McGill Undergraduate Mathematics Journal

the δelta εpsilon

Fall 2012
Sixth Issue

THE δELTA-εPSILON

MCGILL UNDERGRADUATE MATHEMATICS JOURNAL

CONTENTS

A Geometric Interpretation of the Uniformly Minimum-Variance Unbiased Estimator (UMVUE) with the Use of Hilbert Spaces **3**
Jean-Philippe Fortin

Which Propeller Graphs Are The Underlying Graph of a Rotary Map? **7**
Leah Weiner

Interview with Professor Robert Seiringer **12**
Marie-Andrée B.Langlois

Rational Elliptic Curves Constructed Around a Given Point **14**
Dieter Fishbein

Don't Panic: A Crash Course in Set Theory for an Incoming U1. **21**
Benjamin Lewis

Interview with Professor Sergey Norin **24**
Marie-Andrée B.Langlois

How To Make Sense of Negative Probabilities **25**
Samuel Perreault

Certain Infinite Products with a View Toward Modular Forms **28**
Catherine Hilgers

Acknowledgements **34**

Letter from the Editors

Welcome to the sixth issue of The δelta-εpsilon! As in previous years, the journal tries to provide to all mathematically inclined undergraduate students an answer to the frequently asked question, "What even is Mathematics research?" We tackle this question from multiple angles by giving undergraduate students the opportunity to experience the academic publishing process and by exposing students to the original and expository research of their peers. Included in this edition are articles from students in many different stages of their Mathematics degrees and with research interests in various fields, making the collection both fascinating and accessible to all interested students. In addition, we have included once again some comic relief in the form of cartoons and jokes interspersed between articles, as well as a few interviews with professors in the department to help shed some light on a range of aspects of academia.

Although the release of this issue was behind schedule, we hope that it will help motivate students to seek out opportunities in Mathematics research throughout the school year. As always, The δelta-εpsilon relies on undergraduate students to thrive! Consider getting involved either through submitting work of your own or through working with the editorial team.

Best,
Cathryn Supko

Letter from SUMS

On behalf of the Society of Undergraduate Mathematics Students (SUMS), I would like to congratulate the editors of The δelta-εpsilon and its contributors on another inspiring issue. For each edition, the articles submitted are researched with zeal and meticulously edited, giving McGill's undergraduate mathematical community an accessible place to share its efforts. SUMS is proud to support The δelta-εpsilon in this endeavour.

Sincerely,
Catherine Hilgers
SUMS President

A Geometric Interpretation of the Uniformly Minimum-Variance Unbiased Estimator (UMVUE) with the Use of Hilbert Spaces

Jean-Philippe Fortin

We first consider the space of estimators of a random variable X as a Hilbert space whose measure is inherited from $F(x)$, the distribution function of X. We give the definition of the UMVUE and a theorem which characterizes it, and we finally give a geometric proof of this theorem using some results associated with Hilbert spaces.

1 Introduction

In statistics, the goal of estimation theory is to find the values of parameters based on experimental data which have a random component. We assume that the data come from a given probability distribution with unknown parameters and we estimate these parameters using estimators. Estimation theory deals with the properties of the different possible estimators in order to compare them. Most of the time, the definition of a good estimator depends on the context. One definition is to have a minimal mean squared error (MSE). Since the class of all estimators is often too large, we consider a certain subclass of estimators, namely those which are unbiased (we will see later the definition of an unbiased estimator). Under these conditions, the uniformly minimum-variance unbiased estimator (UMVUE) is a likely candidate for a good estimator.

We will show that the space of estimators can be defined as a Hilbert space, and we will use the properties of Hilbert spaces to prove a theorem which characterizes the UMVUE. Since Hilbert spaces are analogous to infinite vector spaces, the theorem will give us a geometric interpretation of the UMVUE.

In section 2, we will introduce some basic notions of probability and statistics and will define an estimator and a UMVUE. In section 3, we will give the basics of Hilbert spaces and we will show that the space of estimators is an example of a Hilbert space. Finally, in section 4, we will proceed to a geometric proof of a theorem which characterizes UMVUEs.

2 Some Notions of Probability and Statistics

Let $(\Omega, S, \mathbb{P})$ be a probability space where Ω is the set of all possible outcomes of an experiment, S is a σ-field associated with Ω and $\mathbb{P}$ is a probability measure defined on S. When we do experiments, we are not really interested in $(\Omega, S, \mathbb{P})$ itself. Most of the time, we look at functions defined on $(\Omega, S, \mathbb{P})$. A *random variable* is a measurable real-valued function $X : \Omega \quad \mathbb{R}$ from the probability space to the real numbers (to see what measurability is, see [1]). The distribution function $F(x)$ associated with X is defined as $F(x) = \mathbb{P}(\ \omega \quad \Omega : X(\omega) \leq x \ )$.

For a given random variable X, let $F(x;\theta)$ be its associated distribution function, where $\theta \quad \Theta \subseteq \mathbb{R}$ is an unknown real parameter. θ can be a vector, but for the purpose of simplicity, we assume that it is a scalar. A sample of size n of X is a vector $\overline{X} = (X_1, X_2, \ldots, X_n)$. An *estimator* $T(\overline{X})$ of θ is a Borel-measurable function $T : \mathbb{R}^n \quad \Theta$. Its role is to give an estimate of the parameter θ using experimental data represented by the random sample $\overline{X}$. One definition of a good estimator is one which has small MSE, i.e. we want to minimize

$$MSE[T] = var(T) + [Bias(T,\theta)]^2$$

where $Bias(T,\theta) = \mathbb{E}(T - \theta)$. An efficient way to minimize it is to set $Bias = 0$, i.e. to consider only the class of unbiased estimators, and to minimize the variance. Such an estimator is called a UMVUE.

Definition. *Let U be the set of all unbiased estimators T of $\theta \quad \Theta$ such that $\mathbb{E}_\theta[T^2] < \infty$ for all $\theta \quad \Theta$. An estimator $T_0 \quad U$ is called a uniformly minimum variance unbiased estimator (UMVUE) of θ if*

$$var_\theta(T_0) \leq var_\theta(T)$$

for all $\theta \quad \Theta$ and every $T \quad U$.

We would like to have criteria to find such an estimator. The following theorem given in [1] gives us a tool to compute the UMVUE.

Theorem 1. *Let U be the class of all unbiased estimators T of a parameter $\theta \quad \Theta$ with $\mathbb{E}_\theta[T^2] < \infty$ for all θ, and suppose that U is nonempty. Let U_0 be the class of all unbiased estimators v of 0, that is,*

$$U_0 = \ v : \mathbb{E}_\theta[v] = 0, \mathbb{E}_\theta[v^2] < \infty \quad \textit{for all} \quad \theta \quad \Theta \ .$$

Then $T_0 \quad U$ is a UMVUE if and only if

$$\mathbb{E}_\theta[vT_0] = 0 \quad \textit{for all } \theta \textit{ and all } v \quad U_0$$

.

The proof of the theorem will be given in section 4 using properties of Hilbert spaces. We need first to introduce them and show that the space of estimators $T(X_1, X_2, \ldots, X_n)$ can be defined as a Hilbert space.

3 Hilbert Spaces and Square Integrable Functions

In this section, we give the definition of a Hilbert space and we show that the space of square integrable functions (relative to a given measure) is an example of a Hilbert space. The theory comes from [2]. Finally, we show that the space of estimators $T(X_1, X_2, \ldots, X_n)$ of a random variable X (where the X_i's are distributed according to X) such that $\mathbb{E}[T^2] < \infty$ is an example of a space of square integrable functions, and hence is a Hilbert space under some conditions.

3.1 Hilbert Spaces

A Hilbert space H is the natural infinite-dimensional analogue of an Euclidean n-space and so can be viewed as an infinite vector space. It has to satisfy the following properties:

1. H is a linear space
2. An inner product (f,g) is defined in H. We define the norm $\quad f \quad$ to be $\quad f \quad = (f,f)^{\frac{1}{2}}$
3. H is complete with the metric
$$d(f,g) = \quad f - g \quad,$$
i.e. H is a Banach space.

Here are some useful definitions and properties of vector spaces which also hold for Hilbert spaces. Two vectors $f, g \quad H$ are *orthogonal* if and only if $(f,g) = 0$. A vector f is *orthogonal to a subspace M* of H if and only if $(f,m) = 0$ for all $m \quad M$. The *orthogonal complement* of a subspace M is the subspace $M \quad = \quad g \quad H : (g,M) = 0 \quad .$

Proposition 2. *If M is a subspace of H, then every $f \quad H$ is uniquely representable in the form $f = h + h$ where $h \quad M, h \quad\; M$.*

In other words, any vector $f \quad H$ can be decomposed uniquely into the sum of its orthogonal projection in M (h) and its orthogonal projection in M (h). We will use this property later.

