Decidability of Collision between a Helical Motion and an Algebraic Motion

Sung Woo Choi[1] Sung-il Pae[2] Hyungju Park[2] Chee K. Yap[3]

[1]Duksung Women's University
Seoul, Korea

[2]Korea Institute for Advanced Study
Seoul, Korea

[3]Courant Institute, New York University
New York, NY USA

Abstract

We show in this paper that collision between two moving balls in $3D$ is decidable if one of the bodies has a helical motion and the other body has an algebraic motion. Furthermore, an explicit polynomial time complexity bound is derived for this problem. Such bounds depend on effective versions of Baker's theorem on linear form in logarithms in transcendental number theory.

1 Introduction

Many geometric problems are solved using the Real RAM model. As long as the solutions remain algebraic, the use of a Real RAM model is feasible. But when transcendental operations such as $\sin x$ and $\exp x$ are involved, it is a major open problem in Exact Geometric Computation [10] whether the Real RAM model can be simulated by a Turing machine. Recently, the first example of a transcendental geometric problem that is provably solvable in the Turing machine model was shown in [2]: this is the problem of computing shortest paths amidst disc obstacles.

In this paper, we study a collision detection problem that is also transcendental in nature. It is well-known that algebraic motion planning is solvable since the early 1980s [6]. Here, obstacles are typically static, and some feasible motion between two positions is to be computed. Superficially, such motions may involve the trigonometric functions such as $\sin x$ and $\cos x$; but they can be resolved by introducing algebraic relations such as $\sin^2 x + \cos^2 x = 1$.

But truly transcendental motion planning problems can arise through the introduction of helical motions. In modeling, computer graphics and robotics, the use of helical motions or geometry is relatively common (e.g., [7, Section 3.1.3], [3, 5]). The simplest helical motion is that of a point p that is moving along a fixed direction u at constant velocity while simultaneously rotating about a fixed axis that is along direction u. Let us suppose that simultaneously, a body $\mathcal{B}$ is moving in some known motion. We want to decide if p and $\mathcal{B}$ will collide. In this paper, we will give decision procedures for answering such questions. Our procedures will be shown to be implementable on Turing machines, not just Real RAMs. As in [2], such results will depend on zero bounds from transcendental number theory.

The possibility of computing such potential collision may seem to be of purely theoretical interest. Nevertheless, there may be a practical need for very high accuracy computations of this sort. On July 4th 2005, in the dramatic display of precision engineering and calculations, NASA successfully sent a man-made projectile into collision course with the comet Tempel 1, traveling with a relative speed of 23,000 mph. More generally, we want to predict if two celestial bodies will ever collide – this may involve computing very far into the future, with guaranteed accuracy. Presumably such questions will arise in the future.

Instead of asking if two bodies will collide, we can also ask if two bodies will come within distance $\varepsilon \geq 0$ of each other. This near-collision problem is a slight generalization of the collision question. For algebraic bodies, their decidability is equivalent. As we shall see, our ability to answer such questions is fairly limited.

Contributions of this paper. Helical motions are one of the simplest forms of non-algebraic motion that are used in applications. This paper shows that a collision problem involving such motion is computable. This adds to our currently sparse collection of transcendental geometric problems known to be computable. The boundary between what is and what is not computable "exactly" in the geometric sense is a fundamental issue in the theory of real computation, and of complexity theory. This area also has practical implications for robust geometric computations.

Overview of Paper. In Section 2, we introduce a simple version of the collision problem involving helical motion. This problem is shown to be decidable. In Section 3, we derive a polynomial time complexity bound assuming the input motions are defined by rational polynomials. In Section 4, we discuss open problems and possible extensions.

2 A Simple Case

Let p be a point in a helical motion and let $h(t) = (\cos t, \sin t, st)$ be the position of p at time t. Suppose that $\mathcal{B}$ is a ball with radius r that moves along a curve and let $c(t) = (c_1(t), c_2(t), c_3(t))$ be the position of $\mathcal{B}$'s center at time t.

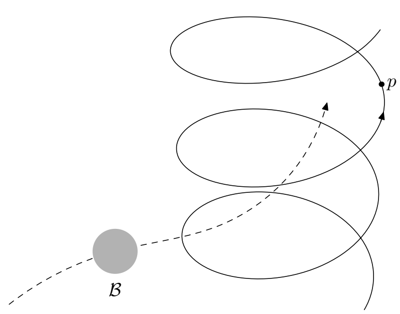

Figure 1: Collision detection of a point p in helical motion and a moving ball $\mathcal{B}$.

Assuming that p and $\mathcal{B}$ are not in collision at the initial time $t = 0$, we want to decide whether p and $\mathcal{B}$ will ever collide at a time $t > 0$. Assume that $c_i(t)$'s are algebraic functions, *i.e.*, there exists a polynomial $P(x, y) \in \mathbb{C}[x, y]$ such that $P(c_i(t), t) \equiv 0$. We shall focus on an interval $I = [T_1, T_2]$ on which $c(t)$ is continuous and differentiable (except at the boundaries), where T_1 and T_2 are algebraic numbers. The most important class of functions in practice for $c_i(t)$'s would be polynomials with rational coefficients, and we will focus on this case in Section 3. Another interesting class is piecewise continuous rational functions, and the assumption on $[T_1, T_2]$ is natural in this situation. In this section, we assume that $c_i(t)$'s are general algebraic functions, and the radius r of $\mathcal{B}$ and the speed parameter s of $h(t)$ are real algebraic numbers. We show that the corresponding collision detection is decidable.

There is a collision if and only if the inequality

$$\|h(t) - c(t)\| \leq r \tag{1}$$

has a real solution in $t \in I$. The inequality (1) is equivalent to

$$\|h(t) - c(t)\|^2 = (\cos t - c_1(t))^2 + (\sin t - c_2(t))^2 + (st - c_3(t))^2 \leq r^2.$$

By continuity, this is equivalent to checking if there is a solution for the equation $\|h(t) - c(t)\|^2 = r^2$ for some $t \in I$. This equation is now equivalent to checking the solvability of equation of the form

$$a(t)\cos t + b(t)\sin t + d(t) = 0, \tag{2}$$

where $a(t) = -2c_1(t)$, $b(t) = -2c_2(t)$, and $d(t) = c_1(t)^2 + c_2(t)^2 + (st - c_3(t))^2 + 1 - r^2$. Note that $a(t)$, $b(t)$, and $d(t)$ are differentiable on (T_1, T_2) and continuous on $[T_1, T_2]$.

