arXiv:2601.08492v1 [cs.LO] 13 Jan 2026

关于判定线性循环的常数运行时间

Florian Frohn[1], J¨urgen Giesl[1], Peter Giesl[2], 和 Nils Lommen[1]

[1] 德国亚琛，亚琛工业大学[2] 英国布莱顿，萨塞克斯大学数学系

摘要。我们研究如下形式的线性单路径循环

$$\textbf{while} \quad \varphi \quad \textbf{do} \quad \vec{x} \leftarrow A\vec{x} + \vec{b} \quad \textbf{end}$$

其中，$\vec{x}$ 是一个变量向量，循环守卫 φ 是关于变量 $\vec{x}$的线性不等式合取式，循环的更新由矩阵 A 和向量 $\vec{b}$表示。已知此类循环的终止性是可判定的。本文研究 A 具有实特征值的循环，并证明：当变量取值范围为 $\mathbb{R}$ 或 $\mathbb{Q}$时，可以判定该循环的运行时间（对所有输入而言）是否有常数上界。这是自动程序验证中的一个重要问题，因为当所有循环的运行时间均为常数时，线性 while 程序的安全性是可判定的；此外，该问题还与多阶段线性秩函数的存在性密切相关，而多阶段线性秩函数常用于终止性和复杂度分析。为评估该判定过程的实际适用性，我们还给出了相应的实现。

1 引言

我们研究如下问题的可判定性：一个线性[3] 单路径循环是否具有常数运行时间（即，该循环的运行时间是否可以对所有输入都由同一个常数界定）。

示例 1（引导性示例）。我们考虑如下形式的线性单路径循环：

$$\textbf{while} \quad 0 \le x + y \le 10 \quad \textbf{do} \quad \underbrace{\begin{pmatrix} x \\ y \end{pmatrix}}_{\vec{x}} \leftarrow \underbrace{\begin{pmatrix} 1 & 0 \\ 0 & 2 \end{pmatrix}}_{A} \begin{pmatrix} x \\ y \end{pmatrix} + \underbrace{\begin{pmatrix} 1 \\ 0 \end{pmatrix}}_{\vec{b}} \quad \textbf{end}$$

该循环仅使用线性算术、合取式循环守卫，并且循环体中没有分支。在我们的示例中，当 $0 \le x + y \le 10$ 时执行循环体。每次迭代中，x 的值增加 1，而 y 的值加倍。我们的目标是判定此类循环的运行时间是否由某个常数界定。稍后我们将证明，示例中的循环确实具有常数运行时间。

本文中，循环中出现的系数始终为有理数。[4] 关于变量的取值域 $\vec{x}$，我们重点研究定义在 $\mathbb{R}$上的循环，但我们的结果也适用于变量取值范围为 $\mathbb{Q}$的情况。

[3] 在本文中，“线性”一词指线性 *polynomials*，即形如 $c_0 + \sum_{i=1}^{d} c_i \cdot x_i$ 的函数（不同于形如 $\sum_{i=1}^{d} c_i \cdot x_i$ 的线性 *transformations*）。[4] 如果系数是代数实数且变量取值范围为 $\mathbb{R}$，我们的方法同样适用。为简便起见，我们将自己限制在有理数系数的情形。

我们的研究动机有三方面。首先，在自动复杂度分析的背景下，这项研究显然具有重要意义，因为它有助于证明常数运行时间。其次，判断一个线性循环是否存在多阶段线性秩函数(MΦRF)，可以归约为判断另一个线性循环相对于给定初始状态集合是否具有常数运行时间的问题 [5, 第 4 节。2]。因此，我们的研究是迈向解决这一长期悬而未决问题的重要一步：对于线性循环，MΦRF 的存在性是否可判定。MΦRF 对自动化终止性分析和复杂度分析都很重要，因为 MΦRF 不仅能证明终止性，还能证明循环的运行时间至多为线性 [4, 定理 7]。然而，我们的方法不考虑初始条件，因此目前还不能用于推导 MΦRF。我们计划在未来的工作中对其加以完善，以支持初始条件。第三，我们的研究对所有使用近似来处理循环的无限状态验证技术都具有意义，例如抽象解释、符号执行、递推分析、循环摘要等。这些技术在存在循环时都会利用近似来避免验证过程发散，但代价是降低精确度。相反，具有常数运行时间的循环 c 只需展开 c 次即可。因此，对于所有循环都具有常数运行时间的线性**while**程序，可达性（因而安全性）都是可判定的。

常数运行时间问题出乎意料地具有挑战性：线性循环在实数域 [28], 有理数域 [7], 和整数集 [17]上的终止性是可判定的。但即使对于那些终止性可判定性早在几十年前就已为人所知的循环类，常数运行时间问题的可判定性也远非显而易见。直观而言，这是因为所有关于线性循环终止性的可判定性结果都利用了最终单调性：对于具有非负实特征值的循环，变量值在有限次循环迭代之后便开始呈现单调变化（忽略循环守卫），而负特征值则很容易消除。对于常数运行时间问题，这种推理并不适用，因为不能忽略有限次循环迭代。

贡献： 在第 2 节正式介绍循环的概念后，我们在第 3节证明，具有实特征值的 $\mathbb{R}$ 上线性循环的常数运行时间问题是可判定的。我们的判定过程将常数运行时间问题编码为一个有效性问题，然后利用实特征值这一限制消除一次量词交替，使所得公式适用于 Fourier-Motzkin 变量消去。我们的结果可立即推广到 $\mathbb{Q}$ 上的循环，但由于使用了 Fourier-Motzkin 变量消去，无法推广到 $\mathbb{Z}$ 上的循环。对于 $\mathbb{Z}$上的循环，我们在第 $\{-1, 0, 1\}$ 节证明，特征值属于 4的线性循环的常数运行时间问题是可判定的。在第 5节，我们讨论相关工作，并在第 6 节评估我们的实现并作出总结。

2 预备知识

我们考虑如下形式的循环

$$\textbf{while} \quad \varphi \quad \textbf{do} \quad \vec{x} \leftarrow A\vec{x} + \vec{b} \quad \textbf{end} \qquad \text{(Loop)}$$

其中， $\vec{x}$ 是一个由 $d \geq 1$ 个变量组成的向量， φ 是由 $\vec{x}$ 上的线性不等式构成的合取式，形式为 $t \sim 0$，其中 $\sim \in \{>, \geq\}$、 $A \in \mathbb{Q}^{d\times d}$，且 $\vec{b} \in \mathbb{Q}^d$。有时，我们将公式 $\varphi \equiv \varphi_1 \wedge \ldots \wedge \varphi_m$ 的合取式视为集合 $\{\varphi_1, \ldots, \varphi_m\}$，从而可以对每个合取项 φ_i 写作 $\varphi_i \in \varphi$ 。对于任何包含来自 $\vec{x}$ 的变量的算术表达式 t ，我们将关于（Loop）的更新函数定义为 $\mathbf{up}(t) := t[\vec{x}/A\vec{x} + \vec{b}]$，其中 $[\vec{x}/A\vec{x} + \vec{b}]$ 表示一种替换，它将 $\vec{x}$ 中的每个变量替换为 $A\vec{x} + b$ 中对应的多项式。

循环（Loop）具有常数运行时间，当且仅当满足以下条件：

$$\exists c \in \mathbb{N}.\ \forall \vec{x} \in \mathbb{R}^d.\ \exists i \in \mathbb{N}_{\leq c}.\ \neg\varphi[\vec{x}/\mathrm{up}^i(\vec{x})] \qquad \text{(Const)}$$

这里，$\mathbf{up}^i$ 表示对 up 应用 i 次，且对于任意 $c \in \mathbb{N}$， $\mathbb{N}_{\leq c} = \{n \in \mathbb{N} \mid n \leq c\}$ 。直观地说，（Const）指出，如果对于每个可能的初始值 $\vec{x} \in \mathbb{R}^d$，循环守卫在经过 $i \leq c$ 次迭代后都不再成立，即 $\neg\varphi[\vec{x}/\mathbf{up}^i(\vec{x})]$ 成立，那么 $c \in \mathbb{N}$ 就是循环（Loop）运行时间的一个上界。

与 [10], 中一样，不失一般性，我们可以将讨论限制在非负循环（即 A 没有负特征值）。原因是，只有当Loop具有常数运行时间时，

$$\textbf{while} \quad \varphi \wedge \varphi[\vec{x}/A\vec{x} + \vec{b}] \quad \textbf{do} \quad \vec{x} \leftarrow A(A\vec{x} + \vec{b}) + \vec{b} \quad \textbf{end}$$

或者，等价地，

$$\textbf{while} \quad \varphi \wedge \varphi[\vec{x}/A\vec{x} + \vec{b}] \quad \textbf{do} \quad \vec{x} \leftarrow A^2\vec{x} + A\vec{b} + \vec{b} \quad \textbf{end} \qquad \text{(Non-Neg)}$$