3.2 Square Integrable Functions

A measure μ is a generalization of the length, area or volume to spaces which are not necessarily Euclidean. It is possible to associate many different measures to a given space R. We will not list the properties of a measure here, but only mention that it is used to generalize the notion of integral. For example, the Lebesgue integral is based on the existence of the Lebesgue measure. For more detail, see [2]. Let R be a μ-measurable set such that $\mu(R) < \infty$. Denote by $L_2(R,\mu)$ the space of square integrable functions $f : R \quad \mathbb{R}$ i.e. the space of measurable functions f satisfying

$$L_2(R,\mu) = \quad f(x) : \int_R f^2(x) d\mu < \infty \quad .$$

By the linearity of the integral, we can easily show that this space is a Euclidean space. Choose the following inner product:

$$(f,g) = \int_R f(x)g(x) d\mu.$$

It follows that the norm of $f(x)$ is

$$f(x) \quad = \left(\int_R f^2(x) d\mu \right)^{\frac{1}{2}}.$$

It can be shown that L_2 is complete with respect to this norm, which implies $L_2(R,\mu)$ is a Hilbert space. $L_2(R,\mu)$ can be seen as an infinite-dimensional vector space, and the square integrable functions $f(x)$ can be considered as infinite vectors in the space L_2. We will show in the next subsection that the space of estimators is a space $L_2(\mathbb{R}^n, \mu)$ with a suitable measure μ.

3.3 Space of Estimators of θ

Consider all the possible estimators $T_\theta(X_1, X_2, \ldots, X_n) : \mathbb{R}^n \quad \mathbb{R}$ of a random variable X distributed according to $F(x;\theta)$, where $\theta \quad \Theta$. Let $f(x)$ be the associated density function. Consider the space L_2 of all such estimators which satisfy $\mathbb{E}_\theta[T^2(\overline{x})] < \infty$, i.e. the estimators whose second moment is finite. For $T(\overline{x}) \quad L_2$, we have

$$\begin{aligned} \mathbb{E}[T^2(\overline{x})] &:= \int_{-\infty}^{\infty} T^2(\overline{x}) f(x) dx \\ &= \int_{-\infty}^{\infty} T^2(\overline{x}) d\mu_F < \infty \end{aligned}$$

where $\mu_F(x)$ is defined as the Lebesgue-Stieltjes measure associated with the distribution function $F(x)$ (indeed it can be shown that this is really a measure). This means that the estimators $T(X)$ which satisfy $\mathbb{E}(T^2) < \infty$ are square integrable functions of the space $L_2(\mathbb{R}^n, \mu_F(x))$.

Let $T_\theta(\overline{x})$ and $S_\theta(\overline{x})$ be two estimators of a n-random sample of $X \sim F(x,\theta)$. Assume $\mathbb{E}[T^2(\overline{x})] < \infty$ and $\mathbb{E}[S^2(\overline{x})] < \infty$ as well. We will show that the covariance of these two estimators can be taken as an inner product on the space $L_2(\mathbb{R}^n, \mu_F(x))$, which means that the norm of an estimator $T_\theta(\overline{x})$ is the same as the square root of its variance.

Proposition 3. *The covariance of the estimators T and S defines an inner product on $L_2(\mathbb{R}^n, \mu_F(x))$, and so*

$$(T,S) = cov(T,S) = \mathbb{E}[T_\theta(\overline{x})S_\theta(\overline{x})].$$

Proof. This is clear from the following properties of the covariance:

$$\begin{aligned} cov(aX+Y,Z) &= \mathbb{E}((aX+Y)Z) - \mathbb{E}(aX+Y)\mathbb{E}(Z) \\ &= \mathbb{E}(aXY+YZ) - \mathbb{E}(aX)\mathbb{E}(Z) \\ &\qquad - \mathbb{E}(Y)\mathbb{E}(Z) \\ &= [\mathbb{E}(aXZ) - \mathbb{E}(aX)\mathbb{E}(Z)] \\ &\qquad + [\mathbb{E}(YZ)_{\text{¸}} - \mathbb{E}(Y)\mathbb{E}(Z)] \\ &= a[cov(X,Z)] + cov(Y,Z). \end{aligned}$$

Moreover,

$$\begin{aligned} T_\theta(\overline{x}) \quad {}^2 &= cov(T_\theta(\overline{x}), T_\theta(\overline{x})) \\ &= \mathbb{E}[T_\theta(\overline{x})^2] - \mathbb{E}[T_\theta(\overline{x})]^2 \\ &= var(T_\theta(\overline{x})) \geq 0. \end{aligned}$$

□

Consequently, we can consider an estimator $T_\theta(\overline{x}) \quad L_2(\mathbb{R}^n, \mu_F(x))$ as an infinite vector whose norm squared is the variance of this estimator with respect to θ. It follows from this that the problem of finding an unbiased estimator which has minimal variance is translated to finding a vector in $L_2(\mathbb{R}^n, \mu_F(x))$ which has minimal norm and which is unbiased. The subclass of unbiased estimators with $\theta = 0$ can be seen as the kernel of a linear functional defined on $L_2(\mathbb{R}^n, \mu_F(x))$. A linear functional $A(T)$ is a mapping $A : L_2(\mathbb{R}^n, \mu_F(x)) \quad \mathbb{R}$ that satisfies linearity. The *kernel* of a linear functional is defined to be

$$ker[A(T)] = \quad T_\theta(\overline{x}) \quad L_2 : A(T_\theta(\overline{x})) = 0 \quad .$$

It is easy to show that the kernel of a linear functional is a linear subspace. We will use the following result to prove Theorem 1. Defining the following linear functional $A(T_\theta(\overline{x}) = \mathbb{E}_\theta[T_\theta(\overline{x})]$, we arrive at the following result.

Proposition 4. *The set of unbiased estimators $T_\theta(\overline{x})$ with $\theta = 0$ and finite second moment is a linear subspace of $L_2(\mathbb{R}^n, \mu_F(x))$.*

4 Geometric Interpretation of the UMVUE

We are now ready to prove Theorem 1 using properties of Hilbert spaces. Denote the space $L_2(\mathbb{R}^n, \mu_F(x))$ as H. We will reformulate the definition of the UMVUE and Theorem 1 in the language of Hilbert spaces. First, we notice that the condition $\mathbb{E}[T^2] < \infty$ implies that $var(T) < \infty$. This corresponds to the condition $\quad T \quad {}^2 < \infty$, meaning that $T \quad H$. We can then consider T as an bounded infinite-dimensional vector. We define $A(T)$ as above, i.e. $A(T) = \mathbb{E}_\theta[T]$.

Definition. *Let U be the set of all vectors $T \quad H$ with $A(T) = \theta$ and $\quad T \quad {}^2 < \infty$ for all $\theta \quad \Theta$. $T_0 \quad U$ is a UMVUE of θ if*

$$T_0 \quad {}^2 \leq \quad T \quad {}^2$$

for all $\theta \quad \Theta$ and every $T \quad U$.

Theorem 5. *Let U be the set of all vectors T with $A(T) = \theta$ and $\quad T \quad {}^2 < \infty$ for all $\theta \quad \Theta$, and suppose that U is nonempty. Let U_0 be the kernel of $A(T)$, i.e.*

$$U_0 = \quad v : A(v) = 0, \quad v \quad {}^2 < \infty \quad \text{for all} \quad \theta \quad \Theta \quad .$$

Then $T_0 \quad U$ is a UMVUE if and only if

$$(v, T_0) = 0 \quad \text{for all } \theta \text{ and all } v \quad U_0.$$

We will now give the proof using geometric arguments.

Proof. Suppose the vector T_0 is a UMVUE and suppose that there exists some vector $v \quad U_0$ such that $(T_0, v) = 0$. This means that T_0 is not orthogonal to the linear subspace U_0. Then there exists a nonzero orthogonal projection $x_0 \quad U_0$. Consider the vector $T = T_0 - x_0$. The Figure 1 helps us to visualize the decomposition of the vector T_0; however, we have to keep in mind that the vectors in H are infinite-dimensional, and hence cannot be represented in a 3-d Euclidean space. Moreover,

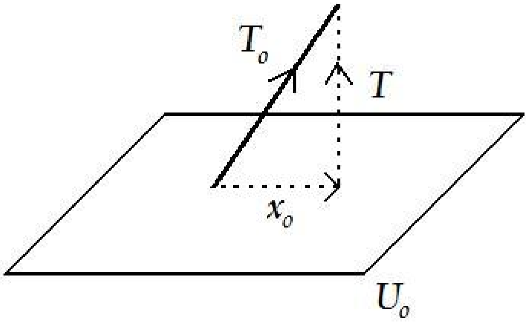


Figure 1: Decomposition of the vector T_0

$$\begin{aligned} A(T) &= A(T_0 - x_0) \\ &= A(T_0) - A(x_0) && \text{since } A \text{ is a linear operator} \\ &= A(T_0) - 0 && \text{since } x_0 \quad U_0 \\ &= \theta && \text{since } T_0 \quad U \ . \end{aligned}$$

Then we conclude that $T \quad U$, and so T is also an unbiased estimator of θ.
Now, since $T_0 = Proj_{U_0}(T_0) \oplus U_0$, then $T_0 = x_0 \oplus T$. Consequently,

$$\begin{aligned} T_0 \ {}^2 = \ x_0 \ {}^2 + \ T \ {}^2 \qquad & T \ {}^2 = \ T_0 \ {}^2 - \ x_0 \ {}^2 \\ & T \ {}^2 < \ T_0 \ {}^2. \end{aligned}$$

This is a contradiction by the definition of the UMVUE T_0. We conclude that $(T_0, v) = 0$ for all $v \quad U_0$.

