} + n^{2kL} + \cdots + n^{LkL}) - \sum_{i=1}^{3k} n^{u_i}\left(n^{kL} + n^{2kL} + \cdots + n^{a_i kL}\right) \end{aligned}$$

通过直接计算（17）的第一分量可得。必要时，两边同乘 n 的非负次幂，我们可以假设 $X \in \mathbb{Z}$，显然，引理 4.7 的假设均得到满足。因此，应用引理 4.7 可知，和式 A^* 与 $\sum_{i=1}^{3k} n^{u_i} A(a_i)$ 都包含相同的 Lk 个 n 的幂。现在，采用命题 4.3 证明中使用的相同步骤（即比较幂并求解 u_i），可知 S 是一个正实例，证明完成。□

推论 4.8. 当 $|n| > 1$ 时，BS(1, n) 上属 1 的不可定向方程的丢番图问题是强 NP 困难的。

5. Complexity upper bounds for quadratic equations over BS(1, n)

本节将对 BS(1, n) 上若干类二次方程的丢番图问题进行计算复杂性分类。我们证明，对于亏格为 $g \geq 1$ 的可定向方程和亏格为$g \geq 2$的不可定向方程，DP(BS(1, n)) 可在线性时间内判定；而当问题限于球面方程或亏格 1 的不可定向方程时，它是 NP 完全。结合定理 1.2，这些结果证明了定理 1.1。我们还证明定理 1.3（分别针对上述每种情形）。请注意，在某些情形下，可以改进$O(|W|^3)$ 解的界（例如，当问题限于亏格大于 2 的不可定向方程时，我们可以保证存在一个为 $O(|W|)$ 的解）；详情见定理 1.3 证明中的各个情形。本节将多次用到以下引理。

引理 5.1. 设 $u =$最大公约数$(v_1, \ldots, v_k)$，其中 $v_1, \ldots, v_k \in \mathbb{N}$。则

$$n^u - 1 = \gcd(n^{v_1} - 1, \ldots, n^{v_k} - 1). \tag{22}$$

证明. 对于任意 $a, b \in \mathbb{N}$，满足 $b \geq a > 0$，有 $n^{b-a} - 1 = (n^b - 1) - n^{b-a}(n^a - 1)$，这意味着

$$\gcd(n^a - 1, n^b - 1) = \gcd(n^a - 1, n^{b-a} - 1).$$

更一般地，如果 $r = b - aq$，则

$$\gcd(n^a - 1, n^b - 1) = \gcd(n^a - 1, n^r - 1),$$

因此，可以对这些指数应用欧几里得算法，从而证明

$$\gcd(n^a - 1, n^b - 1) = n^{\gcd(a,b)} - 1.$$

这就证明了 $k = 2$ 的情形，而一般结果可由归纳法轻易得出。 □

5.1. BS(1, n) 中的球面方程。

命题 5.2. 设 $c_i = (\alpha_i, \beta_i) \in \mathbb{Z}[\frac{1}{n}] \rtimes \mathbb{Z} \cong$BS(1, n)，其中 $i = 1, \ldots, k$，且设 $\beta =$为 $|\beta_1|, \ldots, |\beta_k|$的最大公约数。那么方程

$$\prod_{i=1}^{k} z_i^{-1} c_i z_i = 1 \tag{23}$$

有解，当且仅当满足以下条件:

(i.) $\sum_{i=1}^{k} \beta_i = 0$(ii.) 存在 $x_1, \ldots, x_k \in \mathbb{Z}$，使得 $\alpha_1 n^{x_1} + \cdots + \alpha_k n^{x_k} \equiv 0$ (模 $n^{\beta} - 1$)。此外，若 (23) 有解，则它有一个大小为 $O(|W|^3)$ 的解。

证明。设 $z_i = (v_i, y_i)$ 是 (23) 的一个解。用 z_i w 共轭 c_i e 得到

$$(v_i, y_i)^{-1}(\alpha_i, \beta_i)(v_i, y_i) = (n^{y_i}(\alpha_i + v_i(n^{-\beta_i} - 1)), \beta_i),$$

因此

$$(0,0) = \prod_{i=1}^{k} (v_i, y_i)^{-1}(\alpha_i, \beta_i)(v_i, y_i) = \left(\sum_{i=1}^{k} n^{y_i - \sum_{j=1}^{i-1} \beta_j} (\alpha_i + v_i(n^{-\beta_i} - 1)), \sum_{i=1}^{k} \beta_i \right), \tag{24}$$