Theorem 1. *It is decidable whether there is a real solution of the equation of type (2).*

Note that equation (2) includes transcendental functions. To prove the theorem, we transform the equation into a form to which we can apply the zero bound. (See Section 3.2.) Let $A_0 = \{t \in I \mid a(t)^2 + b(t)^2 > 0\}$, the set of t for which $a(t)$ and $b(t)$ are not simultaneously zero. For $t \in A_0$, let

$$\alpha(t) = \frac{a(t)}{\sqrt{a(t)^2 + b(t)^2}}, \quad \beta(t) = \frac{-b(t)}{\sqrt{a(t)^2 + b(t)^2}}, \quad \delta(t) = \frac{-d(t)}{\sqrt{a(t)^2 + b(t)^2}}.$$

Then, for each $t \in A_0$, there is $\theta(t)$ such that $\cos\theta(t) = \alpha(t)$ and $\sin\theta(t) = \beta(t)$, and equation (2) is reduced to

$$\cos(t + \theta(t)) = \delta(t). \tag{3}$$

Let us fix a branch of arc cosine, say $\arccos : [-1, 1] \to [0, \pi]$. Then $\theta(t) = \arccos\alpha(t)$ when $\beta(t) \geq 0$, and $\theta(t) = -\arccos\alpha(t)$ when $\beta(t) \leq 0$. Rewrite (3) as

$$\cos(t \pm \arccos\alpha(t)) = \delta(t), \tag{4}$$

subject to the sign of $\beta(t)$. Now let $A = \{\, t \in I \mid -1 \leq \delta(t) \leq 1,\ a(t)^2 + b(t)^2 > 0 \,\}$. By definition, we have $A \subseteq A_0$. Since $-1 \leq \delta(t) \leq 1$ on A, we can take arccos on both sides of (4) and obtain the following equations:

$$t + \arccos\alpha(t) - \arccos\delta(t) = 0 \mod 2\pi, \tag{5}$$
$$t + \arccos\alpha(t) + \arccos\delta(t) = 0 \mod 2\pi, \tag{6}$$
$$t - \arccos\alpha(t) - \arccos\delta(t) = 0 \mod 2\pi, \tag{7}$$
$$t - \arccos\alpha(t) + \arccos\delta(t) = 0 \mod 2\pi, \tag{8}$$

where equations (5) and (6) are subject to the condition $\beta(t) \geq 0$, and equations (7) and (8) are subject to the condition $\beta(t) \leq 0$. The following lemma justifies the reduction of equation (2) to equations (5)–(8).

Lemma 2. *For $t \in A$, equation (2) holds if and only if one of the equations (5)–(8) holds.*

Proof. Suppose that t_0 is in A and satisfies (2). There is a unique $\theta_0 \in [0, 2\pi)$ such that $\cos\theta_0 = \alpha(t_0)$, $\sin\theta_0 = \beta(t_0)$. This θ_0 clearly satisfies $\cos(t_0 + \theta_0) = \delta(t_0)$. Since $t_0 \in A$, we have $-1 \leq \delta(t_0) \leq 1$, and thus

$$\arccos\delta(t_0) = \arccos\cos(t_0 + \theta_0) = \pm(t_0 + \theta_0) \pmod{2\pi}, \tag{9}$$

depending on which quadrant $t_0 + \theta_0$ is contained in. Now, depending on the sign of $\beta(t_0)$, we have either $\theta_0 = \arccos\alpha(t_0)$ or $\theta_0 = 2\pi - \arccos\alpha(t_0)$. By eliminating θ_0 in (9) with this, we conclude that t_0 satisfies one of (5)–(8).

Conversely, if t_0 satisfies equations (5) or (6), then clearly we have $\cos(t_0 + \arccos\alpha(t_0)) = \delta(t_0)$. Note that if $\beta(t_0) \geq 0$, then $\sin\arccos\alpha(t_0) = \sin t_0$. By expanding cosine, we obtain (2) for t_0. For equations (7) or (8), we have $\cos(t_0 + \arccos\alpha(t_0)) = \delta(t_0)$. Because $\beta(t_0) \leq 0$ in this case, then $\sin\arccos\alpha(t_0) = -\sin t_0$. So we obtain (2) for t_0 by expanding cosine. □

Lemma 2 takes care of the case where t is in A. If $t \in I - A$, the only case that our argument does not capture is when $a(t) = b(t) = 0$. The following lemma is clearly true.

Lemma 3. *If $t \in I - A$, equation (2) holds if and only if $a(t) = b(t) = d(t) = 0$.*

Now we show how to decide the existence of a zero of equation (2). Given algebraic functions $a(t)$, $b(t)$ and $d(t)$, we first check if $a(t), b(t)$ and $d(t)$ have a simultaneous zero in $[T_1, T_2]$, and this is clearly a decidable problem. If they have a solution, we can stop and conclude that there is a collision. In this degenerate case, $a(t) = -2c_1(t) = 0$, and $b(t) = -2c_2(t) = 0$. So the ball's center is at the axis of the helix. And $d(t) = (st - c_3(t))^2 + 1 - r^2 = 0$ means that p is touching the ball's surface. This can happen only when $r \geq 1$.

Now suppose that there is no simultaneous zero of $a(t), b(t)$ and $d(t)$ in $[T_1, T_2]$. By Lemma 3, we only need to check whether there is a zero in A, and the rest of this section is devoted to this question. We first show that A is a union of a finite number of closed intervals with algebraic endpoints.

Lemma 4. *If there is no simultaneous zero of $a(t), b(t)$ and $d(t)$ in $[T_1, T_2]$, then A is a union of a finite number of closed intervals with algebraic endpoints.*

Proof. Since there is no simultaneous zero of $a(t), b(t)$ and $d(t)$, if $a(t)^2+b(t)^2 = 0$, then $d(t) \neq 0$. Because $d(t)$ does not vanish, by continuity of $a(t)$, $b(t)$ and $d(t)$, the condition $-1 \leq \delta(t) \leq 1$ implies that $a(t)^2+b(t)^2 > 0$; otherwise, $\delta(t) = -d(t)/\sqrt{a(t)^2 + b(t)^2}$ would not be bounded in the neighborhood of zeros of $a(t)^2 + b(t)^2$. Hence, we can remove the condition $a(t)^2 + b(t)^2 > 0$ in the definition of A, and the set A is determined by only the inequality $d(t)^2 \leq a(t)^2 + b(t)^2$. The function $f(t) = d(t)^2 - a(t)^2 - b(t)^2$ is continuous on $I = [T_1, T_2]$, which is a compact set. The set $A = \{\, t \in I \mid d(t)^2 - a(t)^2 - b(t)^2 \leq 0 \,\} = f^{-1}((-\infty, 0]) \cap [T_1, T_2]$ is an intersection of a closed set and a compact set in $\mathbb{R}$ and therefore is a compact set. So A is a union of a finite number of closed intervals. The endpoints of the intervals in A are the zeros of f, T_1 or T_2, which are algebraic. □

