Drawing Math

Lev Stambler

May 12, 2022

Abstract

Given an object in cartesian space, we ask whether a repeating sequence of spherical updates to the object's position cause it to travel on a closed path. A spherical update to a position in D-dimensional space can be written as $(r, \theta_1, \theta_2, ..., \theta_{D-1})$. In this paper, we consider $D-1$ non-terminating rational numbers where for time-step i, the spherical updates' difference function is given by $r' \leftarrow r$, $\theta_1' \leftarrow \theta_1 + \text{digit}(q_1, i)$, ..., $\theta_{D-1}' \leftarrow \theta_{D-1} + \text{digit}(q_{D-1}, i)$. We then proceed to derive a formula for finding if the object takes a closed, repeating path. Moreover, we explore interesting properties of this problem and relate it to discrete log, roots of a multinomial, and center of mass.

1 Introduction

A glum Pittsburgh day inspired the authors to take a random walk down YouTube's recommended when they encountered the Numberphile video on "Plotting Pi" [MH22]. In the video, Henderson and Brady introduce the idea of taking a Python Turtle and deriving a series of updates to its position based off of various decimal sequences, some rational, some irrational. More specifically, they place an object in 2D, cartesian space starting at $(0, 0)$ and "facing" to the right. They then take a generating number, like π or $35/99$, which gives a decimal sequence (3.14... and $0.\overline{35}$ respectively). Then, at time step i, $i \geq 1$, they rotate the object by the ith digit divided by the base of the decimal sequence. Then, the Turtle moves a constant distance in the direction which it faces. For example, if the second digit is 4, the turtle is rotated by $\frac{4}{10}$ths of a circle counterclockwise at time step 2 and then moves 10 units in its new direction.

Whenever the Turtle moves, the program draws a red line along the Turtle's path. Thus, different lines are drawn. The authors noticed that using rational numbers to generate the sequence often drew geometrically aesthetic, closed shapes.

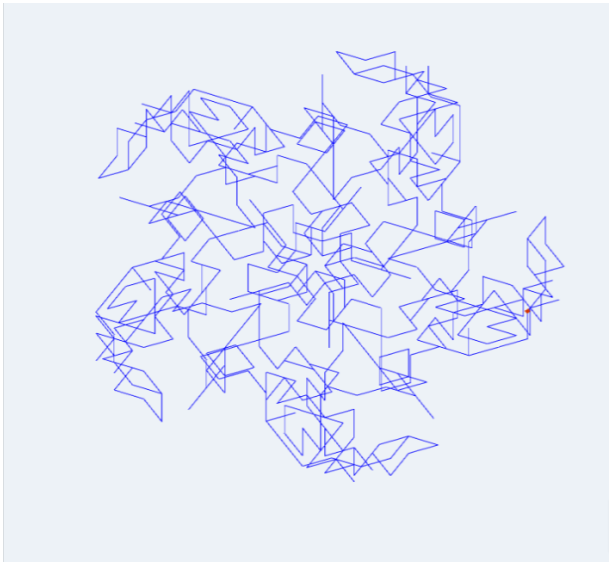

Figure 1: The closed shape generated from $\frac{13}{113} = 0.0977443609...$ in base 10.

Naturally, the authors were curious whether a Turtle in "3D" would also draw aesthetic shapes. In other words, what if the Turtle's orientation was described by 2 angles, pitch and yaw. The pitch and yaw would then by independently updated by 2 decimal sequences generated from 2 rational

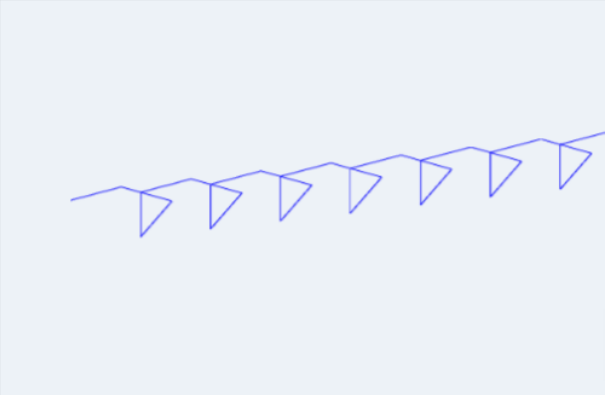

Figure 2: A non-closing shape generated from $\frac{2134}{9999} = 0.\overline{2134}$ in base 10.

numbers. After writing the program, we noticed that the Turtle would often fail to close. In other words, the Turtle would go off in one direction forever. But, the Turtle *sometimes* closed.

The authors then proceeded to ask why the Turtle would sometimes close and sometimes go off into the ether. After finding a closed form solution in 3 dimensional space, we proceeded to ask the same question in D dimensional space: given $D-1$ rational decimal sequences which determine the Turtle's orientation in space, does the Turtle move in a closed shape (i.e. is the Turtle position always contained within some D dimensional sphere off constant radius)?

