Spring 2023

Applying Hallgren's algorithm for solving Pell's equation to finding the irrational slope of the launch of a billiard ball

Sangheon Choi
Rose-Hulman Institute of Technology, CHOIS3@rose-hulman.edu

Applying Hallgren's algorithm for solving Pell's equation to finding the irrational slope of the launch of a billiard ball

Sangheon Choi

October 2, 2023

Introduction

This thesis is an exploration of Quantum Computing applied to Pell's equation in an attempt to find solutions to the *Billiard Ball Problem*. Pell's equation is a Diophantine equation in the form of $x^2 - ny^2 = 1$, where n is a given positive nonsquare integer, and integer solutions are sought for x and y. We will be applying Hallgren's algorithm for finding irrational periods in functions, in the context of billiard balls and their movement on a friction-less unit square billiard table. Our central research question has been the following:

Given the cutting sequence of the billiard ball's movement, can you find the irrational slope value in which the billiard ball was put in motion?

Given a function that provides the cutting sequence, we theorize it can be input into Hallgren's algorithm and find the slope (the irrational period). Here, the cutting sequence is the sequence of 0s or 1s that track the walls of the billiard table the ball has had contact with.

For example: Figure 1 contains a billiard with cutting sequence $0101\ldots$. We can observe the trajectory that some billiard ball would take, if it started at the bottom left corner of the table. As the first wall it touches is the top horizontal wall, we record a 0. The next wall it touches is the right-side vertical wall so we record a 1. This continues as the ball moves forward.

We rigorously study Pell's equation due to the parallels it can provide to solving the billiard ball problem. Pell's equation provides us with a function $f(x)$ that we can input into Hallgren's algorithm that produces a value known as the *regulator* that can be used to find solutions for some d value. Similiarly, we expect to find some function $f(x)$ that produces the cutting sequence, that we can then input into Hallgren's algorithm to produce the pseudo-period and find an irrational slope value that the billiard ball is launched at.

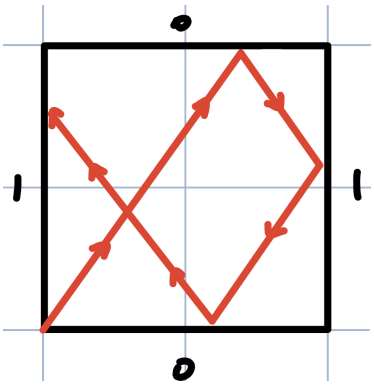

Figure 1: Example billiard table

1 Motivation

Because many questions in theoretical mathematics are the complete opposite of applied, a question often asked is, why should the reader care? This is an attempt to provide context to the reader of why this work is interesting.

Pell's equation

This is Pell's equation:

$$x^2 - dy^2 = 1$$

Pell's equation is the simplest non-linear equation and it has a long history of study [7, p. 76], dating back to the times of ancient Greeks and Indians. The ancient Greeks (Archimedes and Diophantus) and Indians (Brahmagupta and Baudhayana) found solutions to specific examples of Pell's equation, such as examples when $n = 2$. Later Indian mathematicians found general solutions to Pell's equation, as Bhaskara II built on Brahmagupta's work to develop the *chakravala* method [4, pp. 247–250].

The Greeks had an associated word problem that Pell's equation was meant to solve, known as *Archimedes's Cattle Problem* [9]. The solution consisted of solving simultaneous Diophantine equations. Diophantine equations are equations of the form $ax + by + cz + \ldots = d$, where $a, b, c \ldots d$ are all integers, and x, y, z are integers that are solutions to the equation. These equations can be used to model Archimedes's Cattle Problem with various relations between different types of cows and their ratios between one another as the coefficients for the equations. Such natural occurrences of Pell's equation indicate serious studies will yield results in many unforseen ways (including that 7.76×10^{206544} cattle is the smallest number necessary to solve all simultaneous equations of conditions set out by the Cattle Problem's parameters).

Pell's equation also has applications to cryptography. Pell's equation can be

used to generate public-key cryptographic systems, in the form of the Buchmann-Williams cryptosystem. [1].

Billiard Balls

Billiard balls and theoretical mathematics, on the surface, do not share a clear link. Our key text on this subject, *Geometry and Billiards* [8, p. 7], cites that the 1,400 different articles on Billiards alone (in 2005) is proof that this field is of great interest. Billiards provide a framework in which to study dynamical systems, with connections to geometry and physics. Billiards and billiard tables have been described as not a field of mathematics, but a mathematician's playground in which to play with and test various methods [3]. Russian mathematics has always veered on the side of study for study's sake, and the pursuit of knowledge alone is often justification for study.

2 Literature Review

2.1 Explorations in Quantum Computing

A text referenced for this project was the textbook *Explorations in Quantum Computing* by Colin P. Williams [9]. This text explores fundamental concepts in Quantum Computing, and has a dedicated section on Hallgren's algorithm and its relation to Pell's equation. This text also introduces the Cattle Problem of Archimedes and the regulator. The Cattle Problem of Archimedes is an interesting application of Pell's equation, and the regulator, $R = \ln x_1 + \sqrt{d}y_1$, where (x_1, y_1) is used to uniquely identify least positive solutions to Pell's equation for some non-square coefficient value d.

To discuss Hallgren's algorithm, we must first learn about Shor's algorithm. Shor's algorithm is arguably one of the most famous algorithms discovered under the umbrella of quantum computing. Shor's algorithm is a quantum algorithm for integer factorization, which means that it can find the prime factors of a given integer exponentially faster than any known classical algorithm. One of the key steps in Shor's algorithm is period-finding, which is used to find the period of a certain function. The period-finding step of Shor's algorithm works as follows: Given an integer N and an integer a that is relatively prime to N, we want to find the smallest positive integer r such that a^r is congruent to 1 modulo N. In other words, we want to find the period of the function $f(x) = a^x$ modulo N. The computation is performed on a quantum computer using the quantum Fourier transform, and is followed by classical post-processing to obtain the period.

Hallgren's algorithm, also known as the "irrational period-finding algorithm", builds on the period-finding step of Shor's algorithm, but instead of finding the period of a periodic function, it finds the irrational period of a certain non-periodic function. It uses the same basic structure of applying the quantum Fourier transform, with classical post-processing. However, the irrational

period-finding is a unique contribution, as no matter how much you apply Shor's algorithm to estimate an irrational period value with rational intervals, there are far too many rounding errors that occur when using that estimation in future calculations. Further sections elaborate on the details of Hallgren's algorithm, and how we plan to apply it to the billiard ball problem.

2.2 Geometry and Billiards

A crucial text for understanding the problem was the text *Geometry and Billiards* by Serge Tabachnikov. This book is meant for undergraduate and graduate students to use to explore mathematical billiards. Our focus was on understanding the concepts in Chapter 2, where the cutting sequence, billiard table and trajectory of the ball are introduced.