Now we focus on each connected interval of A and decide whether equations (5)–(8) have a zero using a zero bound for linear forms in arc cosines. Consider one connected interval $[t_1, t_2] \subset A$ and equation (5). Note, again, that t_1 and t_2 are zeros of $\delta(t) \pm 1$, T_1 or T_2. For $t \in [t_1, t_2]$,

$$t_1 - 2\pi \leq t + \arccos \alpha(t) - \arccos \delta(t) \leq t_2 + 2\pi.$$

Therefore, we need to check only a finite number of equations

$$t + \arccos \alpha(t) - \arccos \delta(t) - 2n\pi = 0,$$

for integers n. For a fixed integer k, define $F : [t_1, t_2] \to \mathbb{R}$ by

$$F(t) = t + \arccos \alpha(t) - \arccos \delta(t) - 2k\pi,$$

and we are to check the existence of a zero of F in $[t_1, t_2]$. Note that F is continuous on $[t_1, t_2]$, but may not be differentiable on $[t_1, t_2]$ since arccos is not differentiable at ± 1. Since $\delta(t) \neq \pm 1$ on (t_1, t_2), we find the t values in (t_1, t_2) where $\alpha(t) = \pm 1$, all of which are clearly algebraic, and the number of which is finite. Denote all such t values in (t_1, t_2) by $\tau_1, \tau_2, \ldots, \tau_l$. We also find all zeros of

$$F'(t) = 1 - \frac{\alpha'(t)}{\sqrt{1 - \alpha(t)^2}} + \frac{\delta'(t)}{\sqrt{1 - \delta(t)^2}} = 0$$

in (t_1, t_2), and denote them $\sigma_1, \sigma_2, \ldots, \sigma_m$. They are also algebraic and finite in number. Note that $\beta(t) = 0$ implies $b(t) = 0$, and hence $\alpha(t) = \pm 1$.

Now F and β have the following properties:

(1) F and β are continuous on $[t_1, t_2]$.

(2) F is strictly monotone on each subinterval generated by $\tau_1, \ldots, \tau_l$, $\sigma_1, \ldots, \sigma_m$, and the function β does not change sign on the subintervals.

So the decision problem on the existence of a zero of F in $[t_1, t_2]$ can be resolved by determining the signs of F at the extremal points $t_1, t_2, \tau_1, \ldots, \tau_l, \sigma_1, \ldots, \sigma_m$ and by checking (1) either one of them is a zero or endpoints of the subintervals have opposite signs, and (2) the sign of β at the zero or the signs of endpoints of the subinterval that contains a zero of F.

The sign determination of β on the algebraic points is clearly decidable, since β is algebraic. The sign determination for F can be done exactly as well, since we can determine the zero problem for the following expression with an algebraic t_* [2, 8]:

$$F(t_*) = t_* + \arccos \alpha(t_*) - \arccos \delta(t_*) - 2k \arccos(-1). \quad (10)$$

Clearly, similar procedures work for the other equations (6)–(8).

3 Complexity

In this section, we calculate an explicit bit complexity for our problem. Although the decidability result in Section 2 is valid for any *algebraic* input trajectory $c(t)$, we assume in this section that $c(t)$ is given by polynomials with rational coefficients.

Assumption: The functions $c_1(t)$, $c_2(t)$, $c_3(t)$, which define the trajectory of the moving ball $\mathcal{B}$'s center, are in $\mathbb{Q}[t]$. Also, the constant s and the ball's radius r are rational numbers.

See [1, 9] for more details on the notions introduced in this section.

3.1 Input Size

Let $f(t) = a_n t^n + a_{n-1} t^{n-1} + \cdots + a_0 \in \mathbb{C}[t]$ with $a_n \neq 0$. The *Mahler measure* of f, $M(f)$ is defined by

$$M(f) := |a_n| \cdot \prod_{i=1}^{n} \max\{1, |\gamma_i|\},$$

where $\gamma_1, \ldots, \gamma_n \in \mathbb{C}$ are the zeros of f. It follows from the definition that the Mahler measure is a multiplicative map from $\mathbb{C}[t]$ to $\{x \in \mathbb{R} \mid x > 0\}$, *i.e.*,

$$M(f_1 f_2) = M(f_1) M(f_2), \quad \forall f_1, f_2 \in \mathbb{C}[t]. \quad (11)$$

The *absolute logarithmic height* of f, $\mathrm{ht}(f)$, is defined by

$$\mathrm{ht}(f) := \frac{1}{\deg(f)} \log M(f).$$

Let γ be an algebraic number, and let $f \in \mathbb{Z}[t]$ be its minimal polynomial. The *degree* $\deg(\gamma)$, the *Mahler measure* $M(\gamma)$, and the *absolute logarithmic height* $\mathrm{ht}(\gamma)$ are defined respectively by:

$$\deg(\gamma) := \deg(f), \quad M(\gamma) := M(f), \quad \mathrm{ht}(\gamma) := \mathrm{ht}(f).$$

Here are some properties of the absolute logarithmic height:

Lemma 5. *Let $\gamma, \gamma_1, \ldots, \gamma_n$ be (nonzero) algebraic numbers. Then we have*

(1) $\mathrm{ht}(\gamma_1 \gamma_2) \leq \mathrm{ht}(\gamma_1) + \mathrm{ht}(\gamma_2)$.

(2) $\mathrm{ht}(\gamma_1 + \cdots + \gamma_n) \leq \mathrm{ht}(\gamma_1) + \cdots + \mathrm{ht}(\gamma_n) + \log n$.

(3) $\mathrm{ht}(\gamma^r) = |r| \cdot \mathrm{ht}(\gamma)$, $\forall r \in \mathbb{Q}$.

Proof. See [9]. □

We use the degrees of the input polynomials as a measure of the input size:

Input Condition 1: $\deg(c_1), \deg(c_2), \deg(c_3) \le N$.

For the second measure of input size, consider the following: Let

$$f(t) = \frac{p_n}{q_n} t^n + \frac{p_{n-1}}{q_{n-1}} t^{n-1} + \cdots + \frac{p_0}{q_0} \in \mathbb{Q}[t],$$

where $p_n, q_0, \ldots, q_n \ne 0$, and $(p_i, q_i) = 1$ for $i = 0, 1, \ldots, n$. We define the *bit bound* of f, $B(f)$, by

$$B(f) := \max_{0 \le i \le n} \{\log_2 |p_i|, \log_2 |q_i|\}.$$

Input Condition 2: $B(c_1), B(c_2), B(c_3) \le B$ and $B(s), B(r) \le B$.

The final bit complexity will be expressed in terms of these two input parameters N and B. Here are some properties of the bit bound:

Lemma 6. *For any $f(t), g(t) \in \mathbb{Q}[t]$, we have*

(1) $B(f \pm g) \le B(f) + B(g) + 1$.

(2) $B(fg) \le (N+1)\log_2(N+1) \cdot (B(f) + B(g))$, where $N = \min\{\deg(f), \deg(g)\}$.

(3) $B(f') \le B(f) \log_2(\deg(f))$.

(4) $M(f) \le \sqrt{1 + \deg(f)} \cdot 2^{B(f)}$.