2 Background

- Digital math - Euler's formula - I payed attention in some of my lectures

3 Definitions and questions

3.1 Definitions

Say you (yes you!) had a turtle living in D dimensional Euclidean space and in discrete time. At time step i, where $i \in \mathbb{Z}$ and $i > 0$, the turtle has position $p_i \in \mathbb{R}^D$. Then, lets define $\Delta p_{i+1} = p_{i+1} - p_i$; in other words, Δp_{i+1} is the change in position from time i to $i+1$.

Now say that the turtle's movement is determined by k seed parameter drawn from the same set. Then, for some state space $\mathcal{S}$, define $s_i^j \in \mathcal{S}$ to be some arbitrary state associated with timestamp i for the jth seed parameter where $j \in [k]$. Also, define $\boldsymbol{s}_i = (s_i^1, s_i^2, ..., s_i^k)$. Next we will define a set of functions $SU^j : \mathcal{S} \to \mathcal{S}$ (for State Updater) such that $s_{i+1}^j = SU^j(s_i^j, i)$. Note that for $j, a \in [m]$ where $j \neq a$, s_{i+1}^j is determined solely by s_i^j and i and not s_i^a.

Now that we have our machinery built up, lets define $Comb : \mathcal{S}^k \to \mathbb{R}^d$ such that

$$\Delta p_{i+1} = Comb\left(s_{i+1}^1, s_{i+1}^2, ..., s_{i+1}^k\right).$$

In other words, $Comb$ takes in the state of each seed and returns an update to the position of the turtle.

Finally, let us define

$$\Delta P_{a,b} = \sum_{i=a}^{b} \Delta p_i.$$

In other words, $\Delta P_{a,b}$ is the change in position from timestep a to b.

3.2 The problem

Say we are given, $Comb$, hhSU^j, p_0, and s_0^j for all $j \in [k]$. Informally, the question is whether the turtle draws a "closed" shape or not.
More formally, is there some period T such that

$$p_{i+\ell T} = p_i$$

for $i, \ell \in \mathbb{N}$. Then, note that if there exists a period T such that $\Delta P_{i,i+\ell T} = 0$ for all $i, \ell \in N$, $p_{i+\ell T} = p_i$ and the turtle forms a closed shape.

3.3 Specifying the task ahead of us

For our case, we consider $Comb, SU_i^j$ to all be memoryless (i.e. there output is uniquely determined by the current input). So, we can simplify the overall question. If, $\boldsymbol{s}_i = \boldsymbol{s}_{i+\ell T}$ for some $T \in \mathbb{N}$ and all $i \in \mathbb{N}$, then $\Delta p_i = \Delta p_{i+\ell T}$. So then, $\Delta P_{i,i+\ell T} = \Delta P_{i,i+\ell' T}$ for all $\ell, \ell' \in \mathbb{N}$. Thus, T is a period of the change in position. We can thus break down our problem into two parts:

1. Finding the period, T, of the state $\boldsymbol{s}$.
2. Checking whether $\Delta P_{i,i+T} = 0$.

3.4 Some more restrictions on our problem

We further restrict the problem by only considering $\mathcal{S} = \mathbb{N}^4$ where for $(n, d, b, \theta) \in \mathcal{S}$, n is the numerator of a rational in fraction form, d is the denominator, b is the base (i.e. base 10, base 12, etc.), and $\frac{2\theta}{b\pi}$ is an "angle" associated with the state.

Then, let $\phi^j : \mathbb{R} \to \mathbb{R}$ equal cos or sin.

Now, we will only consider

$$SU_i^j(n, b, d, \theta) = (n, b, d, \theta + \text{digit}(n, b, d, i) \mod b).$$

where digit(n, b, d, i) gives us the ith digit of the decimal expansion of $\frac{n}{d}$ in base b. For the sake of convenience, we will use the word "rational parameter" instead of "seed parameter" from here on out.

Moreover, we consider the case where

$$Comb((.,.,.,.,\theta^1),(.,.,.,.,\theta^2),...,(.,.,.,.,\theta^k)) = \left(\prod_{j=1}^{k} \phi^j\left(\frac{2\pi}{b^j}\cdot\theta^j\right)^{\text{incl}_1^j}, ..., \prod_{j=1}^{k} \phi^j\left(\frac{2\pi}{b^j}\cdot\theta^j\right)^{\text{incl}_D^j}\right)$$

where $\text{incl}_d^j \in \{0, 1\}$ for $d \in [D]$ indicates whether to include a given $x \in R$ determined by rational parameter j for position update in the dth dimension.

Finally, for simplicity's sake, assume that $\theta = 0$ for all $(n, b, d, \theta) \in \boldsymbol{s}_0$, $n < d$, and $\frac{n}{d}$'s decimal expansion is periodic after some $N \geq 0$ decimal places and does not terminate in base b.