具有常数运行时间。这里，循环（Non-Neg）由循环（Loop）通过串接得到；也就是说，（Non-Neg）的每次迭代对应于（Loop）连续进行的两次迭代。显然，如果 A 只有实特征值，那么 A^2 的所有特征值均为非负数。现在，推论2 可直接由 [14, 引理 18]得出。

推论 2（向非负循环的转换）。(Loop)具有常数运行时间，当且仅当(Non-Neg)具有常数运行时间。

3 具有实特征值的循环

从现在起，我们只考虑具有实特征值的循环。因此，不失一般性，借助推论 2，我们可以将讨论限制在如下形式的循环：Loop，其中 A 的所有特征值均为非负。形式如Loop的循环具有如下优势：它们存在合适的闭式，能够用每个变量对应的单个表达式来刻画 n 循环迭代的行为。这些闭式在用于终止性分析、不变式生成和复杂度分析的完备技术中得到了广泛应用（例如参见 [7, 10, 14, 15, 17–19, 25, 28]）。

本节余下部分安排如下：首先，我们在第 3.1 节介绍具有实特征值的线性循环的闭式。然后，在第 3.2 节利用这些闭式，将常数运行时间问题归约为一个有效性问题。也就是说，从此处开始，我们的目标是判定具有特定结构的一阶公式（Const_{n_0}）的有效性。算术表达式

在该公式中包含 $\vec{x}$ 所考虑循环中的变量，以及一个额外的特定变量，用作“循环计数器”。接下来，我们在第 3.3 节证明，这些算术表达式关于循环计数器的实根数量存在一个常数上界，且该上界不依赖于 $\vec{x}$的取值。在第 3.4 节中，我们利用这一事实消去（$\textsc{Const}_{n_0}$）中的最内层量词。在这一步中，所有特征值都是非负实数至关重要。消去最内层量词后，所得公式适用于 Fourier-Motzkin 变量消去的一种变体，该变体允许我们消去变量 $\vec{x}$，详见第 3.5 节和第 3.6 节。由此，我们得到一个包含多项式算术和指数算术的单变量公式。最后，我们在第 3.7 节说明如何判定此类公式的有效性。

3.1 闭式

令 $\mathbb{R}_{\mathbb{A}}$ 表示实代数数（即 $\mathbb{R}_{\mathbb{A}}$ 包含每个作为单变量非零整数系数多项式的根的实数）。此外，$\mathbb{R}_{\mathbb{A}>0}$ 表示正代数实数。与例如 [18, 定理 31] 和 [15,定义 34], 类似，对于具有非负实特征值的循环，可以计算循环的 多项式指数闭式，表示其 n次更新。其形式如下

$$\sum_{i=1}^{M} a_i(\vec{x}) \cdot b_i^n \cdot n^{e_i} \tag{PE}$$

其中 $b_i \in \mathbb{R}_{\mathbb{A}>0}$, $e_i \in \mathbb{N}$，并且 $a_i \in \mathbb{R}_{\mathbb{A}}[\vec{x}]$ 是关于变量$\vec{x}$的线性多项式。这里，我们将 a_i 与函数 $\vec{x} \mapsto a_i$ 视为相同；有时我们写作 $a_i(\vec{x})$，以明确标出变量 $\vec{x}$，其他表达式（向量）也采用相同约定。注意， b_i 是更新矩阵 A的特征值。我们强调，式（PE）中的常数都是代数数，因为非代数数的计算方式尚不明确，因此，包含此类数的闭式不适用于我们的判定过程。

要计算这样的闭式，可以考虑更新矩阵的约当标准形 $J = \operatorname{diag}(B_1, \ldots, B_N)$, 其中 A，对于适当的基变换矩阵 $S \in \mathbb{R}_{\mathbb{A}}^{d \times d}$。这里，每个约当块 B都与一个特征值 $b \in \mathbb{R}_{\mathbb{A}\geq 0}$相关联。注意，约当标准形（以及所有关于代数数的相关计算）总能在多项式时间内完成 [8]。于是， n次更新可由矩阵 $A^n = (S \cdot J \cdot S^{-1})^n = S \cdot J^n \cdot S^{-1}$ 表示（即 S和 S^{-1} 总能相互抵消）。因此，只需为 $J^n = \operatorname{diag}(B_1^n, \ldots, B_N^n$中的每个约当块计算闭式。对于每个约当块 $B \in \mathbb{R}_{\mathbb{A}\geq 0}^{d_B \times d_B}$，该闭式为

$$B^n = \begin{pmatrix} b^n & \binom{n}{1} \cdot b^{n-1} & \cdots & \binom{n}{d_B-1} \cdot b^{n-(d_B-1)} \\ 0 & b^n & \cdots & \binom{n}{d_B-2} \cdot b^{n-(d_B-2)} \\ \vdots & \vdots & \ddots & \vdots \\ 0 & \cdots & 0 & b^n \end{pmatrix} \quad \text{for all } n \in \mathbb{N}$$

如果 $b \neq 0$，或者 $B^n = 0 \in \mathbb{R}_{\mathbb{A}\geq 0}^{d_B \times d_B}$对于所有 $n \geq d_B$，如果 $b = 0$。注意，二项式系数给出了多项式指数表达式（n^{e_i}）中的多项式因子PE。此外，结合基变换矩阵 $S \in \mathbb{R}_{\mathbb{A}}^{d\times d}$，多项式（$a_i$）中的系数$\vec{x}$即可确定。

因此，对于任何仅具有非负实特征值、形式为 (Loop) 的循环，都存在一个由 d 个形式为 (PE) 的多项式指数表达式构成的向量 $\vec{cl}$，以及一个常数 $n_0 \in \mathbb{N}$，使得

$$\mathrm{up}^n(\vec{x}) = \vec{cl} \qquad \text{for all } n \in \mathbb{N} \text{ with } n \geq n_0.$$

更确切地说，n_0 是与特征值 $b = 0$ 相关联的最大约当块 B 的维数 d_B。

例 3（闭式，例*1* 续）。对于例1，我们有闭式

$$\vec{cl} = \begin{pmatrix} x+n \\ 2^n y \end{pmatrix}.$$

为了解常数 n_0 对闭式为何必不可少，请考虑以下循环

$$\textbf{while} \quad x \leq 0 \quad \textbf{do} \quad \begin{pmatrix} x \\ y \end{pmatrix} \leftarrow \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix} + \begin{pmatrix} 0 \\ 1 \end{pmatrix} \quad \textbf{end}$$

这里，$n_0 = 2$，因为更新矩阵已经是约当标准形，其唯一特征值为 0，并且它有一个大小为 2 的约当块。于是我们得到闭式 $\vec{cl} = \begin{pmatrix} 1 \\ 1 \end{pmatrix}$。然而，对于 $n \in \{0, 1\}$，我们有

$$\vec{cl}[n/0] = \begin{pmatrix} 1 \\ 1 \end{pmatrix} \neq \begin{pmatrix} x \\ y \end{pmatrix} = \mathrm{up}^0(\vec{x}) \quad \text{and} \quad \vec{cl}[n/1] = \begin{pmatrix} 1 \\ 1 \end{pmatrix} \neq \begin{pmatrix} y \\ 1 \end{pmatrix} = \mathrm{up}^1(\vec{x}).$$

3.2 从常数运行时间到有效性

现在，我们将常数运行时间问题归约为有效性问题。首先，回顾常数循环的刻画：

$$\exists c \in \mathbb{N}.\ \forall \vec{x} \in \mathbb{R}^d.\ \exists i \in \mathbb{N}_{\leq c}.\ \neg\varphi[\vec{x}/\mathrm{up}^i(\vec{x})] \qquad (\textsc{Const})$$

将 c 平移 1 后，我们得到等价公式

$$\exists c' \in \mathbb{N}.\ \forall \vec{x} \in \mathbb{R}^d.\ \exists i \in \mathbb{N}_{<c'}.\ \neg\varphi[\vec{x}/\mathrm{up}^i(\vec{x})] \qquad (\textsc{Const}_<)$$

这更适合我们后续的分析（尤其是第 3.3 节）。因此，如果（$\textsc{Const}_<$）成立，那么 $c' - 1$ 就是（Loop）运行时间的一个上界。现在我们证明（$\textsc{Const}_<$）等价于

$$\exists c \in \mathbb{N}.\ \forall \vec{x} \in \mathbb{R}^d.\ \exists i \in \mathbb{N}_{<c}.\ \neg\varphi[\vec{x}/\mathrm{up}^{n_0+i}(\vec{x})]$$