Proof. See [9] for the proof of (4). Let $n = \deg(f)$, $m = \deg(g)$, $B_f = B(f)$, $B_g = B(g)$. Write

$$f(t) = \frac{p_n}{q_n} t^n + \frac{p_{n-1}}{q_{n-1}} t^{n-1} + \cdots + \frac{p_0}{q_0}, \quad g(t) = \frac{\tilde{p}_m}{\tilde{q}_m} t^n + \frac{\tilde{p}_{n-1}}{\tilde{q}_{n-1}} t^{n-1} + \cdots + \frac{\tilde{p}_0}{\tilde{q}_0},$$

where $|p_i|, |q_i| \le 2^{B_f}$, $|\tilde{p}_i|, |\tilde{q}_i| \le 2^{B_g}$. Note that a coefficient of $f(t) \pm g(t)$ is of the form:

$$\frac{p}{q} \pm \frac{\tilde{p}}{\tilde{q}} = \frac{p\tilde{q} \pm \tilde{p}q}{q\tilde{q}}.$$

So (1) follows, since $|p\tilde{q} \pm \tilde{p}q|, |q\tilde{q}| \le 2 \cdot 2^{B_f + B_g} = 2^{B_f + B_g + 1}$.

Let $N = \min\{n, m\}$. Note that a coefficient of $f(t)g(t)$ is of the form:

$$\sum_{k=0}^{L} \frac{p_{i_k}}{q_{i_k}} \cdot \frac{\tilde{p}_{j_k}}{\tilde{q}_{j_k}} = \frac{p_{i_0} q_{i_1} \cdots q_{i_L} \cdot \tilde{p}_{i_0} \tilde{q}_{i_1} \cdots \tilde{q}_{i_L} + q_{i_0} p_{i_1} q_{i_2} \cdots q_{i_L} \cdot \tilde{q}_{i_0} \tilde{p}_{i_1} \tilde{q}_{i_2} \cdots \tilde{q}_{i_L} + \cdots + q_{i_0} \cdots q_{i_{L-1}} p_{i_L} \cdot \tilde{q}_{i_0} \cdots \tilde{q}_{i_{L-1}} \tilde{p}_{i_L}}{\prod_{k=0}^{L} q_{i_k} \tilde{q}_{j_k}},$$

for some $L < N$. The bit size of the above number is less than $\log_2 \left\{(N+1) 2^{(N+1)B_f} 2^{(N+1)B_g}\right\}$, from which (2) follows.

Finally, note that the coefficients of $f'(t)$ are:

$$i \cdot \frac{p_i}{q_i}, \quad 0 \le i \le n.$$

So (3) follows, since $|i \cdot p_i|, |q_i| \le n \cdot 2^{B_f}$. □

3.2 Results From Transcendental Number Theory

The following Baker type result is an effective tool for the zero problem of transcendental expressions like (10):

Proposition 7 (Waldschmidt [8], Theorem C)**.** *For $n \geq 2$, let $\gamma_0, \gamma_1, \cdots, \gamma_n$ be algebraic numbers, and let $\beta_1, \cdots, \beta_n$ be nonzero algebraic numbers. For $1 \leq j \leq n$, let $\log \beta_j$ be any determination of the logarithm of β_j. Suppose that*

$$\begin{aligned} D &\geq [\mathbb{Q}(\gamma_0, \gamma_1, \cdots, \gamma_n, \beta_1, \cdots, \beta_n) : \mathbb{Q}], & W &\geq \max_{0 \leq j \leq n} \{\mathrm{ht}(\gamma_j)\}, \\ V_j &\geq \max\{\mathrm{ht}(\beta_j), |\log \beta_j|/D, 1/D\}, & V_1 &\leq \cdots \leq V_n, \\ V_{n-1}^+ &= \max\{V_{n-1}, 1\}, & V_n^+ &= \max\{V_n, 1\}. \\ 1 < E &\leq \min\{e^{DV_1}, \min_{1 \leq j \leq n}\{4DV_j/|\log \beta_j|\}\}. \end{aligned}$$

If $\Lambda := \gamma_0 + \gamma_1 \log \beta_1 + \cdots + \gamma_n \log \beta_n$ is non-zero, then

$$|\Lambda| > \exp\{-2^{8n+51} n^{2n} D^{n+2} V_1 \cdots V_n (W + \log(EDV_n^+))(\log(EDV_{n-1}^+))(\log E)^{-n-1}\}.$$

By applying Proposition 7 after replacing $\gamma_0 \to i\gamma_0$, $\beta_j \to \beta_j + i\sqrt{1-\beta_j^2}$, $1 \leq j \leq n$, we transform Proposition 7 into the following form, which is suitable to our situation:

Corollary 8. *Let $\gamma_0, \gamma_1, \ldots, \gamma_n, \beta_1, \ldots, \beta_n \in \mathbb{C}$ $(n \geq 2)$ be nonzero algebraic numbers. If $\Lambda := \gamma_0 + \gamma_1 \arccos \beta_1 + \cdots + \gamma_n \arccos \beta_n$ is non-zero, then*

$$|\Lambda| > \exp\{-2^{8n+51} n^{2n} D^{n+2} V_1 \cdots V_n (W + \log(EDV_n^+))(\log(EDV_{n-1}^+))(\log E)^{-n-1}\},$$

where

$$\begin{aligned} D &\geq 2^{n+1} \deg(\gamma_0) \cdots \deg(\gamma_n) \cdot \deg(\beta_1) \cdots \deg(\beta_n), & W &\geq \max_{0 \leq j \leq n} \{\mathrm{ht}(\gamma_j)\}, \\ V_j &\geq \max\{2\mathrm{ht}(\beta_j) + \frac{3}{2}\log 2, |\arccos \beta_j|/D, 1/D\}, & V_1 &\leq \cdots \leq V_n, \\ V_{n-1}^+ &= \max\{V_{n-1}, 1\}, & V_n^+ &= \max\{V_n, 1\}, \\ 1 < E &\leq \min\{e^{DV_1}, \min_{1 \leq j \leq n}\{4DV_j/|\arccos \beta_j|\}\}. \end{aligned}$$

3.3 Asymptotic Bit Complexity

Now we bound the bit complexity of the expression from (10)

$$\Lambda := F(t_*) = t_* + \arccos \alpha(t_*) - \arccos(\delta(t_*)) - 2k \arccos(-1), \tag{12}$$

where t_* is a zero of one of the following (algebraic) functions: (i) $\alpha(t) \pm 1$, (ii) $\delta(t) \pm 1$, (iii) $F'(t)$. The complexity argument for the other cases arising from (6), (7), (8) would be identical. To apply Corollary 8, we first need to bound the following quantities:

$$\deg(t_*), \quad \deg(\alpha(t_*)), \quad \deg(\delta(t_*)), \quad \mathrm{ht}(t_*), \quad \mathrm{ht}(\alpha(t_*)), \quad \mathrm{ht}(\delta(t_*)), \quad \mathrm{ht}(2k). \tag{13}$$

Lemma 9. *Let γ be a zero of $f[t] \in \mathbb{Q}[t]$. Then we have:*

(1) $\deg(\gamma) \leq \deg(f)$.

(2) $\mathrm{ht}(\gamma) \leq (\deg(f) + 2)B(f) \log 2 + \frac{1}{2} \log(\deg(f) + 1)$.