Also, lets set

$$\boldsymbol{b} = \operatorname*{lcm}_{(n,b,d,\theta)\in\boldsymbol{s}_0} b.$$

In other words, $\boldsymbol{b}$ can be thought of as a "common base" among all rational parameters.

3.4.1 Some intuition

While the restrictions may seem arbitrary, they aptly match our original problem statement. The original problem statement derives a spherical change in position based off of a rational number's digit at a particular timestep. The polar change in position also has a fixed radius. Translating from a polar to cartesian update then only requires products of sins and coss. See [Blu60] for more details.

Take the three dimensional case for instance. The turtle's update cartesian space is given by

$$\begin{aligned} x &= \cos(\alpha) \\ y &= \sin(\alpha)\cos(\beta) \\ z &= \sin(\alpha)\sin(\beta) \end{aligned}$$

where $\alpha = \frac{2\pi}{b^1} \cdot \theta^1$ and $\beta = \frac{2\pi}{b^2} \cdot \theta^2$. We can thus see that our definition of $Comb$ captures the three dimensional case.

4 Does it close?

In understanding whether a set of given rationals, bases, and updated functions draw a closed shape in D dimensional space, we first need to find the period of the update delta, Δp_i. We then know that the total update over a period will be repeated indefinitely. Consequently, we then seek to find the total change in position over a period. If the total change is 0, the shape will close as the Turtle will end up at its starting point after every period length. If the total update is nonzero, the Turtle will not draw a closed shape.

4.1 Finding period T

We now show how to find a period T of state $\boldsymbol{s}$.

4.1.1 Finding the period of a fraction

For some $(n, b, d, \theta) \in \boldsymbol{s}_0$, we have that the period of the decimal expansion of $\frac{n}{d}$ can be determined by finding the smallest $T^{j'}$ such that

$$b^{T^{j'}} \equiv 1 \mod d \tag{1}$$

by [ho]. More generally though, any nontrivial $T^{j'}$ satisfying equation 1 will be a period of $\frac{n}{d}$. In other words, the decimal sequence specified by $\frac{n}{d}$ will repeat after every $T^{j'}$ steps for all digits $n > n_0$ for some fixed n_0.

Next, let

$$T' = \operatorname*{lcm}_{j \in [k]} T^{j'}.$$

Remark 4.1 (Complexity)**.** Interestingly, period finding of rational numbers is intimately tied to the discrete log problem and factoring. For more information, check out [ho]. This gives some intuition that this closure problem may not be in BPP (Bounded Error Polynomial Time), but may be in BQP (Bounded Error Quantum Polynomial Time) by [Sho97].

4.1.2 Digital sum

Next, we introduce the idea digital sums. For some number $N \in \mathbb{N}$, N can be represented in base b via

$$N = \sum_{i=0}^{m} d_i b^i \tag{2}$$

where $m = \lceil \log_b N \rceil$ and, $\forall i \in [m]$, $d_i \in \mathbb{Z}_b$. Then, we define function $\text{digSum} : \mathbb{N} \to \mathbb{Z}_b$ to give the digital sum such that

$$\text{digSum}(N) = \sum_{i=0}^{m} d_i. \tag{3}$$

Moreover, define $\sigma^j \in \mathbb{Z}_b$ such that

$$\sigma^j = \sum_{i=i_0}^{i_0+T'} \text{digit}(n, d, b, i). \tag{4}$$

In other words, T' is the digital sum over one period.

Remark 4.2 (Complexity)**.** For $d > 2$, prime, and coprime to b, we can find σ^j in polytime by multiplying $(b-1) \cdot \frac{d-1}{2} \mod b$ [KC81]. The authors are unsure as to the complexity of finding σ^j otherwise.

4.1.3 Finding a period of θ^j

For $(n^j, b^j, d^j, \theta_i^j) = s_i^j$, recall that $\theta_{i+1}^j = \theta_i^j + \text{digit}(n, b, d, i) \mod b$. So, after period T',

$$\begin{aligned} \theta_{i+T'} &= \left(\theta_i + \sum_{\ell=i}^{T'+i} \text{digit}(n, b, d, \ell) \right) \mod b \\ &= \left(\theta_i + \sigma^j \right) \mod b. \end{aligned}$$

So, after p periods of length T' where $p \cdot \sigma^j \equiv 0 \mod b$,

$$\theta_{i+pT'} \equiv \theta_i + 0 \equiv \theta_i.$$

For simplicity, lets define

$$T^j = pT'$$

where T^j is a period of the state for rational parameter j.

4.1.4 Finding the period of $\boldsymbol{s}$

We can first see that for $s^j \in \boldsymbol{s}$, s^j has period of T^j. So, $\boldsymbol{s}$ must have a period, T, of

$$\operatorname*{lcm}_{j \in [k]} T^j.$$

I.e. $\boldsymbol{s}_i = \boldsymbol{s}_{i+T}$ for all $i \in \mathbb{N}$.