We want to prove the other direction. Suppose that the vector $T_0 \quad U$ is such that $(T_0, v) = 0$ for all $v \quad U_0$. Take any vector $T \quad U$. Consider the vector $T \ = T_0 - T$. Then

$$\begin{aligned} A(T \ ) &= A(T_0 - T) \\ &= A(T_0) - A(T) \\ &= \theta - \theta \\ &= 0. \end{aligned}$$

It follows that $T \qquad U_0$. Then we have

$$\begin{aligned} (T_0, T \ ) = 0 \qquad & (T_0, T_0 - T) = 0 \\ & (T_0, T_0) - (T_0, T) = 0 \\ & (T_0, T_0) = (T_0, T) \\ & (T_0, T_0) \le \ T_0 \quad T \qquad \text{(by CSI)} \\ & \ T_0 \ {}^2 \le \ T_0 \quad T \\ & \ T_0 \ \le \ T \\ & \ T_0 \ {}^2 \le \ T \ {}^2. \end{aligned}$$

Note that CSI stands for Cauchy-Schwartz inequality. This corresponds to the second definition of the UMVUE. Then T_0 is a UMVUE of θ. The proof is complete.

□

Moreover, we can show that the UMVUE is unique up to a constant. Suppose there exist two UMVUEs T_1 and T_2. Then we have $(T_1, T) = (T_2, T) = 0$ for all $T \quad U_0$ by the previous theorem. It follows that $(T_1 - T_2, T) = 0$ for all $T \quad U_0$. It means that the estimator $T_1 - T_2$ is also a UMVUE. But $A(T_1 - T_2) = A(T_1) - A(T_2) = \theta - \theta = 0$, which implies $T_1 - T_2 \quad U_0$. We conclude $T_1 - T_2 = 0$, i.e. $T_1 = T_2$.

5 Conclusion

We can interpret the UMVUE geometrically as a infinite vector which is perpendicular to the linear subspace of all vectors v which are unbiased estimators of $\theta = 0$.

Acknowledgements: I would like to thank Prof. Masoud Asgharian for his invaluable help and for having introduced me to this problem.

References

[1] Rohatgi, V.K,Saleh, A.K.Md.: *An Introduction to Probability and Statistics*, Wiley Series in Probability and Statistics, (2001), 279-280.

[2] Kolmogorov, A.N., Fomin, S.V.: *Elements of the theory of functions and functional analysis*, Dover Publications, (1961), 179-122.

Which Propeller Graphs Are The Underlying Graph of a Rotary Map?

Leah Weiner

We will explore a sufficient condition for a propeller graph to be the underlying graph of a rotary map. We will describe the composition of the rotary maps which correspond to this set of propeller graphs.

1 Introduction

A *graph* is a mathematical structure composed of vertices and edges. Edges are two-element subsets of the vertex set. If (v_1,v_2) denotes the same edge as (v_2, v_1), then we call this edge *undirected*. However, if the order of the pairing matters, that is if (v_1, v_2) denotes a different edge than (v_2, v_1) then we call this edge a *directed edge*, or *dart*. The darts of a graph Γ are sometimes denoted D(Γ). Graphs are represented by dots (corresponding to the vertices) and lines connecting these dots (corresponding to the edges). We call the number of edges incident to some vertex the *degree*, or *valency*, of that vertex.

Many problems can be modelled as graphs, so generalizing properties of certain classes of graphs can prove to be quite useful. The question of which graphs are the underlying graph of a regular map (defined below) has been studied for many years. Whether a graph is the underlying graph of a rotary map is a newer topic of research. This paper concerns the class of graphs called *propeller graphs*. Little research has been done on propeller graphs, thus very little is known about them. This paper explores one subset of propeller graphs which are the underlying graph of a rotary map.

Given positive (non-zero) integers a, b, c, d, n such that a, b, c, $d < n$, a propeller graph, denoted $Pr_n(a,b,c,d)$, is constructed as follows:

A propeller graph has $3n$ vertices, which we label A_1, A_2,..., A_n, B_1,..., B_n, C_1,..., C_n. The three types of edges are dependent on the values of a, b, c and d. For all $i = 1,2,\dots,n$, the *flat edges* are of the form (A_i, B_i) and (B_i, C_i), the *wing edges* are of the form (B_i, A_{i+b}) and (B_i, C_{i+c}), and the *tip edges* are of the form (A_i, A_{i+a}) and (C_i, C_{i+d}), where addition is done modulo n. Note that flat edges are undirected edges, while tip and wing edges are directed edges.

Figure 1: A Generalized Propeller Graph

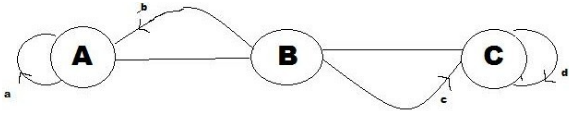
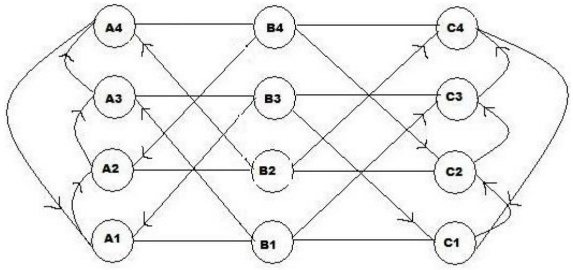


Figure 2: $Pr_4(1,2,2,1)$



We continue with some more definitions.

A *2-manifold* can be defined as a topological space in which every point in the space has an open disk as a neighbourhood. This is equivalent to saying that each point locally looks like a plane. A *closed surface* is then a compact (closed and bounded) 2-manifold. We will refer to a closed surface simply as a surface.

A drawing of a graph Γ on some surface such that no edge (i.e. line representing an edge) crosses any other edge is called an *embedding* of Γ on this surface. It is not the case that every graph has an embedding on every surface. The vertices and edges of Γ, when represented by an embedding on some surface, fully enclose regions of the surface. Each enclosed region is called a *face* of the embedding.

(a) Regular K_4 graph (b) Embedding of K_4 in the finite plane

Figure 3: Examples of K_4 graphs.

Let Γ be a connected graph. It may be possible to embed Γ onto some surface such that each face of the embedded graph is homeomorphic to the open disk. That is, if we are given any two points p_1 and p_2 on some face of the embedding, there is a path from p_1 to p_2 that is completely contained within the face (i.e. the face is simply connected). We call such an embedding of Γ the corresponding *map*.

Each face of a map is composed of corners and sides. We can think of the corners as vertices and the sides as edges. The *underlying graph of a map* is the undirected graph formed from the faces of an embedded map such that each corner of each face in the map becomes a vertex and each side of each face in the map becomes an edge. Although we usually think of a map as being composed of faces, we sometimes will refer to the vertices and edges of a map, in which case we mean the vertices and edges formed from the faces of the map in the way just described.

If a map M is an embedding of the graph Γ on some surface S, then a *symmetry*, or *automorphism*, of M is a permutation of its vertices, edges and faces which can be achieved by a homeomorphism of the surface S onto itself. If σ is an automorphism of a map, then for any edge (v_1, v_2) of our map, the edge $(\sigma(v_1),\sigma(v_2))$ is also an edge of our map. A *stabilizer* of a vertex, edge or face is an automorphism that sends that vertex, edge or face, respectively, to itself.

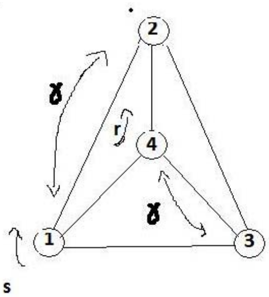


Figure 4: Example of symmetry on a $K_4.\gamma = (12)(34)$ stabilizes the edges (1,2) and (3,4); $s = (243)$ stabilizes vertex 1; and $r = \gamma * s = (142)$

We denote the group formed by these symmetries, together with the operation of composition, as $Aut(M)$.

Let Γ be the underlying graph of some map M. If α is a permutation of the edges of Γ then α is called an *even automorphsim* of M if αR = $R\alpha$, where R is a rotation of the edges. We denote the group of even automorphisms as $Aut^+(M)$.

A map M is an *orientably regular* map if $Aut^+(M)$ acts transitively on the directed edges of M's corresponding graph. That is, for each pair of directed edges, e_1 and e_2, there is a symmetry σ $\quad Aut^+(M)$ such that $e_1 = \sigma(e_2)$ (preserving direction).

A map M embedded on some surface S is *rotary* provided that for some face F of M and some vertex v incident to F, there exists symmetries r and s such that r acts on F as a rotation one step and s acts on v as a rotation one step. That is, r is the rotation of the surface that sends F to itself, moving the edges of F in a circular way. Similarly, s is the rotation of the surface which sends v to itself, moving the edges incident to v in a circular way.

Every rotary map is a regular map. If M is orientably regular, then M is orientable and rotary.

We are now ready to state the focus of this paper.

Each propeller graph of the form $Pr_n(1,2d,2,d)$, where $d^2 = -1(\text{mod } n)$, d is odd, n is even, and $\frac{n}{2}$ is odd, is an underlying graph of some rotary map. The symmetries of these rotary maps, γ, r, and s, which act on an edge, a face and a vertex of the map, respectively, follow a generalized form depending on the value of d. These symmetries are described in detail in Tables 1 and 2.

The rotary maps corresponding to this set of propeller graphs are composed of 12-sided faces. The corners of each of these faces have the ordering AABCCBAABCCB, where a corner is labelled A, B or C according to the labelling of the corresponding vertex in the propeller graph which is the underlying graph of the given rotary map.