2.2.1 Billiard Table

The fundamental object we are working with is the unit square billiard table. Figure 1 is a drawing of the components of the unit billiard table. The billiard

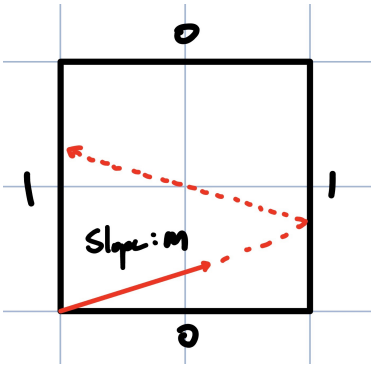

Figure 2: Unit square billiard table

table is friction-less, meaning that the billiard ball, once launched, will move around forever, continuously bouncing off walls. The slope m is the value of the slope of the ball's movement. Whenever the ball hits a vertical wall, we record a 1, and whenever it hits a horizontal wall, we record a 0. This sequence of 1s and 0s is known as the **cutting sequence**. We are interested in the slope value, m. While $m \in \mathbb{R}$ is a real number, we are interested when $m \in \mathbb{R} \setminus \mathbb{Q}$. This is because when $m \in \mathbb{Q}$, the ball will have a set pattern of movement that it will follow forever. It will have a cutting sequence that eventually repeats itself. However, when $m \in \mathbb{R} \setminus \mathbb{Q}$, the cutting sequence never repeats itself. The cutting sequence is an important representation within the billiard ball problem, and we will be exploring its properties often.

2.2.2 The expanded billiard table

To observe the movement of the billiard ball in a wider plane, we expand the billiard table to an infinite grid of unit squares. From this point on, any reference to billiard tables is strictly about the expanded billiard table model.

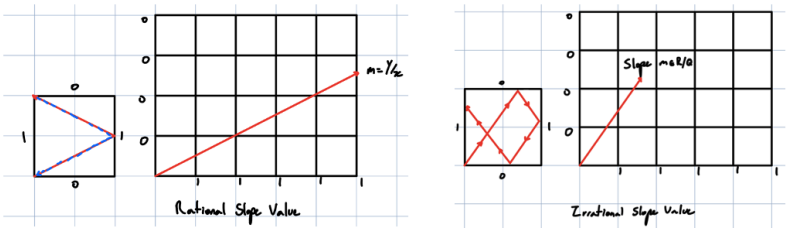

Figure 3: Expanded Billiard Table

Figure 2 provides a perspective on what an expanded billiard table looks like. Instead of visualizing the billiards' movements on a cramped 1×1 square, we can instead track its movements in a straight line over an infinite Cartesian grid. The grid can be discretely divided and indexed, similarly to the Cartesian coordinate system. The index of an individual table is determined by the coordinate of the bottom-left corner point. The origin, where the ball is launched, is at $(0, 0)$. As a billiard ball moves across the grid, it comes in contact with places where the original walls of the billiard table were. However, the direction of the movement of the ball is flipped around the x or y-axis, from the movement the ball would have made in the original table, depending on where on the coordinate system the billiard table is present in. Two neighboring squares share the same properties but are mirrored on the sides they share. The cutting sequence remains consistent with the single unit-square billiard table, where if the ball makes contact with a horizontal wall, a 0 is logged, and if the ball makes contact with a vertical wall, a 1 is logged. However, in the expanded table, the ball would go through the wall into the adjacent billiard table instead of bouncing back into the original table. The billiard thus follows a path that resembles a linear equation on an expanded billiard table that resembles the Cartesian coordinate system. From this point on, the text assumes the expanded billiard table is the default, and will refer to it as the billiard table.

2.3 Polynomial-time quantum algorithms for Pell's equation and the principal ideal problem

Much of the technical prior work is set up with Hallgren's paper [2] outlining his algorithm. This article provides a polynomial-time quantum algorithm for three problems from computational algebraic number theory, and we focus on

its solutions for Pell's equation. Hallgren's paper introduces the idea of *pseudo-periodicity*. Pseudo-periodic functions exhibit some of the characteristics of periodic functions, but have some irregularities or noise values that make it more loosely defined than strictly periodic. Both Shor's period-finding algorithm and Hallgren's irrational-period finding algorithm use the Fourier transform to compute the period of functions and construct rational approximations.

Hallgren's algorithm requires a pseudo-periodic function $f(x)$ as its input. Hallgren's algorithm broadly follows 3 steps for solving Pell's equation: i) Using Pell's equation, find some $f(x)$ that models the equation with coefficient d ii) Input into Hallgren's algorithm and run on a Quantum Computer iii) Produce a regulator R that can uniquely identify the least positive solution for d. We mirror this approach, with our main contribution identifying candidate functions $f(x)$ that produce a cutting sequence for the ball. Inputting this value to Hallgren's algorithm should provide us with a pseudo-period that we hope to use to find the slope value.

3 Technical Details

3.1 Cutting Sequences and their properties

In the right image in figure 3, the cutting sequence of the irrational slope m is $0101\cdots$. As the billiard ball continues to move, the cutting sequence grows in length.

3.1.1 The Golden Ratio

Tabachnikov suggests [8] an interesting irrational number value to explore is when $m = \phi$, also known as the Golden Ratio, $\phi = \frac{1+\sqrt{5}}{2}$. ϕ can also be expressed in continued fraction form,

$$\phi = 1 + \cfrac{1}{1 + \cfrac{1}{1 + \cfrac{1}{1 + \cdots}}}$$

The cutting sequence for when a ball is launched at slope $m = \phi$ is $w = \cdots 0100101001001\cdots$. An interesting observation made is that w is invariant over substitution $\sigma : 0 \mapsto 01,\ 1 \mapsto 0$. We explored this work and discovered this is true using linear algebra.

Proof. We define the trajectory of the ball to be

$$C = \left\{ y = \frac{2}{1+\sqrt{5}}x \right\} = \left\{ (x, \frac{2}{1+\sqrt{5}}x) \right\}$$

We must also introduce the grid that the trajectory is passing through:

$$G_{old} = \left\{ x \begin{bmatrix} 1 \\ 0 \end{bmatrix} + y \begin{bmatrix} 0 \\ 1 \end{bmatrix} | x \in \mathbb{Z}^+ \text{or } y \in \mathbb{Z}^+ \right\}$$

If $x \in \mathbb{Z}$ or $\frac{2}{1+\sqrt{5}}x \in \mathbb{Z}$ then we know that there is an intersection between the trajectory of the ball and the grid, so we must add another character to the cutting sequence. We define the set of points as P,

$$P = \left\{ \langle x, \frac{2}{1+\sqrt{5}}x \rangle \mid x \in \mathbb{Z}^+ \text{ or } \frac{2}{1+\sqrt{5}}x \in \mathbb{Z}^+ \right\}$$

where all $p \in P$ are intersections between the trajectory and the grid.

$P_{old} = P$ and $P_{new} = AP$ are the old and new cutting sequences of a ball moving at slope m. $C_{old} = C$ and $C_{new} = AC$ are the old and new trajectories of the ball.