4.2 Finding the change in position over a period

So now that we know the period of $\boldsymbol{s}$, we can ask if $\Delta P_{i,i+T} = 0$.

Note that

$$\Delta P_{i,i+T} = \Delta P_{q,q+T}$$

for all $i, q \in \mathbb{N}$ by definition of periodicity. So, we will drop the i and replace it with a 0. Then,

$$\begin{aligned}
\Delta P_{0,T} &= \sum_{i=1}^{T} \Delta p_i \\
&= \sum_{i=1}^{T} Comb\left(s_i^1, s_i^2, ..., s_i^k\right) \\
&= \sum_{i=1}^{T} \left(\prod_{j=1}^{k} \phi^j \left(\frac{2\pi}{b^j} \cdot \theta^j \right)^{\text{incl}_1^j}, ..., \prod_{j=1}^{k} \phi^j \left(\frac{2\pi}{b^j} \cdot \theta^j \right)^{\text{incl}_D^j} \right) \\
&= \left(\sum_{i=1}^{T} \prod_{j=1}^{k} \phi^j \left(\frac{2\pi}{b^j} \cdot \theta^j \right)^{\text{incl}_1^j}, ..., \sum_{i=1}^{T} \prod_{j=1}^{k} \phi^j \left(\frac{2\pi}{b^j} \cdot \theta^j \right)^{\text{incl}_D^j} \right).
\end{aligned}$$

We can thus see that $\Delta P_{0,T} = \mathbf{0} = (0, ..., 0)$ iff

$$\sum_{i=1}^{T} \prod_{j=1}^{k} \phi^j \left(\frac{2\pi}{b^j} \cdot \theta^j \right)^{\text{incl}_d^j} = 0 \tag{5}$$

for all $d \in D$. We can thus check for closure by computing (5) for each dimension.

4.3 Algorithm complexity

The algorithm we provide in equation (5) runs in time exponential in the size of the input assuming the Word RAM model. The period for the rational generated from rational parameter j, $1 \leq T^{j'} \leq d^j$. Then, the period over all rationals generated from parameters is at most

$$\operatorname*{lcm}_{j \in [k]} T^{j'} \leq \prod_{j \in [k]} T^{j'} \leq \left(\max_{j \in [k]} d^j \right)^k.$$

Then, $0 \leq T \leq T' \cdot \operatorname*{lcm}_{j \in [k]} b^j \leq T' \left(\max_{j \in [k]} b^j \right)^k$. And because evaluating the product in (5) takes $O(k)$ time, we have that the time for (5) is at most

$$O\left(\left[\max_{j \in [k]} (b^j d^j) \right]^k \right).$$

Then, note that computing the period of rational numbers via known classical methods takes exponential time in the number of digits of the denominator. So, computing $T^{j'}$ takes $O(d^j)$ time. Then, computing the σ^j can take $O(d^j)$ time. We can thus see that period finding takes at most

$$O\left(k \max_{j \in [k]} d^j \right)$$

time.

Because (5) must be computed for each dimension, the algorithm runs in

$$O\left(k \max_{j\in[k]} d^j\right) + O\left(\max_{j\in[k]} D(b^j d^j)^k\right) = O\left(\max_{j\in[k]} D(b^j d^j)^k\right)$$

time. Note that b^j, d^j are also exponential in the size of the input. We can thus see that our running time is quite atrocious (its worse than exponential). Moreover, the algorithm does not produce a proof, verifiable in polytime, for closure or lack there of. Thus, our algorithm is in neither NP or coNP.

5 Interesting Properties and an attempt at certificates

We will now proceed to go over some interesting properties of the closure question which may give rise to an algorithm in NP, coNP, or even BQP. These properties were discovered in the author's pursuit of simplifying the question. Moreover, these properties may guide some intuition as to the probability of closure for random rational seeds, a fixed k, and fixed bases b.

5.1 Property 1: Restricted Multinomials and Closure

Define $A_d = \{\, j \mid j \in [k] \text{ and } \text{incl}_d^j = 1 \,\}$, in other words, A_d is the set of rational parameters which are included in determining the position along the dth dimension. Also, for function $f : \mathbb{Z}_{\boldsymbol{b}}^{|A_d|} \to \mathbb{Z}_{\boldsymbol{b}}$ and $\{a_1, a_2, ..., a_{|A_d|}\} = A_d$, we will denote

$$f\left(\sigma^{a_1}, \sigma^{a_2}, ..., \sigma^{a_{A_d}}\right) = f\left(\sigma\right).$$

Then, let

$$\mathcal{M} = \{f : f(\boldsymbol{x}) = \pm x_1 \pm x_2 ... \pm x_{|A_d|}\}.$$

In other words, $\mathcal{M}$ is the set of all multinomials with $|A_d|$ variables with degree 1 and coefficients ± 1. Then, if

$$f\left(\sigma\right) \neq 0 \tag{6}$$

for all $f \in \mathcal{M}$ and $d \in [D]$, the turtle will always draw a closed shape. See Appendix A for the proof.