其中 n_0 的定义与第 3.1 节中的定义相同。这使我们可以直接将$^{n_0+i}(\vec{x})$替换为其闭式，因为 $i \geq 0$。为此，我们定义实例化的循环守卫

$$\psi := \varphi[\vec{x}/\vec{cl}].$$

因此，我们证明（$\textsc{Const}_<$）等价于

$$\exists c \in \mathbb{N}.\ \forall \vec{x} \in \mathbb{R}^d.\ \exists i \in \mathbb{N}_{<c}.\ \neg\psi[n/n_0 + i], \qquad (\textsc{Const}_{n_0})$$

并且，如果 ($\textsc{Const}_{n_0}$) 成立，那么 $n_0 + c - 1$ 就是 (Loop) 的运行时间上界。

证明 (Const$_<$) 与 (Const$_{n_0}$) 的等价性： 为了证明 (Const$_<$) 和 (Const$_{n_0}$) 等价，我们首先证明 (Const$_{n_0}$) 推出 (Const$_<$)。为此，假设 (Const$_{n_0}$) 成立，但 (Const$_<$) 不成立。因此，存在一个 $c \in \mathbb{N}$ 使得

$$\forall \vec{x} \in \mathbb{R}^d.\ \exists i \in \mathbb{N}_{<c}.\ \neg\psi[n/n_0 + i]. \qquad (\text{Const}^{in}_{n_0})$$

由于（Const$_<$）不成立，对于 $c' = n_0 + c$，存在一个 $\vec{x} \in \mathbb{R}^d$，使得

$$\forall i \in \mathbb{N}_{<n_0+c}.\ \varphi[\vec{x}/\text{up}^i(\vec{x})],$$

这与（$\neg\varphi[\vec{x}/^{\ n_0+i}\ \vec{x}\ ]$ Const$^{in}_{n_0}$ $i \geq 0$ $\neg\psi[n/n_0 + i] \equiv$）矛盾，因为对于每个，我们都有 up()。

为了说明（Const$_<$）蕴含（Const$_{n_0}$），假设（Const$_<$）成立，但（Const$_{n_0}$）不成立。因此，存在一个 $c' \in \mathbb{N}$，使得

$$\forall \vec{y} \in \mathbb{R}^d.\ \exists i \in \mathbb{N}_{<c'}.\ \neg\varphi[\vec{x}/\text{up}^i(\vec{y})]. \qquad (\text{Const}^{in}_{<})$$

由于（Const$_{n_0}$）不成立，对于 $c = c'$，存在一个 $\vec{x} \in \mathbb{R}^d$，使得

$$\forall i \in \mathbb{N}_{<c'}.\ \psi[n/n_0 + i]. \qquad (\dagger)$$

现在，我们在（Const$^{in}_<$）中令 $\vec{y} = \text{up}^{n_0}(\vec{x})$，也就是说，存在一个 $i \in \mathbb{N}_{<c'}$，使得 $\neg\varphi[\vec{x}/\text{up}^i(\vec{y})]$,，或者等价地，$\neg\varphi[\vec{x}/\text{up}^{n_0+i}(\vec{x})]$ 成立。这与（†）矛盾，因为对于每个 $i \geq 0$，我们再次有 $\psi[n/n_0 + i] \equiv \varphi[\vec{x}/\text{up}^{n_0+i}(\vec{x})]$。

虽然 (Const$_<$) 表示循环守卫必须在前 c' 次迭代内失效，但 (Const$_{n_0}$) 会“忽略”前 n_0 次迭代。这使我们能够使用仅对 $n \geq n_0$ 有效的闭式。

例4（从常数运行时间到有效性，例 3 续）。对于例1，接下来需要判断以下命题是否有效:

$$\exists c \in \mathbb{N}.\ \forall x, y \in \mathbb{R}.\ \exists i \in \mathbb{N}_{<c}.\ \neg\left(0 \leq x + i + 2^i y \leq 10\right). \qquad (\text{Val})$$

此外，如果 (Val) 成立，那么 $c - 1$ 就是例 1运行时间的一个上界。

3.3 实根个数有界

回顾一下，(Const$_{n_0}$) 表示存在一个 $c \in \mathbb{N}$，使得对于所有初始值 $\vec{x}$，都存在一次迭代 n，满足 $n_0 \leq n < n_0 + c$，此时循环守卫不成立。因此，我们需要考虑将 n 中的自然数从 n_0 到 $n_0 + c - 1$ 逐一代入。判断 (Const$_{n_0}$) 是否有效时，问题在于 c 尚未知晓。我们的目标是将 (Const$_{n_0}$) 替换为

$$\exists m \in \mathbb{N}.\ \forall \vec{x} \in \mathbb{R}^d.\ \bigvee_{j=0}^{rb} \neg\psi[n/n_0 + j \cdot m], \qquad (\text{QE})$$

其中，我们只检查 n 的 rb $+1$ 个实例化。这里，rb 是一个只取决于 ψ、而不取决于 $\vec{x}$ 的实际实例化的数。因此，我们的目标是替换

存在量词公式 $\exists i \in \mathbb{N}_{<c}.\ \neg\psi[n/n_0+i]$ 它取决于（未知的）值 c 为析取式 $\bigvee_{j=0}^{rb} \neg\psi[n/n_0+j\cdot m]$，其中 rb 是已知且固定的。因此，为了消去 (CONST_{n_0}) 中的内层存在量词，我们证明只需考虑固定数量的“采样点”，而非所有值 $i \in \mathbb{N}_{<c}$。这里，（受存在量词约束的）变量 m 用作这些“采样点”之间的距离。

为了确定数值 rb，将 n 实例化为实数，而非仅限于自然数。接着，以如下方式选取数值 rb：对于任意实数向量 $\vec{v}$，公式 $\psi[\vec{x}/\vec{v}]$（其中仅含变量 n）的不等式中的表达式至多有 rb 个实根。请注意，若不限制特征值为非负实数，实根的数量没有上界。

为了定义 rb，对于任意形如 (PE) 的多项式指数表达式 t，我们首先定义它的根数上界。这里，rootbound(t) 仅取决于加数的数量 M 和指数 e_i，而 rootbound(t) 不取决于 $\vec{x}$。下面的引理表明，对于每个值 $\vec{v} \in \mathbb{R}^d$，rootbound(t) 都是表达式 $t[\vec{x}/\vec{v}]$ 的实根数量的上界。

引理 5（实根数上界）。设 $\vec{v} \in \mathbb{R}^d$，并令

$$t = \sum_{i=1}^{M} a_i(\vec{x}) \cdot b_i^n \cdot n^{e_i}$$

是一个多项式指数表达式，使得 $t[\vec{x}/\vec{v}]$ 不是零多项式。那么

$$\mathsf{rootbound}(t) := M - 1 + \sum_{i=1}^{M} e_i$$

是 $t[\vec{x}/\vec{v}]$的实根个数的一个上界。

证明。 如 [26], 对于任意形式为 s 的表达式

$$\sum_{i=1}^{M'} p_i(n) \cdot b_i^n, \tag{1}$$

其中每个 b_i 都是唯一的，且每个 $p_i(n)$ 都是 n上的多项式，我们定义

$$ord(s) := \sum_{i=1}^{M'} (\mathsf{degree}(p_i(n)) + 1) = M' + \sum_{i=1}^{M'} \mathsf{degree}(p_i(n)). \tag{2}$$

令 $\vec{v} \in \mathbb{R}^d$ 任意但固定。那么我们可以将其改写为

$$t' = t[\vec{x}/\vec{v}] = \sum_{i=1}^{M} a_i(\vec{v}) \cdot b_i^n \cdot n^{e_i}$$

化为（1）的形式，因此根据 [26, 第五部分，第1章，编号 75], ，它至多有ord（t'）-1个实根（其中t'不含除 n之外的其他变量）。由于 $M' \le M$和

$\sum_{i=1}^{M'}$ 次数（p_i（n））$\leq \sum_{i=1}^{M} e_i$，这意味着 t' 由于（2），至多有 $M-1+\sum_{i=1}^{M} e_i$个实根。由于这个上界与 $\vec{v}$无关，结论得证。□

现在我们可以定义所需的数 rb。

定义 6（循环守卫的根界）。我们将实例化循环守卫 ψ 的根界定义为

$$rb := \sum_{(t \sim 0) \in \psi} \mathsf{rootbound}(t),$$

其中 $\sim \in \{>, \geq\}$，也就是说，这里我们考虑合取式 ψ 中出现的所有形如 $t > 0$ 和 $t \geq 0$ 的不等式。

例 7（根界，例 4 续）。对于例 1，$\psi = \varphi[\vec{x}/cl]$ 是

$$0 \leq x + n + 2^n y \leq 10 \quad \equiv \quad x + n + 2^n y \geq 0 \ \wedge \ 10 - x - n - 2^n y \geq 0.$$

这里，我们有

$$\mathsf{rootbound}(x + n + 2^n y) = \mathsf{rootbound}(10 - x - n - 2^n y) = 3$$