Let matrix $A = \begin{bmatrix} 1 & 1 \\ 1 & 0 \end{bmatrix}$ and an eigenvector for A is $\vec{x} = \begin{bmatrix} \phi \\ 1 \end{bmatrix}$. A represents the linear transformation that the grid will make. Applying A to G_{old}, we get G_{new} where,

$$G_{new} = AG_{old} = \left\{ A \left(x \begin{bmatrix} 1 \\ 0 \end{bmatrix} + y \begin{bmatrix} 0 \\ 1 \end{bmatrix} \right) | x \in \mathbb{Z}^+ \text{or } y \in \mathbb{Z}^+ \right\}$$

The new trajectory becomes AC,

$$AC = \left\{ \begin{bmatrix} \phi x \\ x \end{bmatrix} \right\} = \left\{ \phi \begin{bmatrix} x \\ \phi^{-1}x \end{bmatrix} \right\}$$

Therefore, $AC = \{\phi y = x\} = \{y = \phi^{-1}x\} = C$, so the trajectory of the ball does not change as the linear transformation occurs.

Similarly, we must apply the linear transformation to all $p \in P$.

$$AP = \left\{ Ax \begin{bmatrix} x \\ \frac{2}{1+\sqrt{5}}x \end{bmatrix} | x \in \mathbb{Z}^+ \text{or } \frac{2}{1+\sqrt{5}}x \in \mathbb{Z}^+ \right\} = \left\{ \begin{bmatrix} \phi x \\ x \end{bmatrix} | x \in \mathbb{Z}^+ \text{or } \phi^{-1}x \in \mathbb{Z}^+ \right\}$$

We can observe that AP is just the points of P with a ϕ multiplied in front.

We must establish $C \cap G_{old} = P$ and $AC \cap G_{new} = AP$ to determine that there is no change of the cutting sequence between linear transformations A. To establish an intersection between G_{old} and C, the elements must satisfy conditionals of both sets.

Let $H_{old} = \{(x, y) | y \in \mathbb{Z}^+\}$ mapped to 1 and $V_{old} = \{(x, y) | x \in \mathbb{Z}^+\}$ mapped to 0 be the horizontal and vertical lines and $H_{old} \cup V_{old} = G_{old}$.

$$G_{old} \cap C = \left\{ x \begin{bmatrix} 1 \\ 0 \end{bmatrix} + y \begin{bmatrix} 0 \\ 1 \end{bmatrix} | x \in \mathbb{Z}^+ \text{ or } y \in \mathbb{Z}^+ \text{ and } y = \phi^{-1}x \right\}$$

$$\Leftrightarrow G_{old} \cap C = \left\{ x \begin{bmatrix} 1 \\ 0 \end{bmatrix} + \phi^{-1}x \begin{bmatrix} 0 \\ 1 \end{bmatrix} | x \in \mathbb{Z}^+ \text{ or } y \in \mathbb{Z}^+ \text{ and } y = \phi^{-1}x \right\}$$

$$= P$$

Similarly, we find an intersection $G_{new} \cap C = AP$.

$$G_{new} \cap C = \left\{ xA \begin{bmatrix} 1 \\ 0 \end{bmatrix} + yA \begin{bmatrix} 0 \\ 1 \end{bmatrix} | x \in \mathbb{Z}^+ \text{ or } y \in \mathbb{Z}^+ \text{and} y = \phi^{-1}x \right\}$$

$$= \left\{ \begin{bmatrix} x + \phi^{-1}x \\ x \end{bmatrix} | x \in \mathbb{Z}^+ \text{ or } \phi^{-1}x \in \mathbb{Z}^+ \text{ and } y = \phi^{-1}x \right\}$$

$$= AP$$

Using the above definitions, we make the following claims:

1. Every $0 \in P_{new}$ corresponds to $1 \in P_{old}$
2. Every $0 \in P_{new}$ corresponds to a $0 \in P_{old}$ to its left of distance less than 1 unit.
3. Every $1 \in P_{new}$ corresponds to $0 \in P_{old}$ to its left of distance less than 1 unit.

Let $H_{new} = A \cdot V_{old} = \{(x, y) | y \in \mathbb{Z}^+\}$ map to 0 and $V_{new} = A \cdot H_{old} = \{(x, y) | x - y \in \mathbb{Z}^+\}$ map to 1. Using these definitions, we will prove the above statements in the next sections.

Proof of Claim 1. We want to prove that every $0 \in P_{new}$ corresponds to $1 \in P_{old}$. $0 \in P_{new}$ means that there exists some point $(x, y) \in C_{new} \cap H_{new}$, which implies $(x, y) \in C_{new}$ s.t. $x \in \mathbb{R}^+$, $y \in \mathbb{Z}^+$. Since $C_{new} = C_{old}$, $(x, y) \in C_{old}, x \in \mathbb{R}^+, y \in \mathbb{Z}^+$, which implies $(x, y) \in H_{old} \cap C_{old}$ which implies $1 \in P_{old}$. □

Proof of Claim 2. We want to prove that every $0 \in P_{new}$ corresponds to a 0 to the left of distance less than 1 unit. By way of contradiction, assume that the next point in P_{old} to the left is in H_{old}, so that there exists point $(x', y') \in P_{old}$ s.t. $y' \in \mathbb{Z}^+$ and $x > x' > x - 1$. Since we know $y = \phi^{-1}x$ and $y' = \phi^{-1}x'$, we know $y = \phi^{-1}x > \phi^{-1}x' = y'$. Because $(x, y) \in H_{new}$, so $y \in \mathbb{Z}$, $y - 1 \geq y'$

$$\text{implies } \frac{y}{\phi^{-1}} - \frac{1}{\phi^{-1}} \geq \frac{y'}{\phi^{-1}}$$

$$\text{implies } x - \frac{1}{\phi^{-1}} \geq x' > x - 1$$

$$\text{implies } 1 > \phi$$

Hence, there is a contradiction. Therefore, every $0 \in P_{new}$ corresponds to a 0 to the left of distance less than 1 unit. □

Proof of Claim 3. We want to prove that every $1 \in P_{new}$ corresponds to $0 \in P_{old}$ to its left of distance less than 1 unit. With the assumption that the next point in P_{old} to the left is in H_{old}, si that there exists point $(x', y') \in P_{old}$ s.t. $y' \in \mathbb{Z}^+$ and $x > x' > \lfloor x \rfloor$. We know that $y = \phi^{-1}x$ and $y' = \phi^{-1}x'$. From the definition in V_{new}, $x - y \in \mathbb{Z}^+$, $\lfloor x \rfloor - y' \in \mathbb{Z}^+$.

$$x - \lfloor x \rfloor < 1$$

$$y' - y = \phi^{-1}(x' - x) < 0$$

$$x - \lfloor x \rfloor + y' - y < 1$$
$$x(1 - \phi^{-1}) + \phi^{-1}x - \lfloor x \rfloor < 1$$
$$x(1 - \phi^{-1}) + \phi^{-1}x - x' < x(1 - \phi^{-1}) + \phi^{-1}x - \lfloor x \rfloor$$
$$0 < (1 - \phi^{-1})x - (1 - \phi^{-1})x'$$
$$0 < x - \lfloor x \rfloor + y' - y < 1$$

This is a contradiction, as an integer does not exist between 0 and 1. □

□

3.2 Fibonacci

Recall σ is the operation that takes in strings to do the following substitution: $\sigma : 0 \mapsto 01,\ 1 \mapsto 0$ on the cutting sequence w In the text *Geometry and Billiards* by Serge Tabachnikov, it outlines an exercise for the reader to prove that starting with the string 0, if σ gets repeatedly applied, the string lengths of each iteration follow the Fibonacci sequence. The following is an inductive proof for the exercise. We will work with the Fibonacci sequence such that $F_1 = 1$ and $F_2 = 2$.

