

# Drawing Math

Lev Stambler

May 11, 2022

# 1 Introduction

- Numberphile video - I was bored and this looked fun - I wasn't paying attention in one of my lectures... - This paper is purely for funs... for now

## 2 Background

- Digital math - Euler's formula - I paid 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, let's define  $\Delta p_{i+1} = p_{i+1} - p_i$ ; in other words,  $\Delta p_{i+1}$  is the change in position from time  $i$  to  $i + 1$ .

Now say that the turtle's movement is determined by  $k$  seed parameters 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  $j$ th seed parameter where  $j \in [k]$ . Also, define  $\mathbf{s}_i = (s_i^1, s_i^2, \dots, s_i^k)$ . Next we will define a set of functions  $SU^j : \mathcal{S} \rightarrow \mathcal{S}$  (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, let's define  $Comb : \mathcal{S}^k \rightarrow \mathbb{R}^d$  such that

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

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,  $Comb$ ,  $SU^j$ ,  $p_0$ , 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  $i, \ell \in \mathbb{N}$ ,  $p_{i+\ell T} = p_i$  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. their output is uniquely determined by the current input). So, we can simplify the overall question. If,  $\mathbf{s}_i = \mathbf{s}_{i+\ell T}$  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  $\mathbf{s}$ .
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  $\phi^j : \mathbb{R} \rightarrow \mathbb{R}$  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  $\text{digit}(n, b, d, i)$  gives us the  $i$ th 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

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

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  $d$ th dimension.

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

Also, let’s set

$$\mathbf{b} = \text{lcm}_{(n,b,d,\theta) \in \mathbf{s}_0} b.$$

In other words,  $\mathbf{b}$  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 sines 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,  $\Delta p_i$ . 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 $T$

#### 4.1.1 Finding the period of $\frac{n}{d}$

We will first aim to find period  $T$  of the state  $\mathbf{s}$ . For some  $(n, b, d, \theta) \in \mathbf{s}_0$ , by [ho], we have that the period of the decimal expansion of  $\frac{n}{d}$  can be determined by finding the smallest  $T^{j'}$  such that

$$b^{T^{j'}} \equiv 1 \pmod{d}. \quad (1)$$

More generally though, any nontrivial  $T^{j'}$  satisfying equation 1 will be a period of  $\frac{n}{d}$ .

Next, let

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

**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

$$N = \sum_{i=0}^m d_i b^i \quad (2)$$

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

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

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

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

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  $\sigma^j$  in polytime by multiplying  $(b-1) \cdot \frac{d-1}{2} \pmod{b}$  [KC81]. The authors are unsure as to the complexity of finding  $\sigma^j$  otherwise.

#### 4.1.3 Finding a period of $\theta^j$

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

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

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

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

For simplicity, let's define

$$T^j = pT'$$

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

#### 4.1.4 Finding the period of $\mathbf{s}$

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

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

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

### 4.2 Finding the change in position over a period

So now that we know the period of  $\mathbf{s}$ , 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,

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

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

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

Then,  $0 \leq T \leq T' \cdot \text{lcm}_{j \in [k]} b^j \leq T' \left( \max_{j \in [k]} b^j \right)^k$ . 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  $\sigma^j$  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 thereof. 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 Monomials 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  $d$ th dimension. Also, for function  $f : \mathbb{Z}_{\mathbf{b}}^{|A_d|} \rightarrow \mathbb{Z}_{\mathbf{b}}$  and  $\{a_1, a_2, \dots, a_{|A_d|}\} = A_d$ , we will denote

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

Then, let

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

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

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

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  $(\sigma^1, \dots, \sigma^k)$  is uniformly and randomly drawn from  $\mathbb{Z}_{\mathbf{b}}^k$ , we then know by the Schwartz-Zippel Lemma

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

So, this would leave us with

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

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

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

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

**Remark 5.1** (Randomness assumption). The randomness assumption, that  $(\sigma^1, \dots, \sigma^k)$  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  $\sigma^j$ . See [KC81] for more information.

## 6 Conclusion

## 7 Open Questions

## Acknowledgments

## A Proving Property 1

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*

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

*Proof.* We can then see that for  $(n, b, d, \theta_{xT'+y}^j) \in \mathbf{s}_{xT'+y}$ ,

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

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

Let  $\Delta P_{0,T}^d$  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  $\Delta P_{0,T}^d = 0$ ?

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  $d$ th dimension. We can then see that

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

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

Next, observe that

$$\begin{aligned} &\prod_{j \in A_d} \left( \exp \left( \frac{2\pi}{b^j} \theta_{pT'+q}^j I \right) \pm \exp \left( -\frac{2\pi}{b^j} \theta_{pT'+q}^j I \right) \right) \\ &= \exp \left( \frac{2\pi}{b^1} \theta_{pT'+q}^1 + \frac{2\pi}{b^2} \theta_{pT'+q}^2 + \dots + \frac{2\pi}{b^d} \theta_{pT'+q}^d \right) \pm \exp \left( \frac{2\pi}{b^1} \theta_{pT'+q}^1 - \frac{2\pi}{b^2} \theta_{pT'+q}^2 + \dots + \frac{2\pi}{b^d} \theta_{pT'+q}^d \right) + \dots \\ &\quad \pm \exp \left( -\frac{2\pi}{b^1} \theta_{pT'+q}^1 - \frac{2\pi}{b^2} \theta_{pT'+q}^2 - \dots - \frac{2\pi}{b^d} \theta_{pT'+q}^d \right) \end{aligned}$$



which then equals

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

where  $\beta$  can be thought 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

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

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

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

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

Observe that

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

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

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

We then use (10) to show that  $Q$  equals

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

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

Define

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

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  $\sigma^j$  is a constant, we can conclude that

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

is a  $\frac{T}{T'}$ <sup>th</sup> 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

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

where  $W_{\frac{T}{T'}}^p$  is the  $\frac{T}{T'}$ <sup>th</sup> 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

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

So

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

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

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

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

## References

- [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](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
- [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