2 Approach

We are interested in finding which propeller graphs are the underlying graph of a rotary map. It makes sense then to explore previous research regarding graphs which are the underlying graph of a regular map.

In their paper "Characterization of Graphs Which Underlie Regular Maps on Closed Surfaces", Gardiner, Nedela, Siran and Skoviera attain the important result that "a connected graph K of valency ≥ 3 admits an embedding as an orientably regular map (on some closed, orientable surface) if and only if the automorphism group contains a subgroup G acting transitively on $D(K)$ and such that the stabilizer G_v of every vertex v is cyclic". Note that all propeller graphs are connected and of valency ≥ 3, and that orientably regular maps are orientable and rotary. This theorem then implies that all propeller graphs which satisfy the conditions of the second part of the theorem are underlying graphs of a rotary (and orientable) map.

To begin to form a hypothesis regarding the general form of a propeller graph that is the underlying graph of a rotary map, it helps to look at some examples of such propeller graphs and try to observe a pattern. We obtain these examples by utilizing the equivalence described in the previously stated theorem.

The programming language Magma was specifically designed to perform algebraic and graph-related operations easily. Simple code in Magma can generate a list of all the propeller graphs with up to 30 vertices ($n \leq 10$) such that for each graph, the automorphism groups contain a subgroup which acts transitively on the edges of the graph and whose stabilizer of each vertex of the graph is cyclic. The theorem by Gardiner *et al.* then gives a list of propeller graphs with up to 30 vertices which are the underlying graph of some rotary map. This list is not as long as one may initially think. Removing graphs which have an isomorphic graph already in the list leaves about 20 propeller graphs which have less than 30 vertices and which satisfy the conditions stated in the second part of the theorem.

Given these propeller graphs, it is not hard to construct the corresponding maps. Consider labelling the corners of each map A, B, or C in the following way: A corner is labelled "A" if the corresponding vertex in the graph is labelled A_i for any $i \leq n$. Similarly, a corner is labelled "B" if the corresponding vertex in the graph is labelled B_i for any $i \leq n$, and is labelled "C" if the corresponding vertex in the graph is labelled C_i for any $i \leq n$.

A subset of the maps corresponding to this list of propeller graphs have faces composed of 12 sides and 12 corners, with corners in the order AABCCBAABCCB. There was no immediately apparent pattern regarding the values of a, b, c or d of the propeller graphs whose corresponding maps had faces of this type. Thus, as a starting point to generalizing all propeller graphs which are the underlying graph of a rotary map, we consider the set of propeller graphs with $a = 1$ and whose corresponding rotary maps are made up of 12-gons whose corners are ordered AABCCBAABCCB.

Additionally, for each of these maps, we can print out the corresponding set of symmetries γ and s such that γ stabilizes the edge (A_n, B_n) and s stabilizes the vertex A_n. Some maps had multiple symmetries in their automorphism groups that stabilized (A_n, B_n) or v. However, all these maps had at least one symmetry stabilizing (A_n, B_n) and another stabilizing v in their automorphism group which followed a general form.

The patterns which we observe for propeller graphs of the form $Pr_n(1,b,c,d)$ with up to 30 vertices provide us with a hypothesis that generalizes to all propeller graphs. This hypothesis is stated and proved below.

3 Results

One set of propeller graphs which are underlying graphs of a rotary map can be generalized to the form $Pr_n(1,2d,2,d)$, with $d^2 = -1 (\text{mod } n)$, d odd, n even, and $\frac{n}{2}$ odd.

The maps corresponding to this set of propeller graphs have symmetries γ, r, and s, which act on an edge, a face and a vertex of the map, respectively, and follow a general form depending on d, as described below. Because such γ, r and s exist, we can thus conclude that the set of propeller graphs of this form are indeed rotary.

Additionally, the rotary maps corresponding to these graphs are composed of faces made up of 12 sides and 12 corners. The corners of each face in each map are in the order AABCCBAABCCB.

There exists a γ in the automorphism group of each of these propeller graphs such that γ acts on, or stabilizes, the edge (A_n, B_n). For this subset of propeller graphs, we can characterize the symmetry γ for each $i = 1, \ldots, n$ as according to the parity of i:

$$\gamma = \begin{cases} (A_i, B_{-i}) & \text{if } i \text{ is even,} \\ (A_i, C_{1-i})(B_i, C_{-i-d+1}) & \text{if } i \text{ is odd .} \end{cases}$$

Similarly, there exists a symmetry s in the automorphism group of each of these propeller graphs such that s stabilizes the vertex A_n. For this subset of propeller graphs, s is of the form, for all $i = 1, 2, ..., n$:

$$s = \begin{cases} (A_i, A_{di}, A_{-i}, A_{-di}) & \text{if } i \text{ is even,} \\ (A_i, B_{d(i-1)}, A_{-i}, B_{-d(i+1)})\circ & \\ (B_i, C_{d(i-1)}, B_{-2d-i}, C_{d(i-3)+2})\circ & \\ (C_i, C_{d(i-2)}, C_{-2(d-1)-i}, C_{-di+2}) & \text{if } i \text{ is odd.} \end{cases}$$

The symmetries γ and s are also symmetries of the corresponding maps. The symmetry $r = \gamma * s$ stabilizes a face F incident to the edge (A_n, B_n) for each corresponding map. The symmetry s stabilizes the vertex A_n (incident to F). Thus these maps are indeed rotary.

Applying γ and s to these propeller graphs should again yield a propeller graph. Using this crucial piece of information, we can derive the following conditions of a, b, c, d, and n by applying the generalized symmetries γ and s to each of the six generalized types of edges of the propeller graph in both the cases where i is even and where i is odd:

$$\begin{cases} a = 1 \\ c = 2 \\ b = 2d \\ d^2 = -1 \pmod{n} \\ d \text{ odd} \\ n \text{ even} \\ \frac{n}{2} \text{ odd} \end{cases}$$

4 Proof

Tables 1 and 2 demonstrate concisely the results of applying γ and s to each edge of a general propeller graph and what the resulting symmetries imply for the values of b, c and d in our graphs (recall, we are only considering propeller graphs where $a = 1$).

Applying the symmetries to the edges is simple. After applying a symmetry to some edge, we are left with an edge of some unrecognisable form. But because we know that this new edge must be a valid edge in a propeller graph, it must follow the general from of a flat, wing or tip edge.

From this knowledge, we derive values for b, c and d.

This paper will not go through each computation here, but rather give one example of classifying a permuted edge as flat, wing or tip, and one example of finding how we discover what this symmetry implies for the values of b, c and d.

5 Classifying edges

We classify the edges as follows. Consider the flat edge of a propeller graph (A_i, B_i) and the symmetry γ. Applying γ to the edge (A_i, B_i) when i is even yields the edge (B_{-i}, A_{-i}). Because γ is a symmetry of our propeller graph, we must have that (B_{-i}, A_{-i}) is also an edge in our propeller graph. The classification of the (B_{-i}, A_{-i}) as a flat, wing or tip edge is then obtained as follows.

The edges that connect B vertices to A vertices in any propeller graph are either flat edges and wing edges. Thus, the possibility that (B_{-i}, A_{-i}) is a tip edge can easily be eliminated. Wing edges connecting B vertices to A vertices are of the form (B_i, A_{i+b}). Flat edges connected B vertices to A vertices are of the form (A_i, B_i) (recall that flat edges are undirected, so that (A_i, B_i) is equivalent to (B_i, A_i)).

Suppose first that (B_{-i}, A_{-i}) is a wing edge. Recall that wing edges are of the form (B_i, A_{i+b}) so that if (B_{-i}, A_{-i}) were indeed a wing edge, this would imply that $-(i+b) = -i$, which in turn implies that $b = 0$. This is a contradiction to our initial assumption that b is a positive (non-zero) integer.

We can thus conclude that (B_{-i}, A_{-i}) is a flat edge. To verify this, let $j = -i$, and obtain the edge (B_j, A_j), which is indeed a flat edge in a propeller graph.

6 Finding implications

We find the implications on the values of b, c and d as follows. Consider applying γ to the edge (B_i, A_{i+b}) when i is odd.

Applying γ to B_i when i is odd yields C_{-i-d+1}.

Applying γ to A_{i+b} when i is odd yields B_{-i-b} if b is odd ($i+b$ is even), and yields C_{1-i-b} if b is even ($i+b$ is odd). A propeller graph connects C vertices to both B and C vertices, creating a wing edge (C connects to B) or a tip edge (C connects to C). Without knowing whether b is even or odd, no further conditions can be obtained from this application of γ to the edge (B_i, A_{i+b}).

In order to obtain more information, consider what happens in the case when applying γ to the edge (B_i, A_{i+b}) when i is even. Applying γ to B_i would then yield A_i. Applying γ to A_{i+b} would yield either B_{-i-b} (if b is even) or C_{1-i-b} (if b is odd). So since γ is a symmetry of our graph, there must be an edge (A_i, A_{i+b}) or (A_i, C_{1-i-b}).

No propeller graph has edges connected A vertices to C vertices, thus the edge (A_i, C_{1-i-b}) cannot exist. Therefore, we know that b must be even.