Theorem 1. Let $w_n = \sigma^n(0)$. The lengths of w_n are the Fibonacci numbers.

Proof. Base case ($n = 1$)
With the string $w_1 = 0$ since this has length 1, we know this is the first Fibonacci sequence number. Therefore, the base case $n = 1$ is true.

Base case ($n = 2$)
Let us start with the string:

$$w_1 \mapsto 0$$

w_1 has length 1.

$$\text{therefore } |w_1| = f_1 = 1$$

To get w_2, we need to apply σ to string w_1. Applying σ to w_1,

$$\sigma(w_1) = 01$$

This new string is w_2, where

$$w_2 = 01$$

The length of this string is 2, since Therefore,

$$|w_2| = f_2 = 2$$

Therefore, this satisfies the second number of the Fibonacci sequence. Therefore, the base case $n = 2$ is true.

Inductive Step: Assume $n = k, n = k-1$ holds. For the case where $n = k-1$, let us assume that the symbol w_{k-1} is the case where σ has been applied $k-1$ times.

$$w_{k-1} = \sigma_{k-1}(0)$$

Given this, the magnitude of w_{k-1} can be computed as the Fibonacci number f_{k-1}.

$$|w_{k-1}| = f_{k-1}$$

Let us also assume the same about the case where $n = k$

$$w_k = \sigma_k(0)$$

$$|w_k| = f_k$$

For case $(n = k + 1)$

$$w_{k+1} = \sigma_{k+1}(0)$$

$$\sigma_{k+1}(0) = \sigma(\sigma_k(0))$$

Because all characters in $\sigma_k(0)$ are converted to 0 when σ is applied, $\sigma_{k+1}(0)$ has $|\sigma_k(0)|$ 0 characters in it.

Because all 0 characters in $\sigma_k(0)$ have an extra 1 attached, and the number of 0s in $\sigma_k(0)$ is equal to $|w_{k-1}|$. Therefore, $\sigma_{k+1}(0)$ has $|\sigma_{k-1}(0)|$ 1 characters in it.

Therefore, the number of characters in $\sigma_{k+1}(0)$ becomes $|\sigma_{k-1}(0)|+|\sigma_k(0)| = |w_{k-1}| + |w_k| = |w_{k+1}| = |\sigma_{k+1}(0)|$ □

3.3 Properties of cutting sequences where slope $m < 1$

A characteristic we have uncovered about cutting sequences is the combination of intervals between 0 characters. Conceptually, if a line is more perpendicular to the x-axis than the y-axis, it will intersect with more horizontal walls than vertical walls. On the other hand, if it is more perpendicular to the y-axis than the x-axis, it will intersect more with horizontal walls than vertical walls. We study this by observing different *runs* of a cutting sequence. The nth run is defined as the sequence of 1s that come between the nth and the $n + 1$th 0s in the cutting sequence.

Theorem 2. If slope $m < 1$, then the cutting sequence can only have one 0 in a row.

Proof. We use a proof by contradiction. Assume it is possible to have two 0s in a row in the cutting sequence when $m < 1$. For any cutting sequence to have two 0 characters in a row, it must go through the two horizontal lines that form the top and bottom of the table. Let the point of intersection between the trajectory and the bottom of the table be $P_1 = (a_1, b_1)$ and the top be $P_2 = (a_2, b_2)$, as seen in figure 4. For two 0s to happen sequentially, $a_2 - a_1 < 1$ and $b_2 - b_1 \geq 1$. Subsequently, $\frac{b_2-b_1}{a_2-a_1} > 1$. However, this contradicts our original

statement that two 0s can occur in a row when $m < 1$. Therefore, this proves that if $m < 1$, then the cutting sequence can only have one 0. □

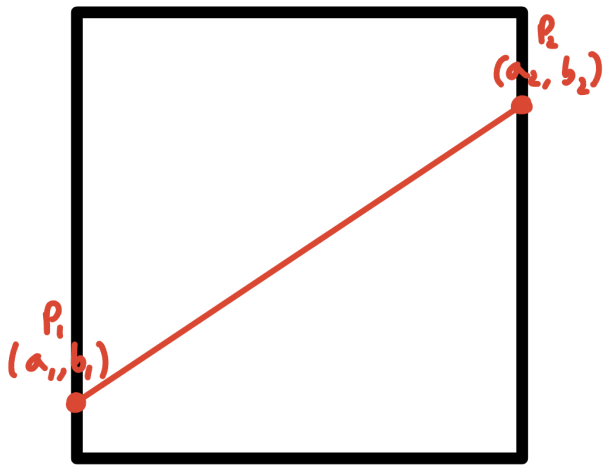

Figure 4: Example of when '0' is recorded in the sequence

A follow up question is: How are subsequent runs between 0s determined? That is, given some sequence w, what makes the subsequent number of characters, denoted by the integer l, 1's? In figure 5, the first run between zeroes would be the 111 value before the red bar, and the second run would be the 111 before hitting another 0 after the red bar.

3.3.1 The first run

The first run denotes the first continuous sequence of 1s that occur between the starting point $(0, 0)$ and the first time the sequence cuts through a horizontal wall, denoted by $(1, m)$. The number of 1s in the first run is determined by $\lfloor \frac{1}{m} \rfloor$, since $\frac{1}{m} = \dfrac{1}{\frac{y}{x}} = \frac{x}{y}$. Since the number of columns intersected is discrete, we must apply the floor function to the value.

3.3.2 Subsequent runs

The number of 1s in the second run is more complicated. As seen in figure 1, there is a small amount of displacement in the x-axis visible, that the second run must start with. We will call this extra displacement C. We express the

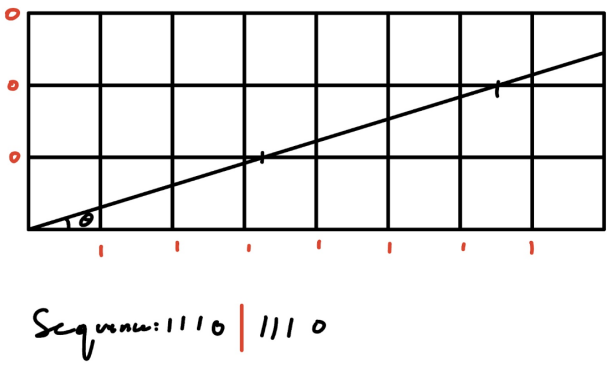

Figure 5: The Cutting Sequence

ball's displacement with $\frac{1}{m} = \lfloor \frac{1}{m} \rfloor + C$. C is the extra displacement that the 3rd run will start with. Subsequent runs use a similar process, where extra displacement continues to increase until $C \geq 1$ at some nth run. Then, the nth run will encounter an extra 1, and C has a 1 subtracted from it to account for the extra 1 in the run, is the excess displacement for runs beyond n.