这立即说明条件 (i) 是必要的。令

$$v_i' = \begin{cases} n^{-\beta_i} v_i \text{ if } \beta_i > 0 \\ -v_i \text{ otherwise} \end{cases}$$

使得 $v_i(n^{-\beta_i} - 1) = -v_i'(n^{|\beta_i|} - 1)$，并令 L 为充分大的非负整数，使得对于 $i = 1$、... ...、k，均有 $n^{L + y_i - \sum_{j=1}^{i-1} \beta_j} v_i' \in \mathbb{Z}$。令 $x_i = L + y_i - \sum_{j=1}^{i-1} \beta_j$，由 (24) 得

$$\alpha_1 n^{x_1} + \cdots + \alpha_k n^{x_k} = \sum_{i=1}^{k} n^{x_i} v_i'(n^{|\beta_i|} - 1), \tag{25}$$

其中右侧是 $n^{|\beta_i|} - 1$ 的整数倍之和。应用引理 5.1 即可证明 (ii) 成立。

反过 来，假设 (i) 和 (ii) 成立，因此存在整数 x_1、.....、x_k，使得

$$\alpha_1 n^{x_1} + \cdots + \alpha_k n^{x_k} \equiv 0 \pmod{n^{\beta} - 1}. \tag{26}$$

我们分三种情况讨论。

情形 1：假设 $\beta_1 = \cdots = \beta_k = 0$（这意味着 $\beta = 0$），于是同余 (26) 变成了形式为 (11) 的方程。显然，在这种情况下，$z_i = t^{x_i}$ 是 (23) 的一个解，并且（将 α_i 乘以 $n^{|W|}$ 以确保系数为整数）定理 4.1 保证存在一个解，其

$$\begin{aligned} 0 \leq x_1, \ldots, x_k &\leq \sum_{i=1}^{k} \log_{|n|}(|\alpha_i||n|^{|W|} + 1) \leq \sum_{i=1}^{k} \log_{|n|}(|n|^{2|W|} + 1) \\ &< k(2|W| + 1) \leq 2|W|(|W| + 1). \end{aligned}$$

因此，解的大小为 $\sum_{i=1}^{k} |z_i|$ O（$|W|^3$）。

情形 2：假设至少有一个 β_i 非零，因此 $\beta \neq 0$ 并且

$$\alpha_1 n^{x_1} + \cdots + \alpha_k n^{x_k} = h(n^\beta - 1)$$

对于某个 $h \in \mathbb{Z}$。由于 $n^\beta \equiv 1$ 模 $(n^\beta - 1)$，我们可以假设 $0 \leq x_i < \beta$，因此

$$|h| \leq \frac{n^\beta}{n^\beta - 1} \sum_{i=1}^{k} |\alpha_i| \leq 2 \sum_{i=1}^{k} |n|^{|c_i|} \leq 2 \prod_{i=1}^{k} |n|^{|c_i|+1} < 2|n|^{|W|},$$

其中第二个不等式由引理 2.2 得出。根据引理 2.7 和引理 5.1，存在$s_1, \ldots, s_k \in \mathbb{Z}$ 使得

$$\alpha_1 n^{x_1} + \cdots + \alpha_k n^{x_k} = h \sum_{i=1}^{k} s_i (n^{|\beta_i|} - 1)$$

with

$$|s_i| < \sum_{i=1}^{k} (|n|^{|\beta_i|} + 1) < k + \prod_{i=1}^{k} |n|^{|\beta_i|+1} \leq |W| + |n|^{|W|} < 2n^{|W|}$$

（再次使用引理 2.2）。令

$$v_i = \begin{cases} n^{\beta_i - x_i} h s_i & \text{if } \beta_i > 0 \\ -n^{-x_i} h s_i & \text{otherwise} \end{cases}$$

$$y_i = x_i + \sum_{j=1}^{i-1} \beta_j$$

我们看到 $z_i = (v_i, y_i)$ 是 (24) 的一个解（因此也是 (23) 的解）。由引理 2.3（使用上文得到的 $|s_i|$ 和 $|h|$ 的界），(v_i, y_i) 可以表示为一个由$\{a, t\}$ 组成的词，其长度小于

$$\begin{aligned} 2|n|(1 + \log_{|n|} |hs_i|) + 2x_i + 2|\beta_i| + |y_i| &< 2|n|(3 + 2|W|) + 3\beta + 2 \sum_{j=1}^{i} |\beta_j| \\ &\leq 2|n|(3 + 2|W|) + 5|W|, \end{aligned}$$