With this new information, we resume our inspection of the case when i is odd. Given that b is even, applying γ to the edge (B_i, A_{i+b}) when i is odd yields that the edge (C_{-i-d+1}, C_{1-i-b}) is in the graph. We can immediately observe that this is a tip edge (since a C vertex is connecting a C vertex), and thus must be of the form (C_i, C_{i+d}). Thus one of the following conditions must hold:

$$\begin{cases} (1) \quad -i-d+1+d = 1-i-b \\ (2) \quad -i-d+1-d = 1-i-b \end{cases}$$

Simplifying equation (1) yields $b = 0$, which is a contradiction to the initial assumptions on b. So equation (2) must be correct. Rearranging equation (2) yields $b = 2d$.

Recall that the symmetry γ was applied to an edge in a general propeller graph. The condition $b = 2d$ is thus necessary for any propeller graph to be the underlying graph of a rotary map whose faces, sides and corners are as described above.

A similar argument yields columns five and six for each (γ * edge) in Table 1 and each (s * edge) in Table 2.

7 Conclusion

We have seen that the class of propeller graphs of the form $Pr_n(1, 2d, 2, d)$, where $d^2 = -1(\text{mod } n)$, d is odd, n is even, and $\frac{n}{2}$ is odd, is a set of underlying graphs of some rotary maps. The corresponding maps are all composed of 12-gons with corners in the order AABCCBAABCCB, and the symmetries of the maps follow the generalized form as described in Tables 1 and 2.

There are other propeller graphs that do not fall into this generalization, but are indeed the underlying graph of a rotary map. They are not discussed here because the general forms of such graphs that do not fall into the category laid out above are not known.

8 ACKNOWLEDGEMENTS

I would like to thank Professor Steve Wilson for his guidance through the research process.

9 REFERENCES

A. Gardiner, R. Nedela, J Siran, and M. Skoviera, Characterization of maps which underlie regular maps on closed surfaces, *J. London Math. Soc (2)* **59**, No. 1 (1991), 100-108

S. Wilson, Families of Regular Graphs in Regular Maps, *Journal of Combinatorial Theory* **B 85**, 269-289 (2002)

1	2	3	4	5	6
Edge	Edge Type	i	γ*Edge	(γ*Edge) Type	Implication
(A_i, B_i)	at	even	(B_{-i}, A_{-i})	at	
		odd	(C_{1-i}, C_{-i-d+1})	tip	$d = d$
(B_i, C_i)	at	even	(A_{-i}, A_{1-i})	tip	$a = 1$
		odd	(C_{-i-d+1}, B_{-i-d+1})	at	
(B_i, A_{i+b})	wing	even	$(A_{-i}, B_{-i-b}\ )$	wing	$b = b$
		odd	$(C{-}i - d + 1, C_{1-i-b})$	tip	$b = 2d$
(B_i, C_{i+c})	wing	even	(A_{-i}, A_{1-i-c})	tip	$a = 1$
		odd	$(C_{-i-d+1}, B_{-i-c-d+1})$	wing	$c = c$
(A_i, A_{i+a})	tip	even	(B_{-i}, C_{1-i-a})	at	
		odd	$(C_{1-i}), B_{-i-a})$	wing	$c = 1 + a (= 2)$
(C_i, C_{i+d})	tip	even	$(A1 - i, B_{-i-2d+1}))$	wing	$b = 2d$
		odd	(B_{-i-d+1}, A_{1-i-d})	at	

Table 1: Applying γ

1	2	3	4	5	6
Edge	Edge Type	i	s*Edge	(s*Edge) Type	Implication
(A_i, B_i)	at	even	(A_{di}, A_{di+1})	tip	$a = 1$
		odd	(B_{di-d}, C_{di-d})	at	
(B_i, C_i)	at	even	$(A_{di+1}, B_{(i-2)+1})$	wing	$b = 2d$
		odd	$(C_{d(i-1)}, C_{d(-2)})$	tip	$d = d$
(B_i, A_{i+b})	wing	even	$(A_{di+1}, A_{di+bd}\ )$	tip	$1 + a = bd (= 2)$
		odd	$(Cdi - 1, B_{d(i-b+1)})$	wing	$c = bd = 2$
(B_i, C_{i+c})	wing	even	$(A_{di+1}, B_{d(i+c-2)-1})$	at	
		odd	$(C_{d(i-1)}, C_{d(i+c-2)})$	tip	$c = 2$
(A_i, A_{i+a})	tip	even	$(A_{di}, B_{d(i+a-1)})$	at	
		odd	$(B_{d(i-1)}), A_{d(i+a)})$	wing	$b = 2d$
(C_i, C_{i+d})	tip	even	$(B_{d(i-2)+1}, C_{d(i+d-2)}))$	wing	$d^2 = 1 - c = 1 - 2 = -1$
		odd	$(C_{d(i-2)}, B_{d(i+d-2)+1})$	at	

Table 2: Applying s

JOKES

A mathematician going through the American border for a group theory conference is interrogated by the customs officer.
"What exactly is the purpose of your visit to the United States?"
After thinking a while of the most concise comprehensible answer, she responds simply "Free groups."
The officer replies "Exactly which groups do you want to liberate?" □

Interview with Professor Robert Seiringer

Marie-Andrée B.Langlois

Professor Seiringer is a mathematical physicist who joined the McGill Mathematics Department last winter.

$\delta\varepsilon$: Tell us about your background, both personal and academic:
I am from the countryside of Austria. I did almost all of my studies at the University of Vienna learning physics. I went to Princeton for my postdoctoral fellowship where I also spent time as an Assistant Professor. After living in the United States for nine years, I moved to Montreal as I had accepted a position as an Associate Professor at McGill where I plan on staying.

$\delta\varepsilon$: Why did you chose to study mathematical physics?
My first objective was to study astronomy; however, I quickly became unhappy because my courses were too superficial. I realized that in order to understand astronomy you need to understand physics. That is why I started doing physics. Then I noticed that in order to understand the aspects of physics I was interested in I needed to know rigorous mathematics so I learned physics through learning mathematics. At the end of it all, I obtained a degree in physics but I took a lot of math classes. My favourite math classes as an undergraduate where analysis, more specifically functional analysis.

$\delta\varepsilon$: What was your favourite part of your mathematical track?
I think that every step has its advantages and disadvantages, but in general I like it more and more as it progresses. I enjoyed going from a postdoctoral fellowship to Assistant Professor at Princeton. I felt like I was becoming a part of the department and that I could make more connections with the people there.

$\delta\varepsilon$: At Princeton you were part of the physics department and here you are in the mathematics department, do you have a preference?
As I am still doing the same type of research I don't see many differences between both departments. I do like the physics colloquial better though.

$\delta\varepsilon$: Do you prefer teaching math or physics classes?
When it comes to basic classes, I think as a professor you can still learn things when teaching elementary physics courses, which is not the case when you teach calculus or linear algebra. On the other hand, I prefer teaching more advanced classes like the ones I am teaching here at McGill.

$\delta\varepsilon$: Are you enjoying McGill and Montreal so far?
I very much like McGill, there are many good students and researchers as well as interesting talks. Because of its many universities, a lot of good research is being done in Montreal. This city is very fascinating. My free time is dedicated mostly to taking care of my young daughter so I have yet to explore the entire city.

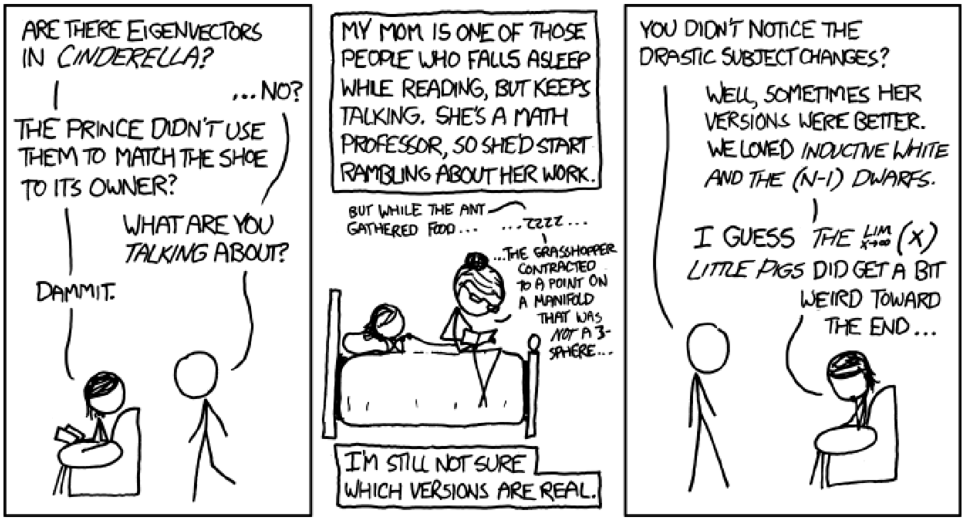
$\delta\varepsilon$: In Austria, you studied Bose gases. Can you briefly explain what these are and tell us a little about your research?
The main objective of physics is to understand the laws of nature. Personally, I am interested in how atoms interact to produce what we see everyday. We know that there is a variety of natural phenomena that respect the same laws of physics. Bose gases are not simply observed in every day life, studying them requires sophisticated lab equipment. The research I do tries to provoke elements to their extremes. For instance, experiments are done at very cold temperatures in order to try and deduce the equations that explain everyday occurrences. Most of the time we have the theory but we do not have the mathematical tools to make good predictions.