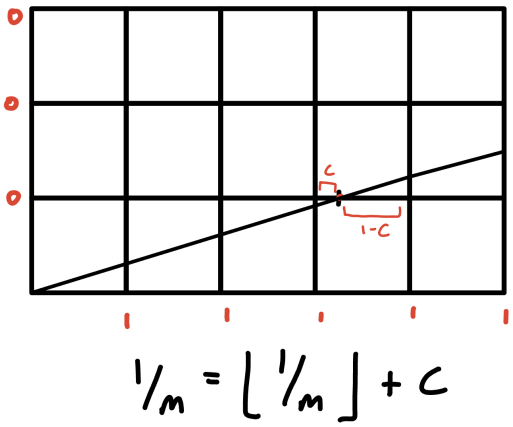

Figure 6: Extra Displacement

Figure 6 demonstrates a close-up visualization of the extra displacement from the first run.

Theorem 3. For the nth run of a sequence w, if the starting slope $m < 1$, there are $\lfloor \frac{n}{m} \rfloor - \lfloor \frac{n-1}{m} \rfloor$ number of 1 characters in that run.

Proof. Let l be the number of 0s encountered. hence the number of runs that

has happened so far. l and n are equal values. m is the slope value, and some y coordinate, the corresponding $\lfloor x \rfloor$ provides the number of 1s encountered so far. Thus, since n is a y coordinate value, $\lfloor \frac{n}{m} \rfloor$ is the number of 1s drawn in the entire sequence so far. The number of 1s encountered up to the $n-1$th run is $\lfloor \frac{n-1}{m} \rfloor$. Subtracting $\lfloor \frac{n}{m} \rfloor - \lfloor \frac{n-1}{m} \rfloor$ gives us the number of 1s between the nth 0 and the $n-1$th 0. □

4 Applying Hallgren's to Pell's

Pell's equation has interesting connections to old problems such as the Cattle Problem. However, there are many contemporary problems that are related to Pell's equation as well as how to solve it. Hallgren [2] discusses several problems related to Pells' equation. The principal ideal problem reduces to Pell's equation, which reduces to the problem of factoring. All these problems are special cases of the Hidden Subgroup Problem, along with other problems such as the Discrete Log Problem, and the unsolved Graph Isomorphism problem. There are several algorithms that use Fourier Sampling as a core concept, including Hallgren's and Shor's algorithm. Hallgren's paper introduces several algorithms that solves the Principal Ideal Problem and generates solutions to Pell's equation. Shor's algorithm solves factoring and the Discrete Log Problem. These concepts can be used for solving several different cryptography schemes. Solving factoring breaks RSA, while solving the discrete log problem solves Diffie-Hellman, both of which are solved by Shor's algorithm. Buchmann-Williams is solved by cracking the Principal Ideal Problem, which is solved by Hallgren's algorithm.

4.1 Pell's equation

Pell's equation is the following. Given a non-square integer d, the Diophantine equation

$$x^2 - dy^2 = 1$$

is known as Pell's equation.

For every value of d, we must find the least positive solution for x and y, noted by x_0, y_0 values. This is a deceptively difficult problem. At first glance from table 1, for small values of d, least positive solutions can be found with some trial and error. However, as the value of d increases, x_0, y_0 can jump erratically and it is impossible to find any correlation between d_n and d_{n-1}.

4.2 Applying Pell's to Archimedes' Cattle Problem

Archimedes' cattle problem is a famous mathematical problem attributed to the ancient Greek mathematician Archimedes. It asks for the number of white, black, dappled and brown bulls and cows that beloing to the Sun God, Helios, given several mathematical restrictions. We list the conditions of the problem, adapted from *Solving the Pell Equation* [5]:

d	x	y	$x^2 - dy^2$
2	3	2	1
3	2	1	1
5	9	4	1
6	5	2	1
7	8	3	1
8	3	1	1
10	19	6	1
11	10	3	1
12	7	2	1
13	649	180	1
14	15	4	1
15	4	1	1
$\vdots$	$\vdots$	$\vdots$	$\vdots$

Table 1: Least positive solutions to Pell's equation up to $d = 15$

1. Let x, y, z, t represent the white, black, brown, dappled and brown bulls, the following are the restrictions on the number of animals.

$$x = \left(\frac{1}{2} + \frac{1}{3}\right) y + t,$$

$$y = \left(\frac{1}{4} + \frac{1}{5}\right) z + t,$$

$$z = \left(\frac{1}{6} + \frac{1}{7}\right) x + t$$

2. There are also restrictions on the number of cows. They are the same colors as the bulls, but their variables are denoted with primes to represent cows.

$$x' = \left(\frac{1}{3} + \frac{1}{4}\right) (y + y')$$

$$z' = \left(\frac{1}{5} + \frac{1}{6}\right) (t + t')$$

$$y' = \left(\frac{1}{4} + \frac{1}{5}\right) (z + z')$$

$$t' = \left(\frac{1}{6} + \frac{1}{7}\right) (x + x')$$

3. The final conditions are that $x + y$ must be a square and $z + t$ must be triangular.

The general solution for the first three equations are $(x, y, z, t) = m(2226, 1602, 1580, 891)$, where m is a positive integer. The general solution for the second set of equations requires that $m = 4657k$, and $(x', y', z', t') = k \cdot (7206360, 4893246, 3515820, 5439213)$. We must now select a k such that $x + y = 4657 \cdot 3828 \cdot k$ is a square and $z + t = 4657 \cdot 2471 \cdot k$ is triangular. By examining the prime factorization of $4657 \cdot 3828 = 2^2 \cdot 3 \cdot 11 \cdot 29 \cdot 4657$, it is evident that the first condition is equivalent to $k = al^2$, where $a = 3 \cdot 11 \cdot 29 \cdot 4657$ and l is an integer.

We will prove that $z + t$ is a triangular number if and only if $8(z + t) + 1$ is a square. Let's consider the equation $8(z+t)+1 = h^2$, where $z+t$ is a positive integer. If we rearrange the equation, we get $8(z + t) = h^2 - 1$. Notice that $h^2 - 1$ is a difference of squares, which can be factored as $(h + 1)(h - 1)$. So the equation can be rewritten as $8(z + t) = (h + 1)(h - 1)$. Since $z + t$ is a positive integer, $8(z + t)$ must be divisible by 8. This means that both $(h + 1)$ and $(h - 1)$ must be even, or in other words, h must be an odd integer. Let's represent h as $h = 2n + 1$, where n is a non-negative integer.

Substituting $h = 2n+1$ back into the equation $8(z+t) = (h+1)(h-1)$, we get $8(z+t) = (2n+2)(2n)$. Dividing both sides by 8, we obtain $(z+t) = n(n+1)/2$, which is the equation for a triangular number.