因为 $M = 3$ 和 $\sum_{i=1}^{3} e_i = 1$，因此 $\mathbf{rb} = 3 + 3 = 6$。

3.4 消除最内层量词

现在我们证明 ($\textsc{Const}_{n_0}$) 等价于

$$\exists m \in \mathbb{N}.\ \forall \vec{x} \in \mathbb{R}^d.\ \bigvee_{j=0}^{rb} \neg\psi[n/n_0 + j \cdot m], \tag{QE}$$

并且如果 (QE) 成立，那么 $n_0 + \mathbf{rb} \cdot m$ 是 (Loop) 的运行时间上界，前提仍然是所有特征值都是非负实数。

回想一下，(QE) 表示存在一个距离 m，使得对于 $\vec{x}$ 的所有初始值，经过 n_0、$n_0+1\cdot m$、.....或 $n_0+\mathbf{rb} \cdot m$ 次迭代后，守卫条件会被违反。

证明 ($\textsc{Const}_{\boldsymbol{n_0}}$) 和 (QE) 等价：要理解为什么 ($\textsc{Const}_{n_0}$) 和 (QE) 等价，请注意

$$\text{(QE) implies } (\textsc{Const}_{n_0}) \text{ by choosing } c = rb \cdot m + 1. \qquad (\text{QE} \Rightarrow \textsc{Const}_{n_0})$$

因此，$n_0 + c - 1 = n_0 + \mathbf{rb} \cdot m$ 是（Loop）运行时间的一个上界。

为证明 ($\textsc{Const}_{n_0}$) 蕴含 (QE)，假设 ($\textsc{Const}_{n_0}$)，也就是说，存在一个$c \in \mathbb{N}$，使得 $\forall \vec{x} \in \mathbb{R}^d.\ \exists i \in \mathbb{N}_{<c}.\ \neg\psi[n/n_0 + i]$。那么对于每个 $j \in \mathbb{N}$，我们有：

$$\begin{aligned} & \forall \vec{x} \in \mathbb{R}^d.\ \exists i \in \mathbb{N}_{<c}.\ \neg\psi[n/n_0 + i] && \text{(for some } c \in \mathbb{N} \text{ by } (\textsc{Const}_{n_0})) \\ \iff\ & \forall \vec{x} \in \mathbb{R}^d.\ \exists i \in \mathbb{N}_{<c}.\ \neg\varphi[\vec{x}/\vec{cl}][n/n_0 + i] && \text{(def. of } \psi) \end{aligned}$$

$$\begin{aligned}
&\iff \forall \vec{x} \in \mathbb{R}^d.\ \exists i \in \mathbb{N}_{<c}.\ \neg\varphi[\vec{x}/\vec{cl}[n/n_0+i]] && \text{（因为 } n \text{ 不出现在 } \varphi \text{ 中）}\\
&\iff \forall \vec{x} \in \mathbb{R}^d.\ \exists i \in \mathbb{N}_{<c}.\ \neg\varphi[\vec{x}/\text{向上}^{n_0+i}(\vec{x})] && \text{（}\vec{cl}\text{的定义，作为 } i \geq 0\text{）}\\
&\implies \forall \vec{x} \in \mathbb{R}^d.\ \exists i \in \mathbb{N}_{<c}.\ \neg\varphi[\vec{x}/\text{up}^{n_0+j\cdot c+i}(\vec{x})] && \text{(for any } j \in \mathbb{N} \text{ (‡))}\\
&\iff \forall \vec{x} \in \mathbb{R}^d.\ \exists i \in \mathbb{N}_{<c}.\ \neg\varphi[\vec{x}/\vec{cl}[n/n_0+j\cdot c+i]] && \text{(def. of } \vec{cl}\text{, as } j\cdot c+i \geq 0)\\
&\iff \forall \vec{x} \in \mathbb{R}^d.\ \exists i \in \mathbb{N}_{<c}.\ \neg\varphi[\vec{x}/\vec{cl}][n/n_0+j\cdot c+i] && \text{（因为 } n \text{ 不出现在 } \varphi\text{中）}\\
&\iff \forall \vec{x} \in \mathbb{R}^d.\ \exists i \in \mathbb{N}_{<c}.\ \neg\psi[n/n_0+j\cdot c+i] && \text{(def. of } \psi\text{)}
\end{aligned}$$

对于步骤（‡），$\vec{x}$ 再次是全称量化的，也就是说，我们可以像证明（$\vec{x}$ 蕴含 $(^{j\cdot c})$ 时那样，用 up$\vec{x}$(Const$_<$) 实例化Const$_{n_0}$；当时，我们用 up $\vec{y}$ ()$\vec{x}$实例化了全称量化变量。因此，（Const$_{n_0}$）蕴含

$$\forall \vec{x} \in \mathbb{R}^d.\ \bigwedge_{j=0}^{rb} \exists i \in \mathbb{N}_{<c}.\ \neg\psi[n/n_0+j\cdot c+i]. \qquad \text{(InIntervals)}$$

因此，(InIntervals)成立，当且仅当对于 $\vec{x}$ 的所有初始值以及所有 $0 \leq j \leq$rb，循环守卫在经过 $n_0+j\cdot c$、$n_0+j\cdot c+1$、.....或 $n_0+(j+1)\cdot c-1$ 次迭代后被违反。

为了证明 (InIntervals) 蕴含 (QE)，我们假设 (InIntervals) 成立而 (QE) 不成立，并推导出矛盾。如果 (QE) 不成立，那么存在一个 $\vec{v} \in \mathbb{R}^d$，使得

$$\bigwedge_{j=0}^{rb} \psi[n/n_0+j\cdot c][\vec{x}/\vec{v}] \qquad \text{(AtBorders)}$$

在 (QE) 中选择 $m = c$。于是，根据介值定理，对于每个 $0 \leq j \leq$ rb，至少存在一个 $(t_j \sim_j 0) \in \psi$，其 $\sim_j \in \{>, \geq\}$ 满足 $t_j[\vec{x}/\vec{v}]$ 在区间内有一个实根

$$[n_0+j\cdot c,\ n_0+(j+1)\cdot c-1] \qquad (3)$$

由（InIntervals）可知，如果我们考虑将 n 实例化为实数，而不仅仅是自然数。原因在于，（AtBorders）意味着对所有 $(t \sim 0) \in \psi$，都有 $t[\vec{x}/\vec{v}][n/n_0+j\cdot c] \sim 0$；而（InIntervals）意味着存在一个值 $k \in [n_0+j\cdot c,\ n_0+(j+1)\cdot c-1]$，以及一个 $(t_j \sim_j 0) \in \psi$，使得 $t_j[\vec{x}/\vec{v}][n/k] \sim_j 0$ 不成立。于是，对于某个 k_0，我们还必须有 $t_j[\vec{x}/\vec{v}][n/k_0] = 0 \neq t_j[\vec{x}/\vec{v}][n/k_{\neq 0}]$，$k_{\neq 0} \in [n_0+j\cdot c,\ n_0+(j+1)\cdot c-1]$，因为 $t_j[\vec{x}/\vec{v}]$ 是关于变量 n 的连续函数。[5] 换句话说，对于每个区间（3），都存在一个 $t_j[\vec{x}/\vec{v}]$，它在区间的"边界"处满足 $t_j[\vec{x}/\vec{v}] \sim_j 0$，却在区间内部违反 $t_j[\vec{x}/\vec{v}] \sim_j 0$。因此，我们有 $t_j[\vec{x}/\vec{v}] \neq 0$（即 $t_j[\vec{x}/\vec{v}]$ 不是零多项式），并且它在该区间内必有一个实根。因此，所有非零表达式 $t[\vec{x}/\vec{v}]$ $(t \sim 0) \in \psi$ 的实根数量之和至少为 rb $+1$，即

$$\sum_{\substack{(t\sim 0)\in\psi \\ t[\vec{x}/\vec{v}]\neq 0}} |\mathsf{roots}(t[\vec{x}/\vec{v}])| > rb = \sum_{(t\sim 0)\in\psi} \mathsf{rootbound}(t).$$

[5] $t_j[\vec{x}/\vec{v}]$ 连续的原因是，$t_j[\vec{x}/\vec{v}]$ 中的所有指数表达式对于 $b_i \in \mathbb{R}_{\geq 0}$ 都具有 b_i^n 的形式，因为循环的所有特征值都是非负实数。

这与以下事实矛盾：根数上界（t）是由引理给出的 $t[\vec{x}/\vec{v}]$ 的实根数量上界 5。因此，由于我们将 m 实例化为 c，从而推出（AtBorders），我们证明了

$$\neg(\mathrm{QE}) \text{ and } (\mathrm{Const}_{n_0}) \text{ yield a contradiction by choosing } m = c$$

或者，等价地，

$$(\mathrm{Const}_{n_0}) \text{ implies } (\mathrm{QE}) \text{ by choosing } m = c. \qquad (\mathrm{Const}_{n_0} \Rightarrow \mathrm{QE})$$