$\delta\varepsilon$: Could you explain stability of matter?
Everything is made out of atoms and, contrary to popular belief, there are not many of them. The electrostatic forces between them are what determine the physical state of a substance. The research I do tries to establish why, given the many interactions between positive and negative charges within objects, is there still stability? Why does matter not collapse? Quantum mechanics can explain why a single atom is stable, yet we need to understand what happens when we have more. Questions like why two litres of water occupy twice the volume of one can be explained using Schroedinger's equation. However, we must also understand Pauli's principles and the uncertainty principle in order to describe other properties of substances. If matter were not stable, pouring a glass of water would release more energy than an atomic bomb.

$\delta\varepsilon$: What are you currently working on?
I am working on problems that deal with the stability of matter. For example, how particles interact with consideration to quantum mechanics and condensed metaphysics. I also work on developing mathematical tools required to do physics. As I am still doing mathematics. I am proving theorems but my motivation comes from physics.

$\delta\varepsilon$: What advice would you give to undergraduate students?
In general I'd say do what you are interested in and do not be afraid to ask questions to professors or other students. Also keep your eyes open to all fields, interdisciplinary work is exciting.

JOKES


ARE THERE EIGENVECTORS IN *CINDERELLA?*
...NO?
THE PRINCE DIDN'T USE THEM TO MATCH THE SHOE TO ITS OWNER?
WHAT ARE YOU *TALKING* ABOUT?
DAMMIT.
MY MOM IS ONE OF THOSE PEOPLE WHO FALLS ASLEEP WHILE READING, BUT KEEPS TALKING. SHE'S A MATH PROFESSOR, SO SHE'D START RAMBLING ABOUT HER WORK.
BUT WHILE THE ANT GATHERED FOOD...
...ZZZZ...
...THE GRASSHOPPER CONTRACTED TO A POINT ON A MANIFOLD THAT WAS *NOT* A 3-SPHERE...
I'M STILL NOT SURE WHICH VERSIONS ARE REAL.
YOU DIDN'T NOTICE THE DRASTIC SUBJECT CHANGES?
WELL, SOMETIMES HER VERSIONS WERE BETTER. WE LOVED *INDUCTIVE WHITE AND THE (N-1) DWARFS.*
I GUESS *THE* $\lim_{x\to\infty}(x)$ *LITTLE PIGS* DID GET A BIT WEIRD TOWARD THE END...

Q: Why can't you grow wheat in $\mathbb{Z}/6\mathbb{Z}$?
A: It's not a field. □

Q: Why did the mathematician name his dog Cauchy?
A: Because he left a residue at every pole. □

Q: What is the difference between a mathematician and a philosopher?
A: The mathematician only needs paper, pencil, and a trash bin for his work - the philosopher can do without the trash bin... □

A mathematician is asked by a friend who is a devout Christian: "Do you believe in one God?"
He answers: "Yes—up to isomorphism." □

Rational Elliptic Curves Constructed Around a Given Point

Dieter Fishbein

We examine the problem of constructing a rational elliptic curve with small coefficients around a given point. We establish an upper bound on the “size” of the smallest of such curves and describe heuristics addressing other theoretical questions related to the problem. We present an algorithm to generate a small curve given a point, where the point is likely to be a generator for the curve.

1 Preliminaries

An *elliptic curve* over $\mathbf{Q}$ is a smooth, projective algebraic curve of genus 1 having rational coefficients. For our purposes, it will be sufficient regard an elliptic curve as any non-singular curve that is bi-rationally equivalent to a a curve,

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$$

with a_i $\mathbf{Q}$. By two curves being *bi-rationally equivalent*, we mean that there exists a bijective mapping between them that maps rational points to rational points. One very interesting aspect of elliptic curves is that we can define an operation on rational points that turns the collection of rational points on a given curve into an abelian group. The group actually contains one other point, called *the point at infinity* denoted $\mathscr{O}$ which can be pictured to be lying in the direction of the positive y axis at an infinite distance away. Elliptic curves are best treated in the projective plane where one can define $\mathscr{O}$ rigorously, but an intuitive understanding will be sufficient for our purposes. We define the group operation below:

Definition. *To add P and Q, we construct a line through these two points. This line will always intersect the curve at a third point, $P * Q$. We construct another line through $P * Q$ and join it to $\mathscr{O}$. We take the third intersection of this line, $(P * Q) * \mathscr{O}$, and this represents the addition of the points P and Q. So we have, $P + Q = (P * Q) * \mathscr{O}$.*

The verification that this law turns the collection of rational points into a group is non-trivial, but is beyond the scope of this paper. According to the Mordell-Weil theorem, this group is finitely generated. The structure theorem for finitely generated abelian groups then tells us that the group of rational points will be isomorphic to a direct sum of a torsion-free abelian group and a finite abelian group. We call the dimension of the torsion-free summand, the *rank* of the curve. Since the group is finitely generated, in particular the torsion-free summand is also finitely generated. We call elements of the torsion-free summand, *points of infinite order* on the curve. We call each element of a generating set for the torsion-free summand, a *generator* of the curve. It is relatively rare to find rational elliptic curves of rank greater than 3, i.e, elliptic curves that have more than 3 generators.

2 Introduction

In this article, we wish to address an interesting theoretical and computational question that has not, to my knowledge, been discussed before. Given a rational point in $\mathbf{R}^2$, (x, y), what is the “smallest” non-singular elliptic curve, E, that we can construct such that (x, y) is a point on E. When considering this problem, certain questions come to mind. Namely, how does one define the notion of the “size” of a curve? Can one give an a priori upper bound for the size of the smallest elliptic curve through a given point? Is there a “typical” size for such a curve? We begin by discussing these questions and attempting to answer some of them. We then consider the problem of actually computing the smallest elliptic curve through a given point and present an algorithm that has had some success in doing so. Lastly, we describe methods of choosing (x, y) in order to increase the likelihood of being able to construct a small elliptic curve around it and present examples of such points and corresponding curves. For most of these examples, (x, y) is likely a generator for the group of rational points on the curve.

2.1 Definitions

We wish to have some quantitative measure of the size’ of an elliptic curve. What we want to capture by our definition is a rough estimate of the total number of digits in both the numerators and denominators of the coefficients of the curve in long Weierstrass form. So it is natural to define the size of the curve as we do below.

Definition. *For, E, an elliptic curve over $\mathbf{Q}$, the* size *of E is $F(E) := \log_{10}\left(\prod_{a_i} num(a_i) denom(a_i) \right)$, where the product is taken over all non-zero coefficients of E in long Weierstrass form and $num(a_i)$ and $denom(a_i)$ denote the numerator and denominator of a_i respectively. .*

Similarly, we define the notion of the size of a point.

Definition. *For, $P = (\frac{a}{b}, \frac{c}{d})$, a rational point in $\mathbf{R}^2$ such that gcd(a,b)=gcd(c,d)=1, $\frac{a}{b} = 0$ and $\frac{c}{d} = 0$, the* size *of P is $F(P) := \log_{10}(\ abcd\ )$. If $\frac{a}{b} = 0$ and $\frac{c}{d} = 0$ (resp. $\frac{c}{d} = 0$ and $\frac{a}{b} = 0$) then we define the* size *of P as $F(P) := \log_{10}(\ cd\ )$ (resp. $F(P) := \log_{10}(\ ab\ )$. If both $\frac{a}{b} = \frac{c}{d} = 0$ we define the* size *of P to be 1.*

Throughout this article, the discussion of the size of curves or points of being large or small will refer to the definition above. We could have used a standard height function to measure the size of the point, however, defining the size in this way gives us a better handle on the complexity of the point.

Definition. *We define the* impressiveness *of a pair (E,P), where E is an elliptic curve and P, a point on E as, $I(E,P) := \frac{F(P)}{F(E)}$.*

Later, we will also want to describe how good certain examples of large points on small elliptic curves are. We use the notion of *impressiveness* to quantify this. It is a consequence of the group law on elliptic curves, that we can get points of arbitrarily large height on any elliptic curve of positive rank. By the *height* of a point, we mean $h(P) = h(x,y) = h(\frac{m}{n}, y) = max(\ m\ ,\ n\ )$ where $P = (x,y)$ and $x = \frac{m}{n}$. Thus, it does not make sense to talk about the impressiveness of large points on small curves in general. What we consider later is the impressiveness of examples where the point in question is likely a generator for the curve. For this case, we cannot find arbitrarily large points on arbitrarily small curves. This is because the collection of elliptic curves up to a given size is finite. Therefore, the collection of their generating points is also finite.

3 Theoretical Questions

We now wish to attempt to provide answers to the questions discussed in the introduction. In most cases we will only be able to provide heuristics and direction, rather than complete, rigorous results. We first give an upper bound for the smallest non-singular elliptic curve through a given point.

Proposition 1. *Given a point $(x_0, y_0) = (\frac{a}{b}, \frac{c}{d})$ with $a,b,c,d \quad \mathbf{Z}$. There exists a non-singular elliptic curve, E, passing through P, such that $F(E) \leq max(\log_{10}(\ a^2b^2\ ),$ $\log_{10}(\ (c^2b^3 - a^3d^2)(d^2b^3)\ ))$.*

Proof. We proceed constructively and divide the proof into three cases. First let $x_0 = y_0 = 0$. Then let $E : y^2 + xy + y = x^3 + x^2 + x$. Clearly, $(0,0)$ is a point on E. E is non-singular since the elliptic discriminant, Δ, is $\Delta = -83 = 0$. Also, $F(E) = \log_{10}(1) = 0$.