Assume that $z + t$ is a triangular number, i.e., $z + t = \frac{n(n+1)}{2}$ for some positive integer n. We want to show that $8(z + t) + 1$ is a perfect square, i.e., $8(z+t)+1 = m^2$ for some integer m. Substituting $z+t = \frac{n(n+1)}{2}$ into equation $8(z + t) + 1$, we get $8\left(\frac{n(n+1)}{2}\right) + 1$. Simplifying, we have $4n(n + 1) + 1$. Notice that the left-hand side of the equation is of the form $4n(n + 1) + 1$, which can be rewritten as $(2n+1)^2$. Taking the square root, we get $2n+1$. Since $2n+1$ is an odd integer, we can let $m = 2n + 1$, such that $8(z + t) + 1 = m^2$ is satisfied. Therefore, we have shown that if $z+t$ is a triangular number, then $8(z+t)+1$ is a perfect square, completing the proof in the other direction. Therefore, we can conclude that $z + t$ is a triangular number if and only if $8(z + t) + 1$ is a square, where $z + t$ is a positive integer.

Therefore, we can rewrite the equation as $h^2 = 8(z + t) + 1 = 8 \cdot 4657 \cdot 2471 \cdot al^2 + 1$, which is equivalent to the Pell's equation $x^2 - dy^2 = 1$ for $d = 2 \cdot 3 \cdot 7 \cdot 11 \cdot 29 \cdot 353 \cdot (2 \cdot 4657)^2 = 410,286,423,278,424$.

4.3 Pseudo-periodicity

Hallgren's algorithm requires as input a function $f(x)$ that is pseudo-periodic. The definition of pseudo-periodicity is as follows:

Definition 1. A function $f : \mathbb{Z} \mapsto X$, where X is any set, is called *pseudo-periodic with period S, at offset k* if for each i either $f(k) = f(k + \lfloor iS \rfloor)$ or $f(k) = f(k + \lceil iS \rceil)$, where $S \in \mathbb{R}$.

We have found an example of a pseudo-periodic function. Let $S = 200\pi$, $k = 0$, $f(x) = \lceil \frac{1000 \sin(\frac{x}{N} + \frac{\pi}{2})}{100} \rfloor$. Using the function parameters, $f(k) = 10$. We will prove that this function satisfies the definition of pseudo-periodic, such that for all i, $f(x) = f(\lfloor 200\pi i \rfloor)$ or $f(x) = f(\lceil 200\pi i \rceil)$.

We use algebra to reduce the above equality:

$$0.9995 < \sin\left(\frac{\lfloor 200\pi i \rfloor}{100} + \frac{\pi}{2}\right) < 1.0005 \text{ or } 0.9995 < \sin\left(\frac{\lceil 200\pi i \rceil}{100} + \frac{\pi}{2}\right) < 1.0005$$

The square brackets [and] are used when we want to denote either the floor or ceiling function. To remove the ceiling and floor functions, we established an inequality that looks like the following:

$$0.9995 < \sin\left(\frac{[200\pi i]}{100} + \frac{\pi}{2}\right) < 1.0005$$

We want to prove for all i, there exists n, y in $\mathbb{Z}$ such that the following holds:

$$(-3.16\ldots + 200\pi n < y < 3.16\ldots + 200\pi n) \text{ and } (200\pi i - 1 < y < 200\pi i + 1)$$

Let $y = \lfloor 200\pi i \rfloor$ or $\lceil 200\pi i \rfloor$ and let $n = i$. Then if we plug those values into the equality that we want to prove, we get

$$-3.16\ldots + 200\pi i < 200\pi i - 1 < y < 200\pi i + 1 < 3.16\ldots + 200\pi i$$

Since for all i, there exists an n and y such that the equality statement holds, we know that the function f is pseudo-periodic with period $200 * \pi$ and with offset equal to 0.

4.4 How does Hallgren's algorithm work on Pell's equation?

Hallgren's algorithm solves Pell's equation in polynomial time. [2]

1. A function $f(x)$ is outlined in Hallgren [2] in Definition 2.2 that can be input into Hallgren's algorithm.
2. Hallgren's algorithm takes in $f(x)$ to find the regulator value, which is the pseudo-period of $f(x)$.
3. Using the regulator, calculate the least positive solution to Pell's equation for some positive non-square integer d.

Following this framework, we have devised a similar plan of approaching the billiard ball problem:

1. We must find some $f(x)$ that describes the cutting sequence.
2. Input this function into Hallgren's algorithm and produce a pseudo-period.
3. Use the pseudo-period to find the irrational slope value for billiard ball launch.

The function $f(x)$ is what we are interested in the most, and we introduce one in section 5. In the literature review found in section 1.3 of Hallgren's paper *Polynomial-time quantum algorithms for Pell's equation and the principal ideal problem*, we outlined the need for $f(x)$, the input to Hallgren's algorithm to be pseudo-periodic.

4.5 The regulator

The logarithm, $R = \ln x_1 + \sqrt{d}y_1$ is called the *regulator*. $R \in \mathbb{R}/\mathbb{Q}$ can be used to uniquely identify the solution (x_0, y_0) [9]. Since $R = \ln(x_0 + \sqrt{d}y_0)$, we can remove the natural log and raise both sides to the natural number e, s.t. $e^R = x_0 + \sqrt{d}y_0$

Quadratic irrationals are numbers like the regulator that are irrational (i.e., not expressible as a ratio of two integers) and are the roots of quadratic equations with integer coefficients. In other words, they are solutions to quadratic equations of the form $ax^2 + bx + c = 0$, where a, b, and c are integers, and x is the unknown variable.

We define Simple Continued Fractions as the following:

Definition 2. A Simple Continued Fraction is an expression of the form

$$a_1 + \frac{1}{a_2 + \frac{1}{a_3 + \ldots}}$$

where the a_i are a possibly infinite sequence of integers such that a_1 is non-negative and the rest of the sequence is positive.

Theorem 4. [[6, Theorem 7.19]] Any periodic Simple Continued Fraction is a quadratic irrational number, and conversely.

Hallgren's algorithm returns a regulator R, which is an irrational number [2]. This number can be rewritten into a continued fraction form. Using Theorem 4, we know this is a periodic Simple Continued Fraction, which we can use to then create a closed form fraction, which we prove in Lemma 1. The expression can be infinite, in which case the continued fraction represents an irrational number. If the expression terminates, then the continued fraction represents a rational number.

4.6 Continued fractions and the Golden Ratio

To apply and explore the idea of continued fractions, we are going to look again at the Golden Ratio. We remind the reader that $\phi = \frac{1+\sqrt{5}}{2} = 1.618\ldots$. $\frac{1+\sqrt{5}}{2}$ is a solution to the equation $\phi^2 - \phi - 1 = 0$. We can rewrite the equation to

$$\phi^2 = \phi + 1$$

Dividing both sides by ϕ, we get the value

$$\phi = 1 + \frac{1}{\phi}$$

We can replace ϕ of the denominator of the equation with the right hand side.

$$\phi = 1 + \frac{1}{1 + \frac{1}{1 + \phi}}$$

ϕ can be replaced infinitely many times by the fraction $\frac{1}{1+\phi}$ to construct a beautiful continued fraction.

$$\phi = 1 + \cfrac{1}{1 + \cfrac{1}{1 + \cfrac{1}{1 + \cfrac{1}{1 + \cdots}}}}$$

It is important to notice we can also reverse this process for all numbers represented by Simple Continued Fractions. Here, we can take the infinite continued fraction form of ϕ back to a terminating, finite form and create a quadratic equation. This technique works for all irrational numbers, as they can also be converted into Simple Continued Fractions based off theorem 4 We will use this technique in Section 4.7 to compute the regulator and eventually find the least positive solution to Pell's equation when $d = 5$.