即 $O(|W|)$。因此，整个解的大小为 $O(k|W|) = O(|W|^2)$。

□

推论 5.3. 球面方程的丢番图问题

$$W = \prod_{i=1}^{k} z_i^{-1} c_i z_i = 1$$

在 BS(1, n) 上是 NP 完全。此外，球面方程类满足定理 1.3。

证明。推论 4.5 证明了 NP 困难性，而命题 5.2 中的条件显然可以构成证书，从而证明该问题属于 NP。命题 5.2 也确立了定理 1.3 中的解的大小上界。□

5.2. O 亏格为 $g \geq 1$ 的可定向方程。考虑一个亏格为 n

$$W = \prod_{j=1}^{g} [x_j, y_j] \prod_{i=1}^{k} z_i^{-1} c_i z_i = 1 \tag{27}$$

$g \geq 1$、系数为 $c_i \in \mathrm{BS}(1, n)$、变量为 x_j, y_j, z_i 的方程。

命题 5.4。方程 (27) 有解，当且仅当

$$\sigma_t\left(\prod_{i=1}^{k} c_i\right) = 0 \quad and \quad \sigma_a\left(\prod_{i=1}^{k} c_i\right) \ is \ a \ multiple \ of \ n-1. \tag{28}$$

因此，方程 (27) 的丢番图问题可在线性时间内判定。

证明。容易看出，$\prod_{i=1}^{k} c_i$ 满足引理 2.4 的条件，当且仅当 $\prod_{i=1}^{k} z_i^{-1} c_i z_i$ 满足这些条件（对任意 z_i 的取值）。因此，由引理 2.5 可知，$W = 1$ 有解，当且仅当 $\prod_{i=1}^{k} c_i$ 属于导出子群，而这又当且仅当条件 (28) 成立。这些条件显然可以在线性时间内检验。□

定理 1.3 关于亏格为 $g \geq 1$ 的可定向方程的证明。如果 $W = 1$ 是一个形如 (27) 且有解的方程，那么 $\prod_{i=1}^{k} c_i \in \mathrm{BS}(1, n)'$，并且对于满足界限条件的某些 $p, K \in \mathbb{Z}$，有 $\prod_{i=1}^{k} c_i = t^p a^{K(n-1)} t^{-p}$

$$|K(n-1)| < |W||n|^{|W|} \quad \text{and} \quad 0 \leq p \leq |W|$$

根据引理 2.1。这得到一个解，其中 $x_1 = t$、$y_1 = a^{-K} t^{-p}$ 以及所有其他变量都等于 1。由 $|K|$ 和 p的界可知，$a^{-K} t^{-p}$ 可以表示为长度为 $O(|W|)$ 的词，从而完成此情形的证明。□

5.3. 不可定向方程。在本节中，我们证明：对于亏格 $g \geq 2$，不可定向二次方程的丢番图问题可以在线性时间内求解；对于亏格 $g = 1$，只要 $|n| > 1$，该问题就是 NP 完全的。我们首先考虑亏格 1 的情形。

5.3.1. 亏格 $g = 1$。下面是命题 5.2 的不可定向版本。

命题 5.5。设 $c_i = (\alpha_i, \beta_i) \in \mathbb{Z}[\frac{1}{n}] \rtimes \mathbb{Z}$（$i = 1, \ldots, k$），设 $\beta =$ 为 $\gcd(|\beta_1|, \ldots, |\beta_k|)$，并设 $\beta_x = -\frac{1}{2} \sum_{i=1}^{k} \beta_i$。则方程

$$x^2 \prod_{i=1}^{k} z_i^{-1} c_i z_i = 1 \tag{29}$$

有解当且仅当满足以下条件

(i.) $\sum_{i=1}^{k} \beta_i \equiv 0$（模 2）(ii.) 存在 $x_1, \ldots, x_k \in \mathbb{Z}$，使得

$\alpha_1 n^{x_1} + \cdots + \alpha_k n^{x_k} \equiv 0$（模 K），

其中 $K =$ 最大公约数$(n^{|\beta_x|} + 1, n^{\beta} - 1)$。此外，如果 (29) 有解，那么它有一个满足 $O(|W|^3)$ 的解。

证明。假设 $x=(\alpha_x,\beta_x)$，$z_i=(v_i,y_i)$ 是 (29) 的一个解。与引理 5.2 的证明一样，直接计算可得

$$\left(\alpha_x(n^{-\beta_x}+1)+n^{-2\beta_x}\sum_{i=1}^{k}n^{-\sum_{j=1}^{i-1}\beta_j}n^{y_i}(\alpha_i+v_i(n^{-\beta_i}-1)),2\beta_x+\sum_{i=1}^{k}\beta_i\right)=(0,0),$$