Proof. (1) is obvious. For the proof of (2), let $f_\gamma(t) \in \mathbb{Z}[t]$ be the minimal polynomial of γ. Let $n = \deg(f)$ and $B = B(f)$. Write

$$f(t) = \frac{p_n}{q_n}t^n + \frac{p_{n-1}}{q_{n-1}}t^{n-1} + \cdots + \frac{p_0}{q_0},$$

where $p_n, q_0, \ldots, q_n \neq 0$, and $\max_{i=0}^n \{|p_i|, |q_i|\} \leq 2^B$. Note that

$$\begin{aligned} f(t) &= \frac{1}{q_0 q_1 \cdots q_n} \cdot \left(q_0 \cdots q_{n-1} p_n t^n + q_0 \cdots q_{n-2} p_{n-1} q_n t^{n-1} + \cdots + p_0 q_1 \cdots q_n\right) \\ &= \frac{1}{q_0 q_1 \cdots q_n} \cdot f_\gamma(t) g(t), \end{aligned}$$

for some $g(t) \in \mathbb{Z}[t]$. From (11), we have $M(q_0 \cdots q_n) \cdot M(f) = M(f_\gamma)M(g)$, and hence,

$$\begin{aligned} M(f_\gamma) &\leq M(q_0) \cdots M(q_n) \cdot M(f) = |q_0| \cdots |q_n| \cdot M(f) \leq 2^{(n+1)B} \cdot M(f) \\ &\leq 2^{(n+1)B} \cdot \sqrt{1+n} \cdot 2^B = 2^{(n+2)B}\sqrt{1+n}, \end{aligned}$$

where the last inequality comes from Lemma 6 (4). Now we have

$$\begin{aligned} \mathrm{ht}(\gamma) &= \frac{1}{\deg(f_\gamma)} \log(M(f_\gamma)) \leq \log(M(f_\gamma)) \\ &\leq \log\left(2^{(n+2)B}\sqrt{1+n}\right) = (n+2)B\log 2 + \frac{1}{2}\log(n+1), \end{aligned}$$

which completes the proof. □

Lemma 10. *Let γ be an algebraic number, and let $g(t) \in \mathbb{Q}[t]$. Suppose that $\mathrm{ht}(\gamma) \geq 1$. Then we have*

$$\mathrm{ht}(g(\gamma)) \leq \frac{1}{2}\deg(g)\left(\deg(g)+1\right) \cdot \mathrm{ht}(\gamma) + 2\log 2 \cdot (\deg(g)+1)B(g) + \log(\deg(g)+1). \quad (14)$$

Proof. Let $n = \deg(g)$ and $B = B(g)$. Write

$$g(t) = \frac{p_n}{q_n}t^n + \frac{p_{n-1}}{q_{n-1}}t^{n-1} + \cdots + \frac{p_0}{q_0},$$

where $p_n, q_0, \ldots, q_n \neq 0$ and $\max_{i=0}^n \{|p_i|, |q_i|\} \leq 2^B$. Now we have

$$\begin{aligned} \mathrm{ht}(g(\gamma)) &= \mathrm{ht}\left(\frac{p_n}{q_n}\gamma^n + \frac{p_{n-1}}{q_{n-1}}\gamma^{n-1} + \cdots + \frac{p_0}{q_0}\right) \\ &\leq \mathrm{ht}\left(\frac{p_n}{q_n} \cdot \gamma^n\right) + \mathrm{ht}\left(\frac{p_{n-1}}{q_{n-1}} \cdot \gamma^{n-1}\right) + \cdots + \mathrm{ht}\left(\frac{p_0}{q_0}\right) + \log(n+1) \\ &\leq \sum_{i=1}^{n} \mathrm{ht}\left(\gamma^i\right) + \sum_{i=0}^{n} \left(\mathrm{ht}\left(p_i\right) + \mathrm{ht}\left(q_i\right)\right\} + \log(n+1) \\ &\leq \mathrm{ht}\left(\gamma\right) \cdot \sum_{i=1}^{n} i + \sum_{i=0}^{n} 2\log\left(2^B\right) + \log(n+1) \\ &\leq \frac{1}{2}n(n+1) \cdot \mathrm{ht}(\gamma) + 2\log 2 \cdot (n+1)B + \log(n+1), \end{aligned}$$

which completes the proof. □

Lemma 11. *The following hold for the polynomials $a(t)$, $b(t)$, and $d(t)$:*

$$\begin{aligned} B(a) = O(B), \qquad B(b) = O(B), \qquad B(d) = O(BN\log N), \\ B(a') = O(B\log N), \quad B(b') = O(B\log N), \quad B(d') = O\left(BN(\log N)^2\right). \end{aligned}$$

Proof. Use the relations between a, b, d and c_1, c_2, c_3, and Lemma 6, along with the following:

$$\begin{aligned}
B(d) &\leq B\left(c_1^2 + c_2^2 + (st - c_3)^2 + 1 - r^2\right) \\
&\leq B\left(c_1^2\right) + B\left(c_2^2\right) + B\left((st - c_3)^2\right) + B\left(r^2\right) + 4 \\
&\leq 2 \cdot (N+1)\log_2(N+1) \cdot 2B + (N+1)\log_2(N+1) \cdot 2B(st - c_3) + 2B + 4 \\
&= O(BN \log N), \\
B(d') &\leq B\left(2c_1c_1' + 2c_2c_2' + 2\left(st - c_3\right)\left(s - c_3'\right)\right) \\
&\leq 1 + B\left(c_1c_1' + c_2c_2' + \left(st - c_3\right)\left(s - c_3'\right)\right) \\
&\leq B\left(c_1c_1'\right) + B\left(c_2c_2'\right) + B\left(\left(st - c_3\right)\left(s - c_3'\right)\right) + 3 \\
&\leq 2 \cdot N \log_2 N \cdot \left(B + O\left(B \log N\right)\right) + N \log_2 N \cdot \left(B + O\left(B \log N\right)\right) + 3 \\
&= O\left(BN\left(\log N\right)^2\right).
\end{aligned}$$

□

By using Lemmas 5, 6, 9, 10, and 11, we obtain the following estimates for the quantities in (13) for each of the cases (i) $\alpha(t_*) \pm 1 = 0$, (ii) $\delta(t_*) \pm 1 = 0$, and (iii) $F'(t_*) = 0$.