例 8（量词消去，例 4 和 7 续）。对于（Val），接下来需要判定其有效性

$$\exists m \in \mathbb{N}.\ \forall x, y \in \mathbb{R}.\ \bigvee_{j=0}^{6} \neg\left(0 \leq x + j \cdot m + 2^{j \cdot m} y \leq 10\right). \qquad (\mathrm{Val}^{\vee})$$

在我们的例子中，有 $n_0 = 0$ 且 $rb = 6$。因此，如果（$\mathrm{Val}^{\vee}$）成立，那么循环的运行时间就有如下上界 $n_0 + rb \cdot m = 6 \cdot m$，此循环见例 1。

上述证明得出了以下推论，后文将会用到。

推论 9。考虑子公式

$$\forall \vec{x} \in \mathbb{R}^d.\ \bigvee_{j=0}^{rb} \neg\psi[n/n_0 + j \cdot m] \qquad (\mathrm{QE}^{in})$$

(QE)，其唯一的自由变量 m 的取值范围为 $\mathbb{N}$。那么 (QE^{in}) 要么不可满足，要么对 m 的无穷多个不同取值都成立。

证明。首先假设 $\mathsf{rb} = 0$。那么 (QE^{in}) 不依赖于 m，因此它要么不可满足，要么对 m 的所有可能取值都成立。

现在令 $\mathsf{rb} > 0$，并假设 (QE^{in}) 仅对 m 的有限多个取值成立。令 $v \in \mathbb{N}$ 为满足以下条件的最大数：将 m 取为 v 时，(QE^{in}) 成立。于是，由 ($\mathrm{QE} \Rightarrow \mathrm{Const}_{n_0}$) 可知，将 c 取为 $rb \cdot v + 1$ 时，($\mathrm{Const}_{n_0}^{in}$) 成立。接着，由 ($\mathrm{Const}_{n_0} \Rightarrow \mathrm{QE}$) 可知，将 m 取为 $rb \cdot v + 1$ 时，(QE^{in}) 成立。由于 $\mathsf{rb} > 0$，我们有 $\mathsf{rb} \cdot v + 1 > v$，也就是说，($\mathrm{QE}^{in}$) 对一个大于 v 的数也成立，这与我们关于 v 最大性的假设矛盾。□

3.5 最终符号

与公式（Const_{n_0}）相比，在（QE）中，我们消去了最内层量词，并将其替换为 rb 个 $+1$ 子公式，其中 rb 是固定的。所得公式（QE）关于程序变量 $\vec{x}$ 是线性的，关于 m是多项式指数的。

接下来，我们想通过一种傅里叶-莫茨金消元的变体来消去 $\vec{x}$。为了说明即使存在以下情况也能应用傅里叶-莫茨金消元：

中的非线性项 m，我们暂且忽略 (QE) 的最外层量词，也就是说，假设已知 $m \in \mathbb{N}$。那么，证明 (QE) 就相当于证明一个不等式析取式的有效性。相比之下，傅里叶-莫茨金消元用于检验可满足性，对象是合取式。因此，要证明 (QE) 有效，我们的目标是使用傅里叶 - 莫茨金消元证明以下公式不可满足

$$\pi := \bigwedge_{j=0}^{rb} \psi[n/n_0 + j \cdot m],$$

它由对 (QE) 取否定得到。

然而，傅里叶-莫茨金消元法仅适用于线性不等式。为了将其应用于我们的情形，我们将 π 中的（多项式指数）不等式视为关于 $\vec{x}$ 的线性不等式，其系数是关于 m 的单变量多项式指数表达式，即系数具有以下形式

$$0 \qquad \text{or} \qquad \sum_{i=1}^{M} d_i \cdot b_i^m \cdot m^{e_i} \tag{Coeff}$$

其中 m 是唯一变量，$M \geq 1$、$d_i \in \mathbb{R}_{\mathbb{A}} \setminus \{0\}$、$b_i \in \mathbb{R}_{\mathbb{A}>0}$ 和 $e_i \in \mathbb{N}$。再次注意，d_i 和 b_i 是代数数，因此适用于算法处理。要应用傅里叶-莫茨金消元，必须知道这些系数的符号，但一般情况下并非如此。

然而，我们可以轻松识别表达式 (Coeff) 中渐近占优的加项，它决定了该表达式的符号，只要 m 足够大即可。此外，根据推论 9，不失一般性，我们可以假设 m 足够大：如果 (QE) 对某个较小的 m 值成立，那么也存在任意大的 m 值，使得 (QE) 成立。

更正式地说，为确定充分大的 m 所对应的符号，不妨假设对于 (Coeff) 中的每个加项，(b_i, e_i) 都是唯一的。于是，只需考虑渐近占优加项 $d_j \cdot b_j^m \cdot m^{e_j}$，其中对于所有 $1 \leq i \leq M$，$(b_j, e_j) \geq_{lex} (b_i, e_i)$，即 (b_j, e_j) 关于字典序是最大的。由于所有特征值 b_i 都是非负实数，当 m 充分大时，系数 (Coeff) 的符号等于 d_j 的符号，或者该系数恒为 0。更准确地说，对于任意数 v，令：

$$\mathsf{sign}(v) = -1 \text{ if } v < 0 \qquad \mathsf{sign}(0) = 0 \qquad \mathsf{sign}(v) = 1 \text{ if } v > 0$$

注意，由于我们要求 $d_i \neq 0$，并要求对于每个加项，(b_i, e_i) 是唯一的，因此，当用足够大的数实例化 m 时，只要 (Coeff) 具有 $\sum_{i=1}^{M} d_i \cdot b_i^m \cdot m^{e_i}$ 的形式，就有 $\mathsf{sign}(\text{Coeff}) \neq 0$。在这种情况下，我们有

$$\exists m_0 \in \mathbb{N}.\ \forall m \geq m_0.\ \mathsf{sign}(\text{Coeff}) = \mathsf{sign}(d_j).$$

我们将 (Coeff) 的最终符号定义为 $\mathsf{esign}(\text{Coeff}) := 0$，当 (Coeff) 为 0 时；否则定义为 $\mathsf{esign}(\text{Coeff}) := \mathsf{sign}(d_j)$。

例 10（最终符号，例 8 续）。重新考察 (VAL$^\vee$)。这里，变量 x 的系数为 1 和 -1，显然 esign(1) $= 1$，且 esign$(-1) = -1$。变量 y 的系数为 $2^{j\cdot m}$ 和 $-2^{j\cdot m}$，对应于 $0 \leq j \leq 6$，其中 esign$(2^{j\cdot m}) = 1$，且 esign$(-2^{j\cdot m}) = -1$。再看一个更复杂的例子，考虑 $(3^m \cdot m^2 - 10 \cdot 2^m \cdot m^3) \cdot x$。由于 (3, 2) $\geq_{lex}$ (2, 3)，我们有 esign$(3^m \cdot m^2 - 10 \cdot 2^m \cdot m^3) = 1$，也就是说，$x$ 的渐近占优系数最终变为正数。

3.6 变量消去

现在我们说明如何从 π 中的变量向量 $\vec{x}$ 里消去单个变量 x。于是立即可知，可以消去 $\vec{x}$ 中的所有变量，从而只剩下变量 m。回想一下，π 定义为

$$\pi := \bigwedge_{j=0}^{rb} \psi[n/n_0 + j \cdot m].$$

因此，特别地，π 是一组不等式的合取。要消去 x，考虑以下集合：

$$\check{\pi}_x := \{p \cdot x + t \sim 0 \text{ occurs in } \pi \mid \sim \in \{>, \geq\}, \mathsf{esign}(p) > 0\}$$
$$\hat{\pi}_x := \{p \cdot x + t \sim 0 \text{ occurs in } \pi \mid \sim \in \{>, \geq\}, \mathsf{esign}(p) < 0\}$$

其中，p 是将 $p \cdot x + t$ 视为关于 $\vec{x}$ 的线性多项式时，x 的系数，其系数的形式为（COEFF）。换句话说，选择 p，使得 t 不含有 x。因此，$\check{}\pi_x$ 包含 π 中那些在 m 足够大时为 x 提供下界的不等式，而 $\hat{}\pi_x$ 则包含那些提供上界的不等式。接下来，我们将 π_x 定义为满足以下条件的最小集合：

$$\begin{array}{rl} \text{If} & p_1 \cdot x + t_1 \sim_1 0 \in \check{\pi}_x \quad \text{and} \quad p_2 \cdot x + t_2 \sim_2 0 \in \hat{\pi}_x, \\ \text{then} & p_1 \cdot t_2 - p_2 \cdot t_1 \sim 0 \in \pi_x, \end{array}$$