Satisfying (6) is true for all f is equivalent to

$$\prod_{f\in\mathcal{M}} f(\sigma) \neq 0.$$

where $\prod_{f\in\mathcal{M}} f$ is a polynomial of degree at most $2^{|A_d|} \leq 2^k$.

If we were to then assume that $(\sigma^1, ..., \sigma^k)$ is uniformly and randomly draw from $\mathbb{Z}_{\boldsymbol{b}}^k$, we then know that

$$\mathbf{Pr}\left[\prod_{f\in\mathcal{M}} f(\sigma) = 0\right] < \frac{2^k}{\boldsymbol{b}}$$

by the Schwartz-Zippel Lemma [Sch80] [Zip79]. So, this would leave us with

$$\mathbf{Pr}\left[\prod_{f\in\mathcal{M}} f(\sigma) \neq 0\right] > 1 - \frac{2^k}{\boldsymbol{b}}.$$

In particular, this means that the probability of closure would be at least

$$1 - \frac{2^k}{\boldsymbol{b}}.$$

Somewhat surprisingly, we can then see that probability of closure may increase exponentially with a decreasing k. Moreover, a larger $\boldsymbol{b}$ also increases the lower bound!

Remark 5.1 (Randomness assumption)**.** The randomness assumption, that $(\sigma^1, ..., \sigma^k)$ is drawn from a random distribution is very much not true. But, given a rational parameter there does seem to be some element of randomness for σ^j. See [KC81] for more information.

5.2 Property 2: Root of Restricted Multinomial and Closure

First note that

$$\mathcal{M} = \{f : f(\boldsymbol{x}) = \pm x_1 \pm x_2 ... \pm x_{|A_d|}\} = \left\{ \sum_{j \in |A_d|} (-1)^{\beta_j} \sigma^j : \beta \in \{0, 1\}^{|A_d|} \right\}.$$

Let $f_\beta \in \mathcal{M}$ then equal $\sum_{j \in |A_d|} (-1)^{\beta_j} \sigma^j$.

Then, let

$$\mathcal{B} = \{\beta : f_\beta(\sigma) = 0\}$$

and $\overline{\mathcal{B}} = \mathcal{M} \setminus \mathcal{B}$. Then, if for all $\beta \in \mathcal{B}$,

$$\sum_{q=0}^{T'-1} \exp\left(I \frac{2\pi}{\boldsymbol{b}} \sum_{\ell=0}^{q} \sum_{j \in A_d} (-1)^{\beta_j} \frac{\boldsymbol{b}}{b^j} \text{digit}(n, b, d, \ell) \right) = 0$$

the Turtle will draw a closed shape. While this may seem arbitrary, there is a unique and interesting geometric interpretation. Let rational sequence $a_1, a_2, ..., a_{T'}$ be equal to $\forall \ell \in [T']$,

$$a_\ell = \sum_{j \in A_d} (-1)^{\beta_j} \frac{\boldsymbol{b}}{b^j} \text{digit}(n, b, d, \ell).$$

In other words, we are creating a "common" rational sequence by summing and subtracting our rational parameters in the least common multiple base $\boldsymbol{b}$. Then, if

$$\sum_{q=0}^{T'-1} \exp\left(I \frac{2\pi}{\boldsymbol{b}} \sum_{\ell=0}^{q} a_\ell \right) = 0$$

the Turtle closes. If $r_i = \frac{2\pi}{\boldsymbol{b}} \sum_{\ell=0}^{q} a_\ell$ for $i \in \{0, ..., T' - 1\}$. Then $\exp(I \cdot r_i)$ can be thought of as some point around the unit circle. Also, note that $r_{i+1} = r_i + \frac{2\pi}{\boldsymbol{b}} a_{i+1}$. In otherwords, r_i denotes some position around the complex unit circle where the subsequent updates to position are given by a sum and subtraction of rational parameters. Then, if the center of mass of these points around the unit circle is 0, the Turtle draws a closed shape! The authors are unsure as to the underlying intuition for why this is true.

Over one common period for a all rational sequences, T',

6 Open Questions and Future Work

A whole host of questions naturally arise from this problem. We will proceed to list the ones which immediately stand out. For a complete list of open problems, which have been solved, and the associated (financial) reward to each question, see our website

1. **Periodic Digit Sum in NP?**: As far as the authors are aware, given any rational number, $\frac{n}{d}$ in a fixed base b, is finding the sum of the digits in one period modulo b in NP? I.e. could one give a poly-size certificate to a poly-time verifier which verifies if a digital sum equals $\sigma \in \mathbb{Z}_b$? The size of the input is the number of bits required to describe $\frac{n}{d}$. The authors feel that intuitively the answer should be yes. A certificate could potentially be related to the factors of the denominator and the period length. I.e. we know how to find the periodic digital sum of a prime in polynomial time (see 4.2). So, could we somehow use this in combination with a prime factorization?