(i) When $\alpha(t_*) \pm 1 = 0$:

$$\alpha(t_*) = \frac{a(t_*)}{\sqrt{a(t_*)^2 + b(t_*)^2}} = \pm 1 \quad \rightarrow \quad a(t_*)^2 = a(t_*)^2 + b(t_*)^2 \quad \rightarrow \quad b(t_*) = 0 \quad \rightarrow \quad c_2(t_*) = 0.$$

Note that $\deg(c_2) \leq N$ and $B(c_2) \leq B$. So we have:

$$\deg(t_*) \quad \leq \quad \deg(c_2) \leq N, \tag{15}$$

$$\deg(\alpha(t_*)) \quad = \quad \deg(\pm 1) = 1, \tag{16}$$

$$\deg(\delta(t_*)) \quad = \quad \deg\left(\frac{d(t_*)}{a(t_*)}\right) \leq \deg(t_*) \leq N, \tag{17}$$

$$\begin{aligned}
\mathrm{ht}(t_*) \quad &\leq \quad (\deg(c_2) + 2)B(c_2)\log 2 + \frac{1}{2}\log(\deg(c_2) + 1) \leq (N+2)B\log 2 + \frac{1}{2}\log(N+1) \\
&= \quad O(BN), &(18) \\
\mathrm{ht}(\alpha(t_*)) \quad &= \quad \mathrm{ht}(\pm 1) = 0, &(19) \\
\mathrm{ht}(\delta(t_*)) \quad &= \quad \mathrm{ht}\left(\frac{d(t_*)}{\sqrt{a(t_*)^2 + b(t_*)^2}}\right) = \mathrm{ht}\left(\frac{d(t_*)}{a(t_*)}\right) \leq \mathrm{ht}(a(t_*)) + \mathrm{ht}(d(t_*)) \\
&\leq \quad \frac{1}{2}\deg(a)\left(\deg(a) + 1\right) \cdot \mathrm{ht}(t_*) + 2\log 2 \cdot \left(\deg(a) + 1\right)B(a) + \log\left(\deg(a) + 1\right) \\
&\quad\quad + \frac{1}{2}\deg(d)\left(\deg(d) + 1\right) \cdot \mathrm{ht}(t_*) + 2\log 2 \cdot \left(\deg(d) + 1\right)B(d) + \log\left(\deg(d) + 1\right) \\
&\leq \quad \left\{\frac{1}{2}N(N+1) + N(2N+1)\right\} \cdot O\left(BN\right) + 2\log 2 \cdot (N+1) \cdot O(B) \\
&\quad\quad + 2\log 2 \cdot (2N+1) \cdot O(BN\log N) + \log\left(N+1\right) + \log\left(2N+1\right) \\
&= \quad O\left(BN^3\right). &(20)
\end{aligned}$$

(ii) When $\delta(t_*) \pm 1 = 0$:

$$\rightarrow \quad \delta(t_*) = \frac{d(t_*)}{\sqrt{a(t_*)^2 + b(t_*)^2}} = \pm 1 \quad \rightarrow \quad a(t_*)^2 + b(t_*)^2 - d(t_*)^2 = 0$$

Let $u(t) := a(t)^2 + b(t)^2 - d(t)^2 \in \mathbb{Q}[t]$. Note that $\deg(u) \le 4N$ and

$$\begin{aligned} B(u) &= B\left(a^2+b^2-d^2\right) \le B\left(a^2\right) + B\left(b^2\right) + B\left(d^2\right) + 2 \\ &\le 2\cdot(N+1)\log_2(N+1)\cdot 2B + (2N+1)\log_2(2N+1)\cdot 2B(d) + 2 \\ &= O\left(BN^2(\log N)^2\right) \end{aligned}$$

So we have

$$\begin{aligned} \deg(t_*) &\le \deg(u) \le 4N, && (21) \\ \deg(\alpha(t_*)) &= \deg\left(\frac{a(t_*)}{\sqrt{a(t_*)^2+b(t_*)^2}}\right) \le \deg(t_*) \le 4N, && (22) \\ \deg(\delta(t_*)) &= \deg(\pm 1) = 1, && (23) \end{aligned}$$

$$\begin{aligned} \mathrm{ht}(t_*) &\le (\deg(u)+2)B(u)\cdot\log 2 + \frac{1}{2}\log(\deg(u)+1) \\ &\le (4N+2)\log 2\cdot O\left(BN^2(\log N)^2\right) + \frac{1}{2}\log(4N+1) = O\left(BN^3(\log N)^2\right), && (24) \\ \mathrm{ht}(\alpha(t_*)) &= \mathrm{ht}\left(\frac{a(t_*)}{\sqrt{a(t_*)^2+b(t_*)^2}}\right) = \mathrm{ht}\left(\frac{a(t_*)}{d(t_*)}\right) \le \mathrm{ht}(a(t_*)) + \mathrm{ht}(d(t_*)) \\ &\le \frac{1}{2}\deg(a)\left(\deg(a)+1\right)\cdot\mathrm{ht}(t_*) + 2\log 2\cdot\left(\deg(a)+1\right)B(a) + \log\left(\deg(a)+1\right) \\ &\quad + \frac{1}{2}\deg(d)\left(\deg(d)+1\right)\cdot\mathrm{ht}(t_*) + 2\log 2\cdot\left(\deg(d)+1\right)B(d) + \log\left(\deg(d)+1\right) \\ &\le \left\{\frac{1}{2}N(N+1) + N(2N+1)\right\}\cdot O\left(BN^3(\log N)^2\right) + 2\log 2\cdot(N+1)\cdot O(B) \\ &\quad + 2\log 2\cdot(2N+1)\cdot O(BN\log N) + \log(N+1) + \log(2N+1) \\ &= O\left(BN^5(\log N)^2\right), && (25) \\ \mathrm{ht}(\delta(t_*)) &= \mathrm{ht}(\pm 1) = 0. && (26) \end{aligned}$$

(iii) When $F'(t_*) = 0$: Note that

$$\begin{aligned} F'(t) &= 1 - \frac{\alpha(t)}{\sqrt{1-\alpha(t)^2}} + \frac{\delta(t)}{\sqrt{1-\delta(t)^2}} \\ &= 1 - \frac{\frac{a'(t)\sqrt{a(t)^2+b(t)^2} - a(t)\frac{a(t)a'(t)+b(t)b'(t)}{\sqrt{a(t)^2+b(t)^2}}}{a(t)^2+b(t)^2}}{\sqrt{1-\frac{a(t)^2}{a(t)^2+b(t)^2}}} + \frac{\frac{d'(t)\sqrt{a(t)^2+b(t)^2} - d(t)\frac{a(t)a'(t)+b(t)b'(t)}{\sqrt{a(t)^2+b(t)^2}}}{a(t)^2+b(t)^2}}{\sqrt{1-\frac{d(t)^2}{a(t)^2+b(t)^2}}} \\ &= \frac{1}{\left\{a(t)^2+b(t)^2\right\}\sqrt{a(t)^2+b(t)^2-d(t)^2}} \\ &\quad \cdot\Big[\left\{\left(a(t)^2+b(t)^2\right) - \left(a'(t)b(t) - a(t)b'(t)\right)\right\}\sqrt{a(t)^2+b(t)^2-d(t)^2} \\ &\qquad + \left\{d'(t)\left(a(t)^2+b(t)^2\right) - d(t)\left(a'(t)a(t)+b'(t)b(t)\right)\right\}\Big] \end{aligned}$$