这意味着条件 (i) 是必要的，并表明 $\beta_x=-\frac{1}{2}\sum_{i=1}^{k}\beta_i$。代入第一分量，得到

$$\alpha_x(n^{-\beta_x}+1)+\sum_{i=1}^{k}n^{\sum_{j=i}^{k}\beta_j}n^{y_i}(\alpha_i+v_i(n^{-\beta_i}-1))=0.$$

令 v_i' 如命题 5.2 中所定义，并令

$$\alpha_x'=\begin{cases}-n^{-\beta_x}\alpha_x \text{ if } \beta_x>0\\ -\alpha_x \text{ otherwise}\end{cases}$$

并令 L 满足以下条件：对于 $i=1,\ldots,k$，有 $n^L\alpha_x'\in\mathbb{Z}$ 和 $n^{L+y_i+\sum_{j=i}^{k}\beta_j}v_i'\in\mathbb{Z}$。然后，令$x_i=L+y_i+\sum_{j=i}^{k}\beta_j$，我们得到

$$\alpha_1n^{x_1}+\cdots+\alpha_kn^{x_k}=n^L\alpha_x'(n^{|\beta_x|}+1)+\sum_{i=1}^{k}n^{x_i}v_i'(n^{|\beta_i|}-1). \tag{30}$$

由引理 5.1 可知，(ii) 成立。

反过来，假设 (i) 和 (ii) 成立，因此存在整数 $x_1,\ldots,x_k$，使得

$$\alpha_1n^{x_1}+\cdots+\alpha_kn^{x_k}\equiv 0 \pmod K \tag{31}$$

其中 $K=$最大公约数$(n^{|\beta_x|}+1,n^{\beta}-1)$。我们考虑以下两种情况。

情形 1：假设 $\beta_1=\cdots=\beta_k=0$（因此 $\beta=\beta_x=0$）。那么 $K=n^{|\beta_x|}+1=2$，我们可以通过令 $\alpha_x'=\frac{1}{2}\sum_{i=1}^{k}\alpha_in^{x_i}$和 $v_1'=\cdots=v_k'=0$来求解（30）。按照命题 5.2 的证明，我们由此得到一个 O（$|W|^3$）的解。

情形 2：假设至少有一个 β_i 非零，因此 $\beta\neq 0$。根据引理 2.7 和引理 5.1，存在 s_x、s_1、.....、s_k、$h\in\mathbb{Z}$，使得

$$\alpha_1n^{x_1}+\cdots+\alpha_kn^{x_k}=h\left(s_x(n^{\beta_x}+1)+\sum_{i=1}^{k}s_i(n^{|\beta_i|}-1)\right)$$

其中 $|s_x|$、$|s_i|<|n|^{|\beta_x|}+1+\sum_{i=1}^{k}(|n|^{|\beta_i|}+1)<k+1+\prod_{i=1}^{k}|n|^{|\beta_i|}\leq|W|+|n|^{|W|}$。我们得到的 h 界与命题 5.2 证明中情形 2 的界相同，通过类似的论证可得到一个 O（$|W|^2$）的解。

□

推论 5.6. 属 1 的非定向方程的丢番图问题

$$W=x^2\prod_{i=1}^{k}z_i^{-1}c_iz_i=1$$

关于 $\mathbf{BS}(1,\ n)$ 是 **NP**-完全的。此外，这类方程满足定理 1.3。[17]

5.3.2. 亏格 $g \geq 2$。

命题 5.7。非定向方程

$$W = x_1^2 \cdots x_g^2 \prod_{i=1}^{k} z_i^{-1} c_i z_i = 1 \tag{32}$$

亏格为 $g \geq 2$ 、未知数为 x_i、 z_i 的方程在 BS(1, n) 中有解，当且仅当以下条件成立

$$\sigma_t\left(\prod_{i=1}^{k} c_i\right) \ is \ even \ \wedge \left[n \ is \ even \ \vee \ \sigma_a\left(\prod_{i=1}^{k} c_i\right) \ is \ even \right]. \tag{33}$$

证明。令 $S = \langle x^2 \mid x \in \text{BS}(1, n) \rangle$ 为由平方生成的词子群。由于S包含导出子群 BS(1, n)′，因此 $\prod_{i=1}^{k} z_i^{-1} c_i z_i \in S$当且仅当$\prod_{i=1}^{k} c_i \in S$。于是，根据引理 2.6， $W = 1$有解当且仅当 $\prod_{i=1}^{k} c_i \in S$。根据 (7)，这当且仅当条件 (33) 成立。□