2. **Closure in NP or CoNP?**: For fixed bases of size b, is closure in NP of CoNP? I.e. is there is a poly-sized certificate and poly-time verifier which can prove or disprove that $D-1$ rationals draw a closed shape? The author's are uncertain here but conjecture may be in CoNP. Either a gadget based reduction or a direct algorithm to generate a valid certificate suffice to answer this question.

3. **Distribution** : Given a random rational number $\frac{n}{d}$ where $n \sim \mathbb{Z}_q$ and $d \sim \mathbb{Z}_q$ for some fixed $q \in \mathbb{N}$, what is the distribution of σ, the periodic digital sum modulo base b? Specifically, is the distribution indistinguishable [Bar97] from the uniform distribution of $\mathbb{Z}_b$? See remark 5.1 for an application of this result.

4. **Decomposition**: This one is totally out of left field. From our analysis, it seems as if using rational numbers to draw out shapes has a lot of underlying complexity but also a lot of structure. The authors were wondering if given any closed shape ℓ which can be described with n bits, could poly-n bits be used in combination with the rational sequence drawing algorithm described throughout this paper as description of ℓ. In other words, could some sort of "Fourier Transform" be done between an explicitly described closed shape and a sequence of rationals? We are also interested whether $1-\epsilon$ approximation exists (where the approximation "goodness" could be measured as a function of average distance from the original line to the line generated via the sequence of rationals).

5. **Closure in BQP?**: Given that closure is intimately tied with period finding, the authors wonder if this problem is in BQP (Bounded-error Quantum Polynomial Time). An algorithm or existence result suffices.

6. **A different approach?**: Could a change in basis and/ or vector calculus be used (as a means of dealing with the change of basis from spherical coordinates to cartesian) to simplify the problem analysis? The authors conjecture yes as all updates are in spherical coordinates but most of the paper's analysis is done in cartesian space. But, it is not immediately obvious to the authors how a change of basis could be applied.

7 Conclusion

Acknowledgments

A Proving Property 1 and 2

First let $I = \sqrt{-1}$ instead of i. This is done as i is already reserved to represent the current time step.

Now, before getting to the main proof, we need to prove the following lemma

Lemma A.1. *For all $j \in [k]$ and $x, y \in \mathbb{N}$ where $y < T'$, we have that*

$$\theta^j_{xT'+y} = x \cdot \sigma^j + \sum_{q=0}^{y} \text{digit}(n, b, d, q)$$

Proof. We can then see that for $(n, b, d, \theta^j_{xT'+y}) \in \boldsymbol{s}_{xT'+y}$,

$$\begin{aligned}
\theta^j_{xT'+y} &= \sum_{i=0}^{xT'+y} \text{digit}(n, b, d, i) \\
&= \sum_{p=0}^{(x-1)T'} \sum_{q=0}^{T'-1} \text{digit}(n, b, d, pT' + q) + \sum_{q=xT'}^{xT'+y} \text{digit}(n, b, d, q) \\
&= x \cdot \sigma^j + \sum_{q=xT'}^{T'+y} \text{digit}(n, b, d, q) \\
&= x \cdot \sigma^j + \sum_{q=0}^{y} \text{digit}(n, b, d, q)
\end{aligned}$$

because $\text{digit}(n, b, d, xT' + \ell) = \text{digit}(n, b, d, \ell)$ for any $\ell \in \mathbb{N}$ by definition of periodicity. □

Let $\Delta P^d_{0,T}$ be the change of position along dimension d from timestep 0 to T. We are now ready to determine if we "close" along one dimension. I.e. does $\Delta P^d_{0,T} = 0$?

Define $A_d = \{\, j \mid j \in [k] \text{ and } \text{incl}^j_d = 1 \,\}$, in other words, A_d is the set of rational parameters which are included in determining the position along the dth dimension. We can then see that

$$\begin{aligned}
\Delta P^d_{0,T} &= \sum_{i=1}^{T} \prod_{j=1}^{k} \phi^j \left(\frac{2\pi}{b^j} \cdot \theta^j \right)^{\text{incl}^j_d} \\
&= \pm \sum_{i=1}^{T} \prod_{j=1}^{k} \left(\tfrac{1}{2} \left(\exp\left(\frac{2\pi}{b^j} \theta^j_i I \right) \pm \exp\left(-\frac{2\pi}{b^j} \theta^j_i I \right) \right) \right)^{\text{incl}^j_d} \\
&= \pm 2^{-|A|} \sum_{p=0}^{\frac{T}{T'}-1} \sum_{q=0}^{T'-1} \prod_{j \in A_d} \left(\exp\left(\frac{2\pi}{b^j} \theta^j_{pT'+q} I \right) \pm \exp\left(-\frac{2\pi}{b^j} \theta^j_{pT'+q} I \right) \right)
\end{aligned}$$

by the Euler form of cos and sin and the fact that $\Delta P^d_{0,T}$ is real.