Secondly, let $y_0^2 = x_0^3$ with $x_0 = 0$ and $y_0 = 0$. Let $E : y^2 = x^3 + x^2 - a^2/b^2$. One can see that (x_0, y_0) is on E. Furthermore, $\Delta = \frac{a^2}{b^2}(64 - 432\frac{a^2}{b^2})$. So $\Delta = 0$ if and only if $\frac{a^2}{b^2} = x_0^2 = \frac{64}{432} = \frac{4}{27}$. Then $x_0 = \frac{2}{3\quad 3}$, which contradicts x_0 being rational. Hence $\Delta = 0$ and E is non-singular. Then, $F(E) = \log_{10}(a^2b^2)$.

Lastly, let $y_0^2 = x_0^3$. Then let $E : y^2 = x^3 + y_0^2 - x_0^3$. One can see that (x_0, y_0) is on E. Furthermore, $\Delta = -432(y_0^2 - x_0^3)^2 = 0$, so E is non-singular. Since $y^2 - x^3 = \frac{c^2b^3 - a^3d^2}{b^3d^2}$, $F(E) = \log_{10}(\ (c^2b^3 - a^3d^2)(b^3d^2)\ )$. □

The above proof manages to give us a reasonable upper bound on the size of the smallest elliptic curve through a given point. We will later discuss an algorithm to generate small elliptic curves around a given point. We calculated an upper bound for the smallest elliptic curve generated by this algorithm. However, it turned out that an upper bound based on the algorithm was more difficult to calculate than the above upper bound and very impractical.

3.1 *The Size of the Smallest Elliptic Curve Through a Given Point*

We would like to understand what the most likely size of a small curve around a large point is. Let $P = (x,y) = (\frac{a}{b}, \frac{c}{d})$ with $a,b,c,d \quad \mathbf{Z}$. Then, by proposition 1, there exists and elliptic curve, E, such that $F(E) \leq \max(\log_{10}(\ a^2b^2\ ),$ $\log_{10}(\ (c^2b^3 - a^3d^2)(d^2b^3)\ )) = k$. We consider the following sets where E is an elliptic curve with non-negative coefficients.

$$R_k := \#\ \ E\ \ F(E) \leq k$$

and,

$$L_k := R_k - R_{\frac{k}{10}}$$

Since $F(E)$ is approximately the total number of digits in the numerator and denominator of each a_i and there are 5 rational a_i's, leading to 10 integer parameters to define each curve, the number of elliptic curves in R_k is approximately the number of permutations of 10 non-negative integers that sum to a number less than or equal to k. Each of the non-negative integer parameters represents the size of either the numerator or denominator of some a_i. Using a counting argument, we then see that,

$$R_k = \sum_{i_{10}=0}^{k} \sum_{i_9=}^{k-i_{10}} \sum_{i_8=0}^{k-i_9} \sum_{i_7=0}^{k-i_8} \sum_{i_6=0}^{k-i_7} \sum_{i_5=0}^{k-i_6} \sum_{i_4=0}^{k-i_5} \sum_{i_3=0}^{k-i_4} \sum_{i_2=0}^{k-i_3} (i_2 + 1).$$

This is heuristic because we do not account for each of the a_i's to be in lowest form, so we end up counting some curves twice and we do not take into account the combinations of coefficients that lead to singular curves, so we count some curves that should be excluded from the set. Ultimately we will be concerned with the ratio of L_k to R_k and its asymptotic behaviour as $k \quad \infty$, so we are not extremely concerned with these inaccuracies.

Explicitly evaluating $R(k)$, we get,

$$R_k = \frac{9613}{1209600} k^{10} + \text{lower order terms} \tag{3.1}$$

One can see that reducing k by factor of 10 reduces $R(k)$ by approximately a factor of 10^{10}. This suggests that $\frac{L_k}{R_k}$ will often be close to 1. For examples, when $k = 100$, we get that $\frac{L_k}{R_k} = 0.9999999996$. Asymptotically, we get that,

$$\lim_{k \quad +\infty} \frac{L_k}{R_k} = \frac{9999999999}{10000000000}$$

This suggests that that a very high proportion of elliptic curves in R_k will also be in L_k. This implies that given a point, P, the smallest elliptic curve around P, E, will most often be in L_k. Further indicating that it would be quite exceptional to find examples of elliptic curves with large points such that the size of the elliptic curve is less than or equal to one tenth of the size of the bound given in proposition 1. This estimate is simply based on the distribution of elliptic curves of certain sizes and is far from rigorous.

3.2 The Number of Points Less Than a Given Size on Elliptic Curves Less Than a Given Size

We wish to provide a lower bound for the number of points less than a given size that occur on elliptic curves less than a given size.

Let,

$$S_k := \quad P = (x,y) \ h(x,y) \leq k \quad ,$$

where $h(x,y)$ is the height of the point (x,y), and,

$$T_m := \quad E \ F(E) \leq m \quad .$$

We wish to estimate a lower bound for the number of points from S_k that occur on curves in T_m. For a given elliptic curve, E, the number of rational points it contains of height less than k is roughly equal to $v_E \log(k)^{r_E}$ where v_E is the regulator of E and r_E is the rank of E. Our estimate becomes,

$$N = \sum_{E \quad T_m} v_E \log(k)^{r_E}.$$

We assume that half of the curves in T_m have rank 0 and half have rank 1. Although likely not the case, this assumption is consistent with Goldfeld's conjecture which asserts that the average rank of an elliptic curve is $\frac{1}{2}$ [4]. Since a curve of rank 0 always has $v_E = 1$, we get,

$$N \approx \sum_{E \quad T_m \ rank(E)=0} (1) + \sum_{E \quad T_m \ rank(E)=1} v_E \log(k) \tag{3.2}$$

$$\approx \sum_{k=1}^{\frac{R_m}{2}} (1) + \sum_{k=1}^{\frac{R_m}{2}} v_{E_k} \log(k) \tag{3.3}$$

$$= \frac{R_m}{2} + \sum_{k=1}^{\frac{R_m}{2}} v_{E_k} \log(k), \tag{3.4}$$

where R_m is the number of elliptic curves in T_m as estimated in section 3.1 and the sum in equation 3.4 is over curves of rank 1. For a curve of rank 1, v_E will be equal to the canonical height of the generator for the non-torsion subgroup of the group of rational points. So we get,

$$N \approx \frac{R_m}{2} + \sum_{k=1}^{\frac{R_m}{2}} \hat{h}(P_{E_k}) \log(k),$$

where P_E is the generator of E and $\hat{h}(P)$ is the canonical height of P. Lang's conjecture gives a lower bound on the canonical height of a point of infinite order over a number field [7]. In the case of the rational numbers, it tells us that there exists an absolute constant, $C_{\mathbf{Q}}$ such that given any point of infinite order, P, on an elliptic curve, E, we get,

$$\hat{h}(P) \geq C_{\mathbf{Q}} \log(\ \Delta_E \ ),$$

where Δ_E is the elliptic discriminant for E. This gives us,

$$N \gtrapprox \frac{R_m}{2} + \log(k) \sum_{k=1}^{\frac{R_m}{2}} C_{\mathbf{Q}} \log(\ \Delta_{E_k} \ ) \tag{3.5}$$

$$= \frac{R_m}{2} + \log(k) \frac{\sum_{k=1}^{\frac{R_m}{2}} \log(\ \Delta_{E_k} \ )}{\frac{R_m}{2}} \sum_{k=1}^{\frac{R_m}{2}} C_{\mathbf{Q}}. \tag{3.6}$$

Our hope here is that $\frac{\sum_{k=1}^{\frac{R_m}{2}} \log(\ \Delta_{E_k} \ )}{\frac{R_m}{2}} \geq 1$. In other words, that the absolute value of the average discriminant of the rank 1 elliptic curves in T_m is greater than e. This seems like it could be reasonable, but it is not immediately clear if it is true, or how to prove it if it is. I checked this value with the sum taken over all elliptic curves in T_m for $m = 0.1, 0.2, ..., 1.9, 2.0$. For these values of m, $\frac{\sum_{E \quad T_m} \log(\ \Delta_E \ )}{\frac{R_m}{2}}$ was always greater than 1. Moreover, the ratio appeared to be monotonically increasing with m. Thus, it may be reasonable to assume $\frac{\sum_{k=1}^{\frac{R_m}{2}} \log(\Delta_E)}{\frac{R_m}{2}} \geq 1$. This gives us,

$$\begin{aligned} N &\gtrapprox \frac{R_m}{2} + \log(k) \sum_{k=1}^{\frac{R_m}{2}} C_{\mathbf{Q}} && (3.7) \\ &= \frac{R_m}{2} + \frac{R_m}{2} \log(k) C_{\mathbf{Q}} && (3.8) \\ &= \frac{R_m}{2} (1 + \log(k) C_{\mathbf{Q}}) && (3.9) \end{aligned}$$

Various values for C_Q have been estimated, all are below 1. A fairly recent estimate by Elkies, puts $C_{\mathbf{Q}} \approx \frac{1}{25330}$ [3].

The above calculation suggests that N is increasing at least logarithmically as m is fixed and k increases. It also indicates that as m increases and k is fixed, N will increase in at least polynomial time.