其中，若 $\sim_1$ 和 $\sim_2$ 均为 $\geq$，则 $\sim$ 为 $\geq$；否则，$\sim$ 为 $>$。于是

$$\pi \equiv \pi' \text{ for all large enough values of } m,$$

其中 $\pi' := (\pi \cup \pi_x) \setminus (\check{}\pi_x \cup \hat{}\pi_x)$，根据构造，$x$ 不会出现在 π' 中。

例 11（傅里叶-莫茨金消元，例 *8* 和 *10* 续）。对于公式（VAL$^\vee$），我们得到以下不等式：

$$0 \leq \overbrace{1}^{p} \cdot x + \overbrace{j \cdot m + 2^{j\cdot m} y}^{t} \qquad (\text{for all } 0 \leq j \leq 6)$$
$$x + j \cdot m + 2^{j\cdot m} y \leq 10 \qquad (\text{for all } 0 \leq j \leq 6)$$

因此，我们有：

$$\check{\pi}_x = \{x + j \cdot m + 2^{j\cdot m} y \geq 0 \mid 0 \leq j \leq 6\}$$
$$\hat{\pi}_x = \{-x - j \cdot m - 2^{j\cdot m} y + 10 \geq 0 \mid 0 \leq j \leq 6\}$$

因此，消去 x 后得到

$$\begin{aligned}\pi' &= \{j\cdot m + 2^{j\cdot m}y \geq j'\cdot m + 2^{j'\cdot m}y - 10 \mid j,j' \in \{0,\dots,6\}\}\\ &= \{(j-j')\cdot m + (2^{j\cdot m} - 2^{j'\cdot m})\cdot y + 10 \geq 0 \mid j,j' \in \{0,\dots,6\}\}\\ &= \{(j-j')\cdot m + ((2^j)^m - (2^{j'})^m)\cdot y + 10 \geq 0 \mid j,j' \in \{0,\dots,6\}\} \qquad (\star)\end{aligned}$$

接下来，我们从 π'中消去 y，得到：

$$\begin{aligned}\check{\pi}'_y &\supseteq \{(4^m-1)\cdot y + 2m + 10 \geq 0\} && ((\star) \text{ with } j=2 \text{ and } j'=0)\\ \hat{\pi}'_y &\supseteq \{(1-2^m)\cdot y - m + 10 \geq 0\} && ((\star) \text{ with } j=0 \text{ and } j'=1)\end{aligned}$$

因此，得到的公式 π'' 包含合取项

$$\begin{aligned}&(4^m-1)\cdot(10-m) - (1-2^m)\cdot(2m+10) \geq 0\\ \equiv\ &-4^m\cdot m + 10\cdot 4^m + 2^m\cdot 2m + 10\cdot 2^m - m - 20 \geq 0. \qquad (\lightning)\end{aligned}$$

变量消去的正确性：为说明这一构造为何正确，我们证明

$$\pi \equiv \pi' \text{ for all large enough values of } m,$$

其中 $\pi' := (\pi \cup \pi_x) \setminus (\check{\pi}_x \cup \hat{\pi}_x)$。更准确地说，我们证明，对于每个满足 $\mathsf{sign}(p[m/c]) = \mathsf{esign}(p)$（对所有 π 中的系数 p 均成立）的 $c \in \mathbb{N}$，$\pi[m/c]$ 等价于 $\pi'[m/c]$。

因此，如果 $m_0 \in \mathbb{N}$，使得对于所有 $m \geq m_0$，我们都有 $\mathsf{sign}(p) = \mathsf{esign}(p)$，那么对于所有 $m \geq m_0$，π 也等价于 π'。因此，我们不必检查某个充分大的 m 值下 π 的不可满足性，而可以改为检查某个充分大的 m 值下 π' 的不可满足性。

$\pi[m/c]$ 与 $\pi'[m/c]$ 的等价性：为证明当对所有 π 中的系数 p，均有 $\mathsf{sign}(p[m/c]) = \mathsf{esign}(p)$ 时，$\pi[m/c]$ 等价于 $\pi'[m/c]$，我们可以使用傅里叶–莫茨金消去法的思想，因为 $\pi[m/c]$ 是线性的：

如果所有不等式都是弱不等式（即由 $\geq$ 构成），那么这些不等式

$$p_1[m/c]\cdot x + t_1[m/c] \geq 0$$

在 $\check{\pi}_x[m/c]$ 中等价于 $x \geq \frac{-t_1[m/c]}{p_1[m/c]}$（因为根据 $\check{\pi}_x$ 的定义，$p_1[m/c] > 0$）。同理，这些不等式

$$p_2[m/c]\cdot x + t_2[m/c] \geq 0$$

在 $\hat{\pi}_x[m/c]$ 中等价于 $x \leq \frac{-t_2[m/c]}{p_2[m/c]}$（因为根据 $\hat{\pi}_x$ 的定义，$p_2[m/c] < 0$）。

因此，$\pi[m/c]$ 等价于 $(\pi \setminus (\check{\pi}_x \cup \hat{\pi}_x))[m/c]$ 与下列不等式的合取

$$\frac{-t_1[m/c]}{p_1[m/c]} \leq \frac{-t_2[m/c]}{p_2[m/c]} \qquad (\mathrm{FM})$$

对于所有来自 $\check{\pi}_x$ 的 $p_1\cdot x + t_1 \geq 0$，以及所有来自 $\hat{\pi}_x$ 的 $p_2\cdot x + t_2 \geq 0$。[6]

[6] 这对于 $\mathbb{Z}$ 这样的离散集合并不成立，这正是第 3.6 节的方法无法应用于在 $\mathbb{Z}$ 上的循环的原因。

注意，如果两个不等式 $p_1 \cdot x + t_1 \geq 0$ 或 $p_2 \cdot x + t_2 \geq 0$ 中至少有一个是严格不等式，那么（FM）也是严格不等式。由于 $p_1[m/c] > 0$ 且 $p_2[m/c] < 0$，我们得到

$$(\text{FM}) \quad \equiv \quad -p_2[m/c] \cdot t_1[m/c] \geq -p_1[m/c] \cdot t_2[m/c] \quad \equiv (p_1 \cdot t_2 - p_2 \cdot t_1 \geq 0)[m/c].$$

因此，$\pi[m/c]$ 等价于（$\pi \setminus (\check{}\pi_x \cup \hat{}\pi_x)$）$[m/c] \cup \pi_x[m/c] = \pi'[m/c]$。

3.7 判定有效性

消去所有变量后，我们得到一个由形如 $p > 0$ 或 $p \geq 0$ 的不等式构成的合取，其中 p 的形式为（Coeff）。当 m 的值足够大时，这样的合取不可满足，当且仅当存在一个不等式 $p > 0$ 或 $p \geq 0$，其中 $\mathsf{esign}(p) = -1$，或者存在一个不等式 $p > 0$，其中 $\mathsf{esign}(p) = 0$。因此，对于 $\mathsf{esign}(p) = 0$ 的情形，我们必须区分“>”和“≥”。

然而，以这种方式检查可满足性并不能直接得出 m 的一个实例，使得 π 不可满足。因此，我们无法直接获得运行时间的相应常数界 $n_0 + \mathsf{rb} \cdot m$。不过，如果已证明 π 不可满足，那么要计算所分析循环的运行时间常数界，只需不断展开循环，直到其守卫条件变得不可满足。

例 12（判定有效性，例 *11* 已完成）。对于公式 ($\lightning$)，我们有$\mathsf{esign}(\lightning) = -1$，因为 $-4^m \cdot m$ 是占主导地位的加项，因为：

$$\overbrace{(4,1)}^{-4^m \cdot m} >_{lex} \overbrace{(4,0)}^{10 \cdot 4^m} >_{lex} > \overbrace{(2,1)}^{2^m \cdot 2m} >_{lex} > \overbrace{(2,0)}^{10 \cdot 2^m} >_{lex} \overbrace{(1,1)}^{-m} >_{lex} \overbrace{(1,0)}^{-20}$$

因此，当 $\lightning$ 取足够大的值时，(m) 不可满足，故 (Val$^\vee$) 有效。事实上，对于所有 $\lightning$，($m \geq 11$ （但对于 $0 \leq m \leq 10$则不然）相互矛盾。因此，例 1 具有常数运行时间，我们得到常数界 $n_0 + rb \cdot m = 0 + 6 \cdot 11 = 66$，也就是说，每次运行至多进行 66 次迭代。

因此，在本节中，我们推导出了以下定理。

定理 13（$\mathbb{R}$上的常数运行时间）。具有实特征值的线性循环在 $\mathbb{R}$上的常数运行时间是可判定的。

此外，我们的方法无需调整也可应用于 $\mathbb{Q}$ 上的循环，如以下引理所示。

引理 14（$\mathbb{R} \iff$ 上的常数运行时间与 $\mathbb{Q}$上的常数运行时间）。一个具有实特征值的线性循环在 $\mathbb{R}$ 上的运行时间为常数，当且仅当它在 $\mathbb{Q}$上的运行时间为常数。