Lemma 1. *The infinite continued fraction form of a Simple Continued Fraction for a quadratic irrational can be used to produce a quadratic equation.*

Proof. Given some infinite continued fraction form for a quadratic irrational α, we know that from Theorem 4 that the Simple Continued Fraction expansion is ultimately periodic. We can represent the periodic portion of the SCF using θ, where $\theta =< \overline{a_0, a_1 \cdots a_n} >$, where n represents the number of values in the period, to represent the purely periodic part of the SCF. The integers $a_0, a_1 \cdots$ are the coefficients of the continued fraction, and they are listed between angle brackets to indicate the recursive structure of the fraction. The vinculum represents the repeating part of the continued fraction. Using this, we rewrite the infinite continued fraction with θ, to produce a terminating fraction.

$$\alpha = a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \cfrac{1}{a_3 + \cfrac{1}{a_4 + \cdots}}}}$$

We can replace the periodic portion of α to create a terminating continued fraction.

$$\alpha = a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \cfrac{1}{a_3 + \cfrac{1}{a_4 + \cfrac{\cdots}{\cfrac{1}{a_{b_1-1} + \theta}}}}}}$$

We can isolate θ in the form :

$$\theta = a_{b_1} + \cfrac{1}{a_{b_2} + \cfrac{1}{\cdots + \cfrac{1}{a_{b_n} + \cfrac{1}{\theta}}}}$$

We can use a proof by induction to rewrite θ to equal $\frac{k_1\theta+c}{k_2\theta+d}$ We start with the base case, to rewrite $\cfrac{1}{a_{b_n} + \cfrac{1}{\theta}}$ to the form $\frac{k_{n-1}\theta+c}{k_n\theta+d}$, where $k_{n-(k+1)}, k_{n-k}, c, d \in \mathbb{Z}$.
We can get the following:

$$\frac{1}{a_{b_n} + \cfrac{1}{\theta}} \cdot \frac{\theta}{\theta} = \frac{\theta}{\theta a_{b_n} + 1}$$

Since the base case satisfies the fractional form, the base case is true. We take an inductive step to assume the kth step is true:

$$\cfrac{1}{a_{b_{n-k}} + \cdots \cfrac{1}{a_{b_{n-1}} + \cfrac{1}{a_{b_n} + \frac{1}{\theta}}}} = \frac{k_{n-(k+1)}\theta + c}{k_{n-k}\theta + d}$$

Assuming the above is true, we want to prove that for the $k+1$th case,

$$\cfrac{1}{a_{b_{n-(k+1)}} + \cdots \cfrac{1}{a_{b_{n-1}} + \cfrac{1}{a_{b_n} + \frac{1}{\theta}}}} = \frac{k_{n-(k+2)}\theta + c}{k_{n-(k+1)}\theta + d}$$

Using the inductive step, we can rewrite the continued fraction in the following way

$$\begin{aligned}\cfrac{1}{a_{b_{n-(k+1)}} + \cdots \cfrac{1}{a_{b_{n-1}} + \cfrac{1}{a_{b_n} + \frac{1}{\theta}}}} &= \cfrac{1}{a_{b_{n-(k+1)}} + \cfrac{k_{n-(k+1)}\theta + c}{k_{n-k}\theta + d}} \\ &= \frac{k_{n-k}\theta + d}{(a_{b_{n-(k+1)}}k_{n-k} + k_{n-(k+1)})\theta + c + da_{b_{n-(k+1)}}}\end{aligned}$$

which satisfies the form we want. Assuming the kth step is true, we have proven the $(k+1)$th step is also true. Since we have proven the base case, an infinite periodic continued fraction can be rewritten to a finite fraction form.

Using the equality $\theta = \frac{k_1\theta+c}{k_2\theta+d}$, we can rewrite it into a quadratic equation $k_2\theta^2 + (d-k_1)\theta - c = 0$.

□

4.7 Example: $d = 5$

Let us do an example where $d = 5$. Given this information, we can assume Hallgren returns a regulator R value. In the case where $d = 5$, $R = 2.887\ldots$. To isolate $x_0 + \sqrt{d}y_0$, we can raise e^R such that $x_0 + \sqrt{d}y_0 = 17.944\ldots$. Using the continued fractions idea from subsection 4.6, we can convert this infinite decimal into a closed fraction form.

Let $\epsilon = 17.944\ldots$.

$$\epsilon = 17 + 0.944\ldots = 17 + \cfrac{1}{\cfrac{1}{0.944\cdots}}$$

$$= 17 + \frac{1}{1.059\cdots} = 17 + \cfrac{1}{1 + \cfrac{1}{\cfrac{1}{.059\cdots}}}$$

$$= 17 + \cfrac{1}{1 + \cfrac{1}{16 + 0.949\cdots}}$$

$$= 17 + \cfrac{1}{1 + \cfrac{1}{16 + \cfrac{1}{\cfrac{1}{0.949\cdots}}}}$$

$$= 17 + \cfrac{1}{1 + \cfrac{1}{16 + \cfrac{1}{1 + .053\cdots}}}.$$

At this point, there is a clear pattern visible with a repetition of the fraction $\cfrac{1}{16 + \cfrac{1}{\cdots}}$. To summarize what we have so far,

$$\epsilon = 1 + 16 + \cfrac{1}{1 + \cfrac{1}{16 + \cfrac{1}{1 + \cdots}}}.$$

We can subtract a 1 from both sides. Furthermore, since this is an infinite fraction, we can replace the denominator of the second continued fraction with $\epsilon - 1$, such that

$$\epsilon - 1 = 16 + \cfrac{1}{1 + \cfrac{1}{\epsilon - 1}}.$$

Skipping the algebra to isolate the ϵ value to the left hand side, we a quadratic equation that $\epsilon^2 - 18\epsilon + 1 = 0$. Using the quadratic equation, we can compute that $\epsilon = 9 \pm 4\sqrt{5}$. Thus, knowing the least positive solution pair for Pell's is produced in the form $x_0 \pm d\sqrt{y_0}$ we can isolate $x_0 = 9$ and $y_0 = 4$, which is indeed the least positive solution pair for $d = 5$.

4.8 Summary

Using Hallgren's algorithm to solve Pell's is a parallel to using Hallgren's algorithm to solve the billiard ball problem. Hallgren takes in function $f(x)$ for Pell's equation, and produces the regulator value R to find a least positive solution for some d. Using this similar idea, we hope to find some function $f(x)$ that generates the cutting sequence for some irrational slope in the billiard ball problem. We can similarly input this value into Hallgren's algorithm to produce a pseudo-period value that can be used to evaluate the irrational slope value for the launch of the billiard ball.