So we have $v(t_*) = 0$, where

$$\begin{aligned} v(t) := &\left\{a(t)^2+b(t)^2 - a'(t)b(t) + a(t)b'(t)\right\}^2\left\{a(t)^2+b(t)^2-d(t)^2\right\} \\ &- \left\{d'(t)\left(a(t)^2+b(t)^2\right) - d(t)\left(a'(t)a(t)+b'(t)b(t)\right)\right\}^2 \qquad \in \mathbb{Q}[t]. \end{aligned}$$

Note that $\deg(v) \le 8N$, and

$$\begin{aligned}
B(v) &\le (4N+1)\log_2(4N+1)\cdot\left\{B\left(\left(a^2+b^2-a'b+ab'\right)^2\right)+B(u)\right\} \\
&\quad +4N\log_2(4N)\cdot 2B\left(d'(a^2+b^2)-d(aa'+bb')\right)+1 \\
&\le (4N+1)\log_2(4N+1)\cdot\left\{(2N+1)\log_2(2N+1)\cdot 2B\left(a^2+b^2-a'b+ab'\right)\right. \\
&\qquad \left.+O\left(BN^2(\log N)^2\right)\right\} \\
&\quad +4N\log_2(4N)\cdot 2\left\{B\left(d'(a^2+b^2)\right)+B\left(d(aa'+bb')\right)+1\right\}+1 \\
&\le O\left(N^2(\log N)^2\right)\cdot\left\{B\left(a^2\right)+B\left(b^2\right)+B\left(a'b\right)+B\left(ab'\right)+3\right\}+O\left(BN^3(\log N)^3\right) \\
&\quad +O\left(N\log N\right)\cdot 2N\log_2(2N)\cdot\left\{B\left(d'\right)+B\left(a^2\right)+B\left(b^2\right)+B(d)+B\left(aa'\right)+B\left(bb'\right)+2\right\}+1 \\
&\le O\left(N^2(\log N)^2\right)\cdot O\left(BN(\log N)^2\right)+O\left(BN^3(\log N)^3\right) \\
&\quad +O\left(N\log N\right)\cdot 2N\log_2(2N)\cdot O\left(BN(\log N)^2\right)+1 \\
&= O\left(BN^3(\log N)^4\right).
\end{aligned}$$

So we have

$$\deg(t_*) \le \deg(v) \le 8N, \tag{27}$$

$$\deg(\alpha(t_*)) = \deg\left(\frac{a(t_*)}{\sqrt{a(t_*)^2+b(t_*)^2}}\right) \le \deg(t_*) \le 8N, \tag{28}$$

$$\deg(\delta(t_*)) = \deg\left(\frac{d(t_*)}{\sqrt{a(t_*)^2+b(t_*)^2}}\right) \le \deg(t_*) \le 8N, \tag{29}$$

$$\mathrm{ht}(t_*) \le (\deg(v)+2)B(v)\log 2+\frac{1}{2}\log(\deg(v)+1)=O\left(BN^4(\log N)^4\right), \tag{30}$$

$$\begin{aligned}
\mathrm{ht}(\alpha(t_*)) &= \mathrm{ht}\left(\frac{a(t_*)}{\sqrt{a(t_*)^2+b(t_*)^2}}\right) \le \mathrm{ht}\left(a(t_*)\right)+\mathrm{ht}\left(\sqrt{a(t_*)^2+b(t_*)^2}\right) \\
&= \mathrm{ht}(a(t_*))+\frac{1}{2}\mathrm{ht}\left(a(t_*)^2+b(t_*)^2\right) \le \mathrm{ht}(a(t_*))+\frac{1}{2}\left\{\mathrm{ht}\left(a(t_*)^2\right)+\mathrm{ht}\left(b(t_*)^2\right)+\log 2\right\} \\
&= 2\mathrm{ht}(a(t_*))+\mathrm{ht}(b(t_*))+\frac{1}{2}\log 2 \\
&\le 3\cdot\left\{\frac{1}{2}N(N+1)\cdot\mathrm{ht}(t_*)+2\log 2(N+1)B+\log(N+1)\right\}+\frac{1}{2}\log 2
\end{aligned}$$

$$= O\left(BN^6(\log N)^4\right), \tag{31}$$

$$\begin{aligned}
\mathrm{ht}(\delta(t_*)) &= \mathrm{ht}\left(\frac{d(t_*)}{\sqrt{a(t_*)^2+b(t_*)^2}}\right) \le \mathrm{ht}(d(t_*))+\mathrm{ht}(a(t_*))+\mathrm{ht}(b(t_*))+\frac{1}{2}\log 2 \\
&= O\left(\mathrm{ht}(d(t_*))\right)=O\left(\frac{1}{2}\cdot 2N(2N+1)\cdot\mathrm{ht}(t_*)+2\log 2(2N+1)\cdot O\left(BN\log N\right)+\log(2N+1)\right)
\end{aligned}$$

$$= O\left(BN^6(\log N)^4\right). \tag{32}$$

Lemma 12. *The constant k in (12) is bounded as: $k=O\left(2^{BN^2(\log N)^2}\right)$.*

Proof. t_1 and t_2 in

$$t_1 - 2\pi \le t + \arccos\alpha(t) - \arccos(-\delta(t)) \le t_2 + 2\pi$$

are zeros of $u(t) = a(t)^2 + b(t)^2 - d(t)^2$. So by using the Cauchy bound, we have

$$|2k| \le \frac{|t_i|}{\pi} + 2 \le \frac{1 + 2^{2B(u)}}{\pi} + 2 = O\left(2^{BN^2(\log N)^2}\right). \qquad \square$$

Now we are ready for the following bit complexity bound:

Theorem 13. *The sign of Λ in (12) can be determined using $O\left(B^3 \log B \cdot N^{28} (\log N)^{13}\right)$ bits.*

Proof. Note that $\Lambda = t_* + \arccos\alpha(t_*) - \arccos(\delta(t_*)) - 2k\arccos(-1)$. To apply Corollary 8, we let $n = 3$, $\gamma_0 = t_*$, $\gamma_1 = 1$, $\gamma_2 = -1$, $\gamma_3 = -2k$, $\beta_1 = \alpha(t_*)$, $\beta_2 = \delta(t_*)$, $\beta_3 = -1$. From (15)–(32), we have

$$\deg(\gamma_0) = O(N), \quad \deg(\gamma_1) = \deg(\gamma_2) = \deg(\gamma_3) = 1,$$

$$\deg(\beta_1) = \deg(\beta_2) = O(N), \quad \deg(\beta_3) = 1,$$

$$\mathrm{ht}(\gamma_0) = O\left(BN^4 (\log N)^4\right), \quad \mathrm{ht}(\gamma_1) = \mathrm{ht}(\gamma_2) = 0, \quad \mathrm{ht}(\gamma_3) = O\left(BN^2 (\log N)^2\right),$$

$$\mathrm{ht}(\beta_1) = \mathrm{ht}(\beta_2) = O\left(BN^6 (\log N)^4\right), \quad \mathrm{ht}(\beta_3) = 0.$$