证明。实数域上的常数运行时间显然意味着有理数上的常数运行时间。反过来，假设有理数上的运行时间有常数 c 作为上界。那么 $\varphi^{(0..c)} := \varphi \wedge \mathsf{up}(\varphi) \wedge \cdots \wedge \mathsf{up}^c(\varphi)$ 在有理数上不可满足。注意，该公式只包含线性算术。由于包含线性算术的公式在实数上可满足，当且仅当其在有理数上可满足，因此 $\varphi^{(0..c)}$ 在实数域上也不可满足。因此，实数域上的运行时间也有常数 c 作为上界。□

因此，根据定理 13，以下推论显而易见。

推论 15（$\mathbb{Q}$上的常数运行时间）。具有实特征值的 $\mathbb{Q}$上线性循环的常数运行时间是可判定的。

4 $\mathbb{Z}$上的循环

现在我们考虑整数集上的循环，即（Loop）中的系数取自 $\mathbb{Z}$，并且变量的取值范围也属于 $\mathbb{Z}$。不难看出，第3 节中介绍的过程的所有部分都可以直接沿用到整数情形，只有一点例外：我们无法像第3.6节中那样使用傅里叶-莫茨金消元法消去变量。不过，我们可以利用“单参数 Presburger 算术” [6, 23]的可判定性。这种逻辑通过一个函数 $x \mapsto x \cdot m$扩展了 Presburger 算术，其中 m 是自由变量。因此，所得公式关于 m是非线性多项式，但关于所有其他变量都是线性的。由此，我们可以将这种逻辑的可判定性应用于（QE），但不能直接应用于（Const）。

在我们的设定中，回顾一下，b_i 闭式中出现的指数函数的底数对应于循环的特征值。因此，如果我们将注意力限制在特征值 0 和 1 上，那么所有指数函数都会消失。此外，如果我们还允许特征值 -1，那么应用推论 2中的化简后，剩余的特征值再次只有 0 和 1。因此，我们得到以下推论。

推论 16（在 $\mathbb{Z}$ 上的常数运行时间）。具有来自 $\{-1, 0, 1\}$ 的特征值的 $\mathbb{Z}$ 上的线性循环的常数运行时间是可判定的。

5 相关工作

关于完整技术的相关工作，在 $\mathbb{R}$、 $\mathbb{Q}$和 $\mathbb{Z}$ 上，关于线性单路径循环终止性的可判定性分别由 [28], [7], 和 [17], 证明。此外， [30] 和 [15] 分别给出了关于可解循环和三角弱非线性（twn）循环终止性的可判定性结果。与本文所考虑的循环不同，这类循环允许受限形式的非线性。在 [15], 的基础上，一种解决（非全称）停机问题（即判定一个固定输入的终止性）并推导 twn 循环的多项式运行时间上界的技术在 [14]中被提出。由 [14,15]提出的用于 twn 循环终止性分析和上界推导的完整技术已在工具KoAT [20, 21]中实现。

我们的工作通过给出常数运行时间的判定过程，对这些结果作了补充。与 [21, 引理 22], 类似，我们的方法可以扩展到实数的根（在整数情形下则为 $\{-1, 0, 1\}$ 的根）作为特征值的情况，即特征值 λ 其中 $\lambda^n \in \mathbb{R}$ （或 $\lambda^n \in \{-1, 0, 1\}$），对某个 $n \in \mathbb{N}$ 成立。未来，将我们的结果推广到具有任意特征值（包括不是实数根的复数）的更新矩阵，将会很有意思。不过，在这种情形下，我们的方法中的若干步骤必须修改。例如，涉及复数的多项式指数表达式的根的数量无法像第

3.3 节那样被常数所界定，且第 3.4 节中的量词消去无法再奏效，因而也就不能继续应用傅里叶-莫茨金消元。同样，将我们的结果推广到 $\mathbb{Z}$ 也会很有意思。

请注意，上述技术依赖于这样一个事实：可以轻易确定诸如（PE）这类闭式表达式中渐近占主导地位的加项。在第3.5节中，我们采用了类似的推理，但在那里，我们并不关心（PE）的渐近行为，而是关注某个不等式是否最终会对给定变量 x给出下界或上界。因此，我们只关心将（ x）视为具有多项式指数系数的线性多项式时，其系数中占主导地位的加项。因此，我们的方法PE与以往用于判定终止性的技术有根本区别。尤其是，与以往的方法不同（正如第1节中提到的），我们无法利用具有实特征值的线性循环的“最终单调性”，因为忽略循环守卫时，“非单调”步骤的初始数量通常不受常数限制，即使循环的运行时间是常数。为说明这一点，请看下面这个运行时间为常数的循环：

$$\textbf{while} \quad 0 \le x \le 10 \quad \textbf{do} \quad \begin{pmatrix} x \\ y \end{pmatrix} \leftarrow \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix} + \begin{pmatrix} 0 \\ 1 \end{pmatrix} \quad \textbf{end}$$

此处， x 一旦 y 变为非负值，就会单调变化（因为 $y \ge 0$蕴含 $x \le \mathrm{up}(x)$）。然而，满足 $\mathrm{up}^k(y) \ge 0$ 的数值 k 没有上界，因为它取决于 y的初始值。

文献 [14] 中用于计算 twn-循环多项式运行时间上界的完整技术，可以为任意终止的 twn-循环计算多项式上界。然而，这些上界不一定是紧的，也就是说，即使循环的运行时间为常数，所得上界也可能不是常数。因此，我们的工作与 [14]正交。

有多种用于程序自动复杂度分析的技术和工具（可处理任意多重循环、if-then-else、非确定性等），其中变量的取值范围为 $\mathbb{Z}$。这些工具中的大多数，例如 CoFloCo [9], KoAT [20],Loopus [27], MaxCore [2], 和 RAML [16], ，都会推断最坏情况运行时间复杂度的上界。因此，如果此类工具计算出常数运行时间上界，那么可以保证程序在常数步数内终止。相比之下，也有一些工具，例如 LOBER [3] 或 LoAT [12], ，分别推断循环或程序的最坏情况运行时间复杂度下界。因此，这类工具可以证伪常数运行时间。

6 评估与结论

评估：为了评估我们的判定过程在实际中的适用性，我们使用3 节中的Python 实现了该方法，并使用SymPy [24] 完成所有涉及代数数的计算。我们尚未实现第 $\mathbb{Z}$ 4 节中针对的循环的适配，因为我们尚不了解任何单参数 Presburger 算术判定过程的实现。在评估中，我们使用了以下基准测试集：其中包含 1495 个线性单路径循环

来自类别整数迁移系统终止性的终止问题数据库 [29], 中年度终止性与复杂度竞赛（TermComp） [13]所用的基准测试套件。去除重复项后，我们得到 1336 个循环。这些循环的特征值全为实数，表明我们的方法确实适用于一大类示例。其中 1327 个循环的特征值来自 $\{-1, 0, 1\}$，这表明，即使是我们针对 $\mathbb{Z}$ 循环提出的看似限制严格的结果（见第4节），从实践角度来看也很有意义。

在实验中，我们将工具 Loopy 的性能与所有参加了今年 TermComp 的整数转换系统复杂度分析工具进行了比较，即 CoFloCo、KoAT 和 LoAT。请注意，这三种工具考虑的是来自 $\mathbb{Z}$ 的初始值，而非来自 $\mathbb{R}$ 或 $\mathbb{Q}$的初始值。因此，如果 LoAT 推断某个循环在整数集上的下界不是常数，那么该循环在有理数域和实数域上的运行时间也不是常数；反过来，只要 Loopy 证明某个循环在有理数域和实数域上有常数界，那么该循环在整数集上也有常数上界。据我们所知，没有其他工具能够分析 $\mathbb{R}$ 或 $\mathbb{Q}$上的程序的复杂度。Loopy 证明了 76 个循环的运行时间为常数，并判定其余 1260 个循环的运行时间不是常数；在配备八核中央处理器 AMD Ryzen 7 3700X 的设备上，平均分析时间为 1.71 秒。这表明，我们的判定过程不仅在理论上具有意义，而且在标准基准测试集上也很高效，显示出其在实践中的适用性。CoFloCo 和 KoAT 分别能够证明这 76 个循环中的 5 个和 6 个具有常数运行时间，而 LoAT 则证明了 $\mathbb{Z}$上 1226 个循环的运行时间不是常数。LoAT 判定为非恒定运行时间的所有示例也都被 Loopy 判定为非恒定运行时间，即两者的结果没有冲突。请注意，CoFloCo 和 KoAT 并未实现用于证明常数界的专门技术，因此它们未能推断出更多常数运行时间界并不令人意外。因此，我们的实验表明，上界分析工具可以借助我们的判定过程，提高对此类循环的精确度。如需下载 Loopy 并查看评估的详细结果，请参见 [22]。