5 Conjectured function

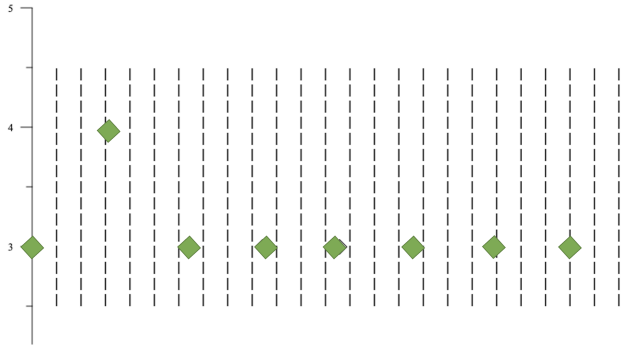

Figure 7: Pseudo-period is too small

Our conjectured function is

$$f(n) = \lfloor \frac{n}{m} \rfloor - \lfloor \frac{n-1}{m} \rfloor$$

We believe this to be a good candidate for determining the runs of a sequence of numbers as explored in section 3.3, as it can be used to determine the string of 1s between the nth 0 and the $n+1$th 0 of the cutting sequence. We believe the function may be pseudo-periodic, where $f(k) = f(k+\lfloor iS \rfloor)$ or $f(k) = f(k+\lceil iS \rceil)$ due to the mostly repetitive nature of the cutting sequence. Despite adding any multiple i of S, where $S = \lfloor iS \rfloor$ or $S = \lceil iS \rceil$, as the slope does not change with

displacement, the number of 1s in the string between 0s can only vary by ± 1. We must find a period S that the definition of pseudo-periodicity for $f(x)$. $f(x)$ makes it a good candidate for pseudo-periodicity as the slope of the trajectory of the ball does not change regardless of the change in n that is input into the function. We believe a good pseudo-period to explore would be $\frac{22}{\pi}$, as every $\frac{22}{\pi}$ runs, there is an extra 1 found in that run in the cutting sequence.

A potential proof would follow the structure of the proof found in section 4.3. Selecting some values for some offset n, for period S, we would use function $f(n)$ and input these values into the function to see if for all values of i, if it satisfies $f(n) = f(n + \lfloor iS \rfloor)$ or $f(n) = f(n + \lceil iS \rceil)$. We can establish inequalities to remove the floor and ceiling values, before rearranging the inequality for some multiple of i that satisfies the inequalities, demonstrating pseudo-periodicity.

However, $f(n)$ requires further refinement. As diagram 7 shows, the green diamonds are the number of 1s, with the index of the diamond (with indexing starting at 0 at the y-axis) corresponding to the index of the run. The vertical bars indicate the potential pseudo-period values that $f(n)$ returns. To prove pseudo-periodicity, the lines must be close to the diamonds, with spacing between lines and diamonds being roughly equivalent. However, in this case, pseudo-periodicity is not meaningful as there are far too many lines between diamonds, meaning that whether iS is rounded up or down, there will always be a value that satisfies the definition of pseudo-periodic.

6 Conclusion

In this thesis, we studied the properties of cutting sequences of a billiard ball that travels on an expanded billiard table. We contribute a literature review that studies prior work on similar problems. In addition to Pell's equation, the paper also introduces Archimedes' Cattle Problem, which ties together the concept of Pell's equation to an interesting problem. The paper then provides a step by step proof of the cattle problem and finding that $d = 410,286,423,278,424$, to provide motivation for solving the problem of finding the irrational slope value of a billiard ball launched using quantum computing.

We provide examples for definitions of the regulator R and pseudo-periodicity, as these are key concepts for understanding the outputs of the algorithm to eventually find the irrational slope value m. The regulator is the output from Hallgren's algorithm, and we can use non-quantum post-processing techniques to solve Pell's equation for some coefficient d. We use the example $d = 5$ to find the regulator value, and use continued fractions to convert the infinite quadratic irrational into a closed form quadratic equation. We have also proven that the function $f(x) = 10 \sin \frac{x}{N} + \frac{\pi}{2}$ satisfies the definition of pseudo-periodicity. Using these definitions, we draw parallels between how Hallgren solves Pell's equation to how we can solve the billiard ball problem can be solved. If a function $f(x)$ can be defined, it can be input into Hallgren's algorithm.

We provided an example of a cutting sequence where the slope $m = \phi$. Using linear algebra, we substituted σ, where $0 \to 01$ and $1 \to 0$. We observed that

this substitution does not change the characters in m's cutting sequence. We also learned about the properties of runs when $m < 1$. Studying the properties of the cutting sequence helps us find a generalized $f(x)$ that generates cutting sequences. We studied the properties of the first and second runs, with the properties of the second run generalizing to all subsequent runs. We used what we explored here to come up with a candidate $f(x)$ to input into Hallgren's algorithm, and outlined a proof so that it can be used to produce a pseudo-period value to find the irrational slope value for the launch of a mathematical billiard ball. We have conjectured that the function $f(n) = \lfloor \frac{n}{m} \rfloor - \lfloor \frac{n-1}{m} \rfloor$ satisfies the definition of pseudo-periodicity in our work. This is an important property to satisfy, as functions input into Hallgren's algorithm must be pseudo-periodic. We outline a potential proof, along with some interesting caveats as to why this function needs further refining to satisfy pseudo-periodicity.

Further work must be done to verify $f(n)$ to be pseudo-periodic. This thesis has explored prior work that that is accessible at the undergraduate level to continue this line of research. Future work could also involve simulating the function and simulating Hallgren's algorithm on a classical computer, or runnning it on a quantum computer to determine the output of the function.

References

[1] Johannes Buchmann and Hugh C. Williams. "A key-exchange system based on imaginary quadratic fields". In: *Journal of Cryptology* (1988), pp. 107–118.

[2] Sean Hallgren. "Polynomial-time quantum algorithms for Pell's equation and the principal ideal problem". In: *Journal of the ACM (JACM)* 54.1 (2007), pp. 1–19.

[3] Anatole B Katok. "Billiard table as a playground for a mathematician". In: *Surveys in modern mathematics*. Vol. 321. London Mathematical Society Lecture Note Series. 2005, pp. 216–242.

[4] Victor J. Katz. *A History of Mathematics*. Addison-Wesley, 1998, pp. 247–250.

[5] Hendrik W Lenstra Jr. "Solving the Pell equation". In: (2002), pp. 182–192.

[6] Ivan Niven, Herbert S Zuckerman, and Hugh L Montgomery. *An introduction to the theory of numbers*. John Wiley & Sons, 1991.

[7] John Stillwell. *The Pell equation*. Springer New York, 2003.

[8] Serge Tabachnikov. *Geometry and billiards*. American Mathematical Soc., 2005.

[9] Colin P Williams, Scott H Clearwater, et al. *Explorations in quantum computing*. Springer, 2011.