推论 5.8. BS(1, n) 中亏格为 $g \geq 2$ 的不可定向方程的丢番图问题可在线性时间内判定。如果存在解，则存在一个大小为$O(|W|)$ 的解。

注意，定理 1.1 可由推论 4.5、5.3、5.6 和 5.8，连同命题 5.4 和定理 1.2 得出。

References

[1] G. Baumslag 和 D. Solitar。某些双生成元单关系非霍普夫群。《美国数学会通报》，68:199–201，1962年。[2] M. Casals-Ruiz 和 I. Kazachkov。关于群自由积上的方程组。《代数学杂志》，333(1):368–426，2011年。[3] L. Ciobanu、D. Holt 和 S. Rees。几乎直积群中的方程。《代数学杂志》，545:88–99，2020年。Charles Sims 纪念专辑。[4] M. Culler。利用曲面求解自由群中的方程。《拓扑学》，20(2):133–145，1981年。[5] A. Duncan、A. Evetts、D. F. Holt 和 S. Rees。利用 EDT0L 系统求解可解鲍姆斯拉格-索利塔尔群中的某些方程，2023年。[6] M. Garey 和 J. Johnson。《计算机与难解性：NP 完全性理论指南》。W. H. Freeman，1979年。[7] R. I. Grigorchuk 和 P. F. Kurchanov。关于自由群中的二次方程。载于《纪念 A. I. Malcev 的国际代数会议论文集》，《当代数学》第131卷，第159–171页。美国数学会，1992年。[8] R. I. Grigorchuk 和 I. G. Lysenok。双曲群中二次方程解的描述。《代数与计算国际期刊》，02(03):237–274，1992年。[9] O. Kharlampovich、L. Lopez 和 A. Miasnikov。某些亚幂零群中的丢番图问题。《计算数学》，89:2507，2020年。[10] O. Kharlampovich、I. Lysenok、A. G. Myasnikov 和 N. Touikan。自由群上二次方程的可解性问题是 NP 完全的。《理论计算机系统》，47:250–258，2010年。[11] M. Lohrey、G. Zetzsche 和 M Ganardi。可解鲍姆斯拉格-索利塔尔群中的背包问题和幂字问题。载于第45届国际计算机科学数学基础研讨会（MFCS 2020），莱布尼茨国际信息学会议论文集第170卷，第67:1–67:15页，德国达格施图尔，2020年。Schloss Dagstuhl–Leibniz-Zentrum f¨ur Informatik。[12] R. Lyndon。自由群中的方程。《美国数学会汇刊》，9(6):445–457，1960年。

[13] I. Lysenok、A. Miasnikov 和 A. Ushakov。格里戈尔丘克群中的二次方程。《群、几何与动力学》，10:201–239，2016年。[14] I. Lysenok 和 A. Ushakov。自由后元群中的球面二次方程。《美国数学会会刊》，144:1383–1390，2016年。[15] I. Lysenok 和 A. Ushakov。自由后元群中的可定向二次方程。《代数学杂志》，581:303–326，2021年。[16] G. Makanin。自由群中的方程。《苏联科学院学报》，数学系列，46:1199–1273，1982年。（俄文，英文译本见《苏联数学学报》，21，3（1983））。[17] R. Mandel 和 A. Ushakov。带指数的代数方程组的丢番图问题。已提交；预印本见 https://arxiv.org/pdf/2210.00086.pdf。[18] G. A. Noskov。有限生成几乎可解群的初等理论。《苏联数学学报》，22(3):465，1984年。[19] A. Razborov。关于自由群中的方程组。博士候选人论文，斯捷克洛夫数学研究所，莫斯科，1987年。（俄文）。[20] V. Roman'kov。群上的方程。《群、复杂性与密码学》，4:191–239，2012年。[21] P. E. Schupp。群中的二次方程、紧曲面上的消去图以及曲面群的自同构。载于《字问题》第二卷（代数中的判定问题会议，牛津，1976年），《逻辑研究与数学基础》第95卷，第347–371页。北荷兰出版社，阿姆斯特丹，1980年。

Department of Mathematics, University of the Basque Country, Bilbao, Spain电子邮箱地址: mandel.richard@ehu.eus

Department of Mathematical Sciences, Stevens Institute of Technology, Hoboken NJ07030 电子邮箱地址：aushakov@stevens.edu