结论：我们提出了首个用于线性循环常数运行时间问题的完整方法。对于 $\mathbb{R}$ 和 $\mathbb{Q}$上的循环，当更新矩阵的特征值为实数时，我们的判定过程适用。对于 $\mathbb{Z}$上的循环，该过程适用于来自 $\{-1, 0, 1\}$的特征值。实证评估表明，我们的方法切实可行。在未来的工作中，我们将尝试为具有实特征值的循环加入对初始条件的支持，从而为长期悬而未决的问题提供部分解答：线性循环 [5]的多阶段线性秩函数是否存在是可判定的。值得注意的是，虽然固定初始值下线性循环的终止性对应于正性问题（该问题数十年来一直悬而未决），但实特征值下的正性问题是可判定的[1]。此外，我们将尝试把方法扩展到任意复特征值（不考虑初始条件）。

数据可用性声明

包含我们在工具 Loopy 中实现的制品可通过以下地址获取 [22]:

https://doi.org/10.5281/zenodo.17313899

此制品可用于复现我们评估中的所有结果。

参考文献

1. Akshay, S., Balaji, N., Vyas, N.: Skolem 问题及相关问题的受限变体的复杂度。载于: MFCS '17 论文集。LIPIcs 83（2017）。https://doi.org/ 10 4230 2017 78 . /LIPICS.MFCS. . . Albert, E., Bofill, M., 2 Borralleras, C., Martın-Mart´ın, E., Rubio, A.: 由（条件）终止性证明驱动的资源分析。 Theory and Practice of Logic Pro- gramming **19** 5 6 722 739 2019 10 1017 1471068419000152 (-), – ( )。 3 https://doi.org/ . /S . Albert, E., Genaim, S., Martın-Martın, E., Merayo, A., Rubio, A.: 利用循环特化和 Max-SMT 进行下界综合。载于: CAV '21 论文集。第 863–886 页。LNCS 12760 9 40 4 2021 10 1007 978 3 030 81688 ( )。https://doi.org/ . / - - - - . Ben-Amram, A.M., Genaim, S.: 关于多阶段线性排序函数。载于: CAV '17 论文集。第 601–620 页。LNCS 10427（2017）。 https://doi.org/ 10 1007 978 3 319 63390 9_32 . / - - - - . Ben-Amram, A.M., 5 Domenech, J.J., Genaim, S.: 多阶段线性排序函数及其与递归集的关系。载于: SAS '19 论文集。第 459–480 页。LNCS 11822 2 22 6 2019 10 1007 978 3 030 32304 -)。https://doi.org/ . / - - - - . Bogart, T., Goodrick, J., Woods, K.: 参数化 Presburger 算术: 逻辑、组合学与拟多项式行为。 Discrete Analysis（2017）。https://doi.org/10 1254 7 19086. /da. . Braverman, M.: 整数线性程序的终止性。载于: CAV '06 论文集。第 372 11817963 34 8 385 4144 2006 10 1007 – 页。 LNCS（）。https://doi.org/ . / . Cai, J.Y.: 在多项式时间内精确计算可交换矩阵的 Jordan 标准形。 International Journal of Foundations of Computer Science 5(3/4), 293 0129054194000165 9 302 1994 10 1142 – （）。https://doi.org/ . /S . Flores-Montoya, A.: 以成本关系表示的程序的摊销成本上界和下界。载于: FM '16 论文集。第 254–273 页。LNCS 9995（2016）。 https://doi.org/10 6 16 10 1007 978 3 319 48989 . / - - - - . Frohn, F., Giesl, J.: 三角整数循环的终止性可判定。载于: CAV '19 论文集。第 426–444 页。LNCS 11562（2019）。 https://doi.org/10 5 24 11 1007 978 3 030 25543 . / - - - - . Frohn, F.: 模块化循环加速的演算。 载于: TACAS '20 论文集。第 58 5 4 12 76 12078 2020 10 1007 978 3 030 45190 – 页。LNCS （）。https://doi.org/ . / - - - - . Frohn, F., Giesl, J.: 使用 LoAT 证明非终止性和运行时间下界 （系统描述）。载于: IJCAR '22 论文集。第 712–722 页。LNCS 13385（2022）。 https://doi.org/10 6 41 13 1007 978 3 031 10769 . / - - - - . Giesl, J., Rubio, A., Sternagel, C., Waldmann, J., Yamada, A.: 终止性与复杂度竞赛。载于: TACAS '19 论文集。第 156–166 页。 LNCS 11429 2019 10 1007 978 3 030 17502 3_10, *Term-Comp* ( )。 https://doi.org/ . / - - - - 网站: https://termination-portal.org/wiki/Termination Competition 14. Hark, M., Frohn, F., Giesl, J.: 多项式循环: 超越终止性。载于: LPAR '20 论 文集。第 279–297 页。EPiC 73（2020）。https://doi.org/10.29007/NXV1

15. Hark, M., Frohn, F., Giesl, J.：三角多项式循环的终止性。Formal Methods in System Design 65(1), 70–132（2025）。https://doi.org/10.1007/s10703-023-00440-z 16. Hoffmann, J., Das, A., Weng, S.：迈向 OCaml 的自动资源界分析。载于：POPL '17 论文集。第 359–373 页（2017）。https://doi.org/10 3009842 17 1145 3009837 . / . . Hosseini, M., Ouaknine, J., Worrell, J.：整数上线性循环的终止性。载于：ICALP '19 论文集。LIPIcs 132（2019）。https://doi.org/10 118 18 4230 2019 . /LIPIcs.ICALP. . . Kincaid, Z., Breck, J., Cyphert, J., Reps, T.：数值循环的闭式。Proceedings of the ACM on Programming Languages 3(POPL)（2019）。https://doi.org/ 10 1145 3290368 . / . 19 Kovacs, L.：针对 P-可解循环的完备不变量生成方法。载于：PSI '09 论文集。第 242–256 页。LNCS 5947（2010）。https://doi.org/10 1 21 20 1007 978 3 642 11486 . / - - - - . Lo mmen, N., Meyer, F., Giesl, J.：通过三角弱非线性循环对整数程序进行自动复杂度分析。载于：IJCAR '22 论文集。第 734–754 页。LNCS 13385 6 43 21 2022 10 1007 978 3 031 10769 ( )。https://doi.org/ . / - - - - . Lommen, N., Giesl, J.：以完备性为目标：使用闭式分析整数程序的规模界。载于：FroCoS '23 论文集。第 3–22 页。LNCS 14279（2023）。https://doi.org/10 6 1 22 1007 978 3 031 43369 . / - - - - . Loopy：工件、评估与基准测试。Zenodo（2025）。https://doi.org/10 17313899 23 5281. /zenodo. . Mansutti, A., Starchak, M.R.：单参数 Presburger 算术具有量词消去性质。载于：MFCS '25 论文集。LIPIcs 345（2025）。https://doi.org/ 10 4230 - 2025 72 . /LIPICS.MFCS. . . 24 Meurer, A., Smith, C.P., Paprocki, M., ˇCertık, O., Kirpichev, S.B., Rocklin, M., Kumar, A., Ivanov, S., Moore, J.K., Singh, S., Rathnayake, T., Vig, S., Granger, B.E., Muller, R.P., Bonazzi, F., Gupta, H., Vats, S., Johansson, F., Pedregosa, F., Curry, M.J., Terrel, A.R., Rou ˇcka, ˇS., Saboo, A., Fernando, I., Kulal, S., Cimrman, R., Scopatz, A.：SymPy：Python 符号计算。PeerJ计算机科学 3, 103 25 103 2017 10 7717 e ( )。https://doi.org/ . / peerj-cs. . Ouaknine, J., Pinto, J.S., Worrell, J.：关于整数线性循环的终止性。载于：SODA ' 15 957 969 2015 10 1137 1 9781611973730 65 论文 26 集。第 – 页（）。https://doi.org/ . / . . . Polya, G., Szego, G.：分析中的问题与定理II：函数论。零点。多项式。行列式。数论。几何学。数学经典，Springer（1976 2 27 10 1007 978 3 642 61905）。https://doi.org/ . / - - - - . Sinn, M., Zuleger, F., Veith, H.：使用差分约束分析命令式程序的复杂度与资源界。自动推理杂志 59 4 28 1 3 45 2017 10 1007 10817 016 9402 04（），–（）。https://doi.org/ . /s - - - . Tiwari, A.：线性程序的终止性。载于：CAV ' 论文集。第 70–82 页。LNCS 3114 9 6 29 2004 10 1007 978 3 540 27813 ( )。https://doi.org/ . / - - - - . TPDB（终止问题数据库），https://github.com/TermCOMP/TPDB 30. Xu, M., Li, Z.B.：可解循环的符号终止性分析。Journal of Sym- bolic Computation 50, 28–49（2013）。https://doi.org/10.1016/j.jsc.2012.05.005