Next, observe that

$$\prod_{j\in A_d}\left(\exp\left(\frac{2\pi}{b^j}\theta^j_{pT'+q}I\right)\pm\exp\left(-\frac{2\pi}{b^j}\theta^j_{pT'+q}I\right)\right)$$
$$=\exp(\frac{2\pi}{b^1}\theta^1_{pT'+q}+\frac{2\pi}{b^2}\theta^2_{pT'+q}+...+\frac{2\pi}{b^d}\theta^d_{pT'+q})\pm\exp(\frac{2\pi}{b^1}\theta^1_{pT'+q}-\frac{2\pi}{b^2}\theta^2_{pT'+q}+...+\frac{2\pi}{b^d}\theta^d_{pT'+q})+...$$
$$\pm\exp(-\frac{2\pi}{b^1}\theta^1_{pT'+q}-\frac{2\pi}{b^2}\theta^2_{pT'+q}-...-\frac{2\pi}{b^d}\theta^d_{pT'+q})$$

which then equals

$$\sum_{\beta\in\{0,1\}^{|A_d|}}\pm\exp\left(\frac{2\pi}{\boldsymbol{b}}I\sum_{j\in A_d}-1^{\beta(j)}\frac{\boldsymbol{b}}{b^j}\theta^j_{pT'+q}\right)\tag{7}$$

where β can be though of as a bit string deciding whether the angle from seed $j\in A_d$ is added to or subtracted from the exponent.

Then, we have that

$$\begin{aligned}\Delta P^d_{0,T}&=\pm\,2^{-|A|}\sum_{p=0}^{\frac{T}{T'}-1}\sum_{q=0}^{T'-1}\sum_{\beta\in\{0,1\}^{|A_d|}}\pm\exp\left(\sum_{j\in A_d}-1^{\beta(j)}\theta^j_{pT'+q}I\right)\\&=\pm\,2^{-|A|}\sum_{\beta\in\{0,1\}^{|A_d|}}\pm\sum_{p=0}^{\frac{T}{T'}-1}\sum_{q=0}^{T'-1}\exp\left(\sum_{j\in A_d}-1^{\beta(j)}\theta^j_{pT'+q}I\right).\end{aligned}$$

Then, lets fix some $\beta\in\{0,1\}^{|A_d|}$, define Q such that

$$Q=\sum_{p=0}^{\frac{T}{T'}-1}\sum_{q=0}^{T'-1}\exp\left(\sum_{j\in A_d}-1^{\beta(j)}\theta^j_{pT'+q}I\right).\tag{8}$$

We will simplify Q to show 2 distinct cases where $Q=0$ for any choice of β.

Observe that

$$\begin{aligned}\exp(\theta^j_{pT'+q}I)&=\exp\left(p\cdot\sigma^j+\frac{\boldsymbol{b}}{b^j}\sum_{\ell=pT'}^{pT'+q}\text{digit}(n^j,b^j,d^j,\ell)\right)&\text{(by lemma A.1)}\\&=\exp\left(p\cdot\sigma^j\right)\exp\left(\frac{\boldsymbol{b}}{b^j}\sum_{\ell=0}^{q}\text{digit}(n,b,d,\ell)\right).&(9)\end{aligned}$$

So then, by equation (9), we get that

$$\begin{aligned}&\exp\left(\sum_{j\in A_d}-1^{\beta(j)}\theta^j_{pT'+q}I\right)\\&=\exp\left(I\sum_{j\in A_d}-1^{\beta(j)}\cdot p\cdot\sigma^j\right)\exp\left(I\sum_{j\in A_d}-1^{\beta(j)}\frac{\boldsymbol{b}}{b^j}\sum_{\ell=0}^{q}\text{digit}(n^j,b^j,d^j,\ell)\right).&(10)\end{aligned}$$

We then use (10) to show that Q equals

$$\sum_{p=0}^{\frac{T}{T'}-1}\left[I\exp\left(pI\sum_{j\in A_d}-1^{\beta(j)}\sigma^j\right)\left(I\sum_{q=0}^{T'-1}\exp\left(\sum_{j\in A_d}-1^{\beta(j)}\frac{\boldsymbol{b}}{b^j}\sum_{\ell=0}^{q}\text{digit}(n^j,b^j,d^j,\ell)\right)\right)\right].\tag{11}$$

Case 1: $\sum_{j\in A_d} -1^{\beta_{(j)}}\sigma^j \neq 0$

Define

$$C_\beta = \sum_{q=0}^{T'-1} \exp\left(\sum_{j\in A_d} -1^{\beta_{(j)}} \frac{\boldsymbol{b}}{b^j} \sum_{\ell=0}^{q} \text{digit}(n,b,d,\ell)\right).$$

Moreover, note that

$$\exp\left(pI \sum_{j\in A_d} -1^{\beta_{(j)}}\sigma^j\right) = \prod_{j\in A_d} \exp\left(-1^{\beta_{(j)}} pI\cdot\sigma^j\right)$$

and that

$$\exp\left(-1^{\beta_{(j)}} pI\cdot\sigma^j\right) = \exp(0) = 1$$

when $p = \frac{T}{T'}$. So, we can see that

$$\prod_{j\in A_d} \exp\left(-1^{\beta_{(j)}} pI\cdot\sigma^j\right) = 1$$

when $p = \frac{T}{T'}$.