Since

$$\begin{aligned} 2^4 \deg(\gamma_0)\deg(\gamma_1)\deg(\gamma_2)\deg(\gamma_3)\deg(\beta_1)\deg(\beta_2)\deg(\beta_3) &= O\left(N^3\right), \\ \max\{\mathrm{ht}(\gamma_0), \mathrm{ht}(\gamma_1), \mathrm{ht}(\gamma_2), \mathrm{ht}(\gamma_3)\} &= O\left(BN^4 (\log N)^4\right), \end{aligned}$$

we take $D = C_1 \cdot N^3$ and $W = C_2 \cdot BN^4 (\log N)^4$ for some positive constants C_1, C_2. Note that $\max\left\{2\mathrm{ht}(\beta_i) + \frac{3}{2}\log 2, \arccos\beta_i/D, 1/D\right\} \le \max\left\{O\left(BN^6 (\log N)^4\right), \pi/\left(C_1 N^3\right)\right\} = O\left(BN^6 (\log N)^4\right)$ for $i = 1, 2$, and $\max\left\{2\mathrm{ht}(\beta_3), \arccos\beta_3/D, 1/D\right\} \le \max\left\{0, \pi/\left(C_1 N^3\right)\right\} \le C_3 \cdot N^{-3}$ for some positive constant C_3. So we take $V_1 = C_3 \cdot N^{-3}$ and $V_2 = V_2^+ = V_3 = V_3^+ = C_4 BN^6 (\log N)^4$. Since $\min\left\{e^{DV_1}, \min_{1\le j\le 3}\left\{4DV_j/|\arccos\beta_j\right.\right.$
$\min\left\{e^{C_1C_3}, (1/\pi)\cdot\min\left\{4C_1C_3, 4C_1C_4BN^9(\log N)^4\right\}\right\}$, we can take $E = C_5$ for some constant $C_5 > 1$. Now by Corollary 8, we have

$$\begin{aligned} -\log(|\Lambda|) &< C \cdot D^5 V_1 V_2 V_3 \cdot \left\{W + \log\left(EDV_3^+\right)\right\} \cdot \log\left(EDV_2^+\right) \cdot (\log E)^{-4} \\ &= C \cdot \left(C_1 N^3\right)^5 \cdot \left\{C_3 C_4^2 B^2 N^9 (\log N)^8\right\} \cdot \left\{C_2 BN^4 (\log N)^4 + \log\left(C_1 C_4 C_5 BN^9 (\log N)^4\right)\right\} \\ &\quad \cdot \log\left(C_1 C_4 C_5 BN^9 (\log N)^4\right) \cdot (\log C_5)^{-4} \\ &= O\left(N^{15}\right) \cdot O\left(B^2 N^9 (\log N)^8\right) \cdot O\left(BN^4 (\log N)^4\right) \cdot O\left(\log B + \log N\right) \\ &= O\left(B^3 N^{28} (\log N)^{12} \cdot (\log B + \log N)\right) = O\left(B^3 \log B \cdot N^{28} (\log N)^{13}\right) \qquad \square \end{aligned}$$

Remark 1. *The number of times we need to determine the signs of such Λ's is bounded by:*

$$(\#\text{ zeros of } \alpha \pm 1, \delta \pm 1, F') \le (\#\text{ zeros of } b, u, w) = O(N).$$

Remark 2. *We have no intention to claim the asymptotic bound in Theorem 13 is the best we can get: The various estimation in Section 3 are rather 'generous'. Furthermore, there has been some improvements [4] for Waldschmidt's result, Proposition 7.*

4 Open Problems and Extensions

The main open problem arising directly from this paper is to decide collision between two helical motions.

The method in Section 2 covers slightly more general situations. For example, the motion of the point p can be of the form: $h(t) = (\cos t, \sin t, st) + (p_1(t), p_2(t), p_3(t))$, where $p_i(t)$'s are algebraic functions. Because non-circular part of the motion can be absorbed by $c(t)$, we obtain the same form of equation as (2). Also considering two balls, instead of a ball and a point, in the same type of motions does not change the form of the equation: say the radii of the balls are r_1 and r_2, then we want to check the equation $\|h(t) - c(t)\| \leq r_1 + r_2$.

However, a fundamentally different situation can occur if we consider, for example, an elliptic motion instead of a circular motion. The second-degree trigonometric functions do not cancel out as in (2). So the corresponding equation would look like

$$\rho \cos 2t + a(t) \cos t + b(t) \sin t + d(t) = 0, \tag{33}$$

for a constant ρ. This equation is not reduced to the form of (3) to which we can apply the zero bound discussed in Section 3.2. Currently, we do not know how to deal with equations of this type.

A similar difficulty arises if we consider a more general semi-algebraic body. Even if we consider a pure helical motion of a point and an algebraically parametrized motion, the collision equation that we have to deal with may involve higher-degree trigonometric functions, for example, up to $\sin dt$, where d is the degree of a polynomial (among possibly many) that defines the semi-algebraic body.

References

[1] A. Baker. *Transcendental Number Theory.* Cambridge University Press, 1979.

[2] E.-C. Chang, S. W. Choi, D. Kwon, H. Park, and C. Yap. Shortest paths for disc obstacles is computable. In *21st ACM Symp. on Comp. Geometry*, pages 116–125, 2005. June 5-8, Pisa, Italy.

[3] M. Hofer, B. Odehnal, H. Pottmann, T. Steiner, and J. Wallner. 3D shape recognition and reconstruction based on line element geometry. In *10th IEEE Intl. Conf. on Computer Vision (ICCV'05)*, volume 2, pages 1532–1538, 2005.

[4] E. M. Matveev. An explicit lower bound for a homogeneous rational linear form in logarithms of algebraic numbers. *Izvestiya, Mathematics*, 62(4):723–772, 1998.

[5] S. Mick and O. Röschel. Interpolation of helical patches by kinematic rational Bézier patches. *Computers and Graphics*, 14(2):275–280, 1990.

[6] J. T. Schwartz and M. Sharir. On the piano movers' problem: II. General techniques for computing topological properties of real algebraic manifolds. *Advances in Appl. Math.*, 4:298–351, 1983.

[7] V. Shapiro. Solid modeling. In G. Farin, J. Hoschek, and M.-S. Kim, editors, *Handbook of Computer Aided Geometric Design.* North-Holland, Amsterdam, 2002.

[8] M. Waldschmidt. Transcendence measures for exponentials and logarithms. *J. Austral. Math. Soc. Ser. A*, 25(4):445–465, 1978.

[9] M. Waldschmidt. *Diophantine Approximation on Linear Algebraic Groups.* Series of Comprehensive Studies in Mathematics, Vol.328. Springer, Berlin, 2000.

[10] C. K. Yap. Robust geometric computation. In J. E. Goodman and J. O'Rourke, editors, *Handbook of Discrete and Computational Geometry*, chapter 41, pages 927–952. Chapmen & Hall/CRC, Boca Raton, FL, 2nd edition, 2004. Expanded from 1997 version.