Because σ^j is a constant, we can conclude that

$$\exp\left(I \sum_{j\in A_d} -1^{\beta_{(j)}}\sigma^j\right)$$

is a $\frac{T}{T'}^{th}$ root of unity iff

$$\sum_{j\in A_d} -1^{\beta_{(j)}}\sigma^j \neq 0$$

So, for $\sum_{j\in A_d} -1^{\beta_{(j)}}\sigma^j \neq 0$, we have that

$$\begin{aligned}
\sum_{p=0}^{\frac{T}{T'}-1}\sum_{q=0}^{T'-1} \exp\left(\sum_{j\in A_d} -1^{\beta_{(j)}}\theta^j_{pT'+q} I\right) &= C_\beta \sum_{p=0}^{\frac{T}{T'}-1} \exp\left(pI \sum_{j\in A_d} -1^{\beta_{(j)}}\sigma^j\right) \\
&= C_\beta \sum_{p=0}^{\frac{T}{T'}-1} \exp\left(W^p_{\frac{T}{T'}}\right) \\
&= 0.
\end{aligned}$$

where $W^p_{\frac{T}{T'}}$ is the $\frac{T}{T'}^{th}$ root of unity.

Case 2: $\sum_{j\in A_d} -1^{\beta_{(j)}}\sigma^j = 0$

If $\sum_{j\in A_d} -1^{\beta_{(j)}}\sigma^j = 0$, then

$$\begin{aligned}
\sum_{p=0}^{\frac{T}{T'}-1}\sum_{q=0}^{T'-1} \exp\left(\sum_{j\in A_d} -1^{\beta_{(j)}}\theta^j_{pT'+q} I\right) &= C_\beta \sum_{p=0}^{\frac{T}{T'}-1} \exp(0) \\
&= C_\beta.
\end{aligned}$$

So

$$\sum_{p=0}^{\frac{T}{T'}-1}\sum_{q=0}^{T'-1}\exp\left(\sum_{j\in A_d}-1^{\beta_{(j)}}\theta^j_{pT'+q}I\right)=0$$

iff $C_\beta = 0$.

To conclude

If, $\forall\beta\in\{0,1\}^{|A_d|}$, $\sum_{j\in A_d}-1^{\beta_{(j)}}\neq 0$ or $C_\beta=0$, then

$$\begin{aligned}\Delta P^d_{0,T} &= \sum_{i=1}^{T}\prod_{j=1}^{k}\phi^j\left(\frac{2\pi}{b^j}\cdot\theta^j\right)^{\mathrm{incl}^j_d}\\ &= 2^{-|A|}\sum_{\beta\in\{0,1\}^{|A_d|}}\sum_{p=0}^{\frac{T}{T'}-1}\sum_{q=0}^{T'-1}\exp\left(\sum_{j\in A_d}-1^{\beta_{(j)}}\theta^j_{pT'+q}I\right)\\ &= 0.\end{aligned}$$

If the above is true for all $d\in D$, then $\Delta P_{0,T}=0$.

References

[Bar97] Boaz Barak. Computational indistinguishability, pseudorandom generators, 2097. 3

[Blu60] L. E. Blumenson. A derivation of n-dimensional spherical coordinates. *The American Mathematical Monthly*, 67(1):63–66, 1960. 3.4.1

[ho] Glen O (https://math.stackexchange.com/users/67842/glen o). Length of period of decimal expansion of a fraction. Mathematics Stack Exchange. URL:https://math.stackexchange.com/q/2611737 (version: 2018-01-19). 4.1.1, 4.1

[KC81] S. Kak and A. Chatterjee. On decimal sequences (corresp.). *IEEE Transactions on Information Theory*, 27(5):647–652, 1981. 4.2, 5.1

[MH22] Brady Haran Matt Henderson. Plotting pi and searching for mona lisa - numberphile. https://www.youtube.com/watch?v=tkC1HHuuk7c, February 2022. 1

[Sch80] J. T. Schwartz. Fast probabilistic algorithms for verification of polynomial identities. *J. ACM*, 27(4):701–717, oct 1980. 5.1

[Sho97] Peter W. Shor. Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer. *SIAM Journal on Computing*, 26(5):1484–1509, oct 1997. 4.1

[Zip79] Richard Zippel. Probabilistic algorithms for sparse polynomials. In Edward W. Ng, editor, *Symbolic and Algebraic Computation*, pages 216–226, Berlin, Heidelberg, 1979. Springer Berlin Heidelberg. 5.1