4 Computations

Now that we have a better understanding of the theory regarding the size of the smallest elliptic curve through a given point and have a better idea on the amount of points of size less than fixed value on the collection of elliptic curves less than a certain size, we turn our attention to the problem of finding small elliptic curves with large generators. When picking a point at random on an elliptic curve, it is extremely likely to be a point of infinite order. This suggests that when constructing an elliptic curve around a given point, the given point is likely to be a point of infinite order on the constructed curve. We will present an algorithm used to construct small elliptic curves around a given point. After this, we will present other methods for generating good examples of small elliptic curves with large points which are likely generators.

4.1 An Algorithm to Compute a Small Elliptic Curve Around a Given Point

Here, we present an algorithm to compute an elliptic curve with small rational coefficients, E, based on a given point, $P = (x, y)$.

```
Algorithm 1: SMALLESTCURVE$(x, y)$
  Input: $y = \frac{a}{b}$ and $x = \frac{c}{d}$ such that a,b,c and d are
      integers and $d^3 = b^2$.
  Output: An array, $[a_1, a_2, a_3, a_4, a_6]$, of small
      coefficients for an elliptic curve in long
      Weierstrass form or nothing, if the algorithm
      fails.
  $C$   SMALLINTEGERRELATION($[-b(a^2 - c^3)$,
      $-acd^2, c^2db, -ad^3, cbd^2, b^3]$)
  if $C[0] = 0$ then
      return $[\frac{C[1]}{C[0]}, \frac{C[2]}{C[0]}, \frac{C[3]}{C[0]}, \frac{C[4]}{C[0]}, \frac{C[5]}{C[0]}]$
  else
      return null
  end if
```

Here, SMALLINTEGERRELATION($[x_1, ..., x_n]$) is a variation of the LLL algorithm developed by Hastad, Helfrich, Lagarias and Schnorr [6]. It returns a small integer relation, m, such that $m^{\mathrm{T}}[x_1, ..., x_n] = 0$. Similarly to the LLL algorithm, this integer relation is not guaranteed to be the smallest possible one. Nevertheless, it does satisfy the following bound,

$$m \leq w \; 2^{\frac{(n-2)}{2}}, \qquad (4.1)$$

where w is the shortest integer relation for $[x_1, ..., x_n]$. Note that equation 4.1 is essentially identical to the Lovász condition in the unmodified LLL algorithm.

The precondition that $b^3 = d^2$ is satisfied by all points on rational elliptic curves in Weierstrass form.

Proposition 2 (Correctness of Algorithm 1)**.** *Referring to the notation in Algorithm 1, let $P = (x, y)$ be a point. Then, $[\frac{C[1]}{C[0]}, \frac{C[2]}{C[0]}, \frac{C[3]}{C[0]}, \frac{C[4]}{C[0]}, \frac{C[5]}{C[0]}] = [a_1, a_2, a_3, a_4, a_6]$ are the coefficients for an elliptic curve in long Weierstrass form, E, which passes through P.*

Proof. Consider the equation that defines E,

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6.$$

By algebraic manipulations we obtain,

$$\begin{aligned} &bd^3(a^2 - a_6b^2) \\ &= b^2(a_2c^2db + a_4cbd^2 - a_1cad^2 - a_3ad^3 + c^3b). \end{aligned}$$

Recall $b^2 = d^3$. By using this relation and subtracting c^3b and adding a_6b^3 to both sides of the equation, we obtain,

$$\begin{aligned} &b(a^2 - c^3) \\ &= (a_2c^2db + a_4cbd^2 - a_1cad^2 - a_3ad^3 + a_6b^3) \end{aligned}$$

□

4.2 *Evidence the Algorithm is Optimal*

We would like to know whether Algorithm 1 is optimal. By optimal, we mean that for a given point, the algorithm produces the smallest possible curve around it. There are two possible ways that we have considered testing this. The first way, is to consider a curve with small coefficients and having $a_6 = 0$. The latter condition is to ensure $P = (0,0)$ is a point on the curve. Then, using the group law of the curve, add the point to itself 9 times. Since the height of a point grows approximately quadratically with the amount of times you add it to itself, this well generate a point of large height on the curve.

There are about 10^{16} curves where a_1 to a_5 are of height less than 100 and $a_6 = 0$. We examined 25874 randomly generated such curves. On average, the height of $9P$ was approximately 10^{162}. Heuristically, there should only be a small amount of curves having coefficients of small height that contain a point of large height. So, it is likely that the only curve having coefficients of height less than 100 that contains $9P$ is the original curve that we generated. If the algorithm, applied to $9P$ is able to recover this curve, then this is evidence that it is an optimal algorithm. In all 25,874 instances, the algorithm recovered the curve that was originally generated. Thus, this provides some numerical evidence that the algorithm is optimal.

Consider equation 4.1. Let $x = [-b(a^2 - c^3), ..., b^3]$. Let $m = [m_0, m_1, m_2, m_3, m_4, m_6]$ be the coefficients generated by SMALLINTEGERRELATION(x) at line 1 of Algorithm 1 for a given input $P = (x,y)$. Let a_1, a_2, a_3, a_4, and a_6 be the coefficients of the corresponding elliptic curve. We can show that m are likely the optimal integers. The denominator of each a_i will be a product of factors of m_0. Then $m_i = a_i m_0$ and $a_0 = 1$. Let $w = [w_0, w_1, w_2, w_3, w_4, w_6]$ be the shortest integer relation for x. Let a_1^*, a_2^*, a_3^*, a_4^*, and a_6^* be the coefficients for the elliptic curve corresponding to w. Then $w_i = a_i^* w_0$ and $a_0^* = 1$. The denominator of each a_i will be a product of factors of w_0. Recall equation 4.1 applied to w and m. We get,

$$m \quad \leq 4 \quad w \quad .$$

Applying the euclidean norm gives us,

$$\sqrt{\sum_i m_i^2} \leq 4 \sqrt{\sum_i (w_i)^2}$$

.

Squaring both sides, dividing by 16 and bringing $\frac{1}{16}$ into the sum on the left hand side gives us,

$$\sum_i \left(\frac{m_i}{4}\right)^2 \leq \sum_i (w_i)^2$$

Given a random integer greater than 10, decreasing it by $\frac{1}{4}$ has a 40 percent chance of decreasing the number by 1 digit. So, there is a 40 percent chance that one of the optimal components is as much as 1 digit less than one of the components given by SMALLINTEGERRELATION, a 16 percent chance two of the optimal components are up to 1 digit less, a less than 1 percent chance three of the optimal components are up to 1 digit less, etc. This shows us that it is likely that SMALLINTEGERRELATION(x) produces optimal components for the integer relation m.

While it's easy to analyze the optimality of the integer relation theoretically, it is much more difficult to analyze the optimality of the generated coefficients. Dividing each m_i by m_0 could have varying effects depending on the factors of m_0 relative to each m_i, it could decrease the height of the coefficients through cancellation or even increase the height. A similar phenomenon occurs with the optimal coefficients, $\frac{w_i}{w_0}$.

This evidence that algorithm 1 is optimal was developed before the upper bound on the size of the smallest elliptic curve through a given point in proposition 1 was calculated. We later showed that some of the curves produced by this algorithm did not satisfy the upper bound, showing that the algorithm is not be optimal. This makes sense, as intuitively, one would think that when using an integer relation algorithm as we did, we would only get optimal coefficients some of the time. Despite the numerical evidence to the contrary, there was little theoretical evidence to support the optimality of algorithm 1.

5 METHODS OF CHOOSING (x,y) TO PRODUCE SMALL ELLIPTIC CURVES USING ALGORITHM

Despite algorithm 1 not being optimal, we had some success using it to produce good examples of small curves with large points. These examples would not be of interest to us, if it was not for the tendency of the point to be a generator of the curve. Before we begin, it is useful to have a measurement of how impressive' an example is.

We define an example to be *impressive* if $I(E,(x,y)) \geq 1$. The heuristics presented in section 3.1 suggest that it may be appropriate to look at the difference in size of the generated curve to the bound given by proposition 1 in order to asses impressiveness. Impressive examples could then be defined as curves having size less than one tenth of the upper bound given in 1 applied to their corresponding point. This may be a more appropriate way to determine impressiveness, but more work needs to be done to asses this.

In this section we will first present evidence as to why all examples we generated likely have the point as a generator of the curve constructed around it. We tried many methods of choosing (x,y) so that a small curve around (x,y) is computed by algorithm 1, we will describe three of the most successful ones. For each method, we will present the examples with the highest value of $I(E,(x,y))$.

5.1 Evidence of Points Being Generators

It is very difficult to calculate the generators of an arbitrary elliptic curve. There is a standard algorithm to do so, John Cremona's `mwrank` algorithm. However it is non-deterministic and the coefficients of the elliptic curve must be small or the curve must have a rational point of order 2 for it work reasonably quickly. Neither of these characteristics applied to our examples, so we had to employ an alternative method. We considered the reduction of E modulo p, $\tilde{E}$, for a given prime p and looked to see whether there was a point , Q $\tilde{E}$ such that $nQ = P$. What we hoped is that for each value of n, we could find some prime p, such that $\tilde{E}$ did not have a a point, Q, such that $nQ = P$. This gives us evidence that P is not a multiple of any other point on the curve. Assuming E is rank 1, this then gives us evidence that P is a generator. If E has rank greater than 1, then there is the possibility that P could be a linear combination of generators, hence this method does not provide strong evidence of P being a possible generator. We will refer to this method as the *reduction test*.

We applied the reduction method to all impressive examples that we will present. Since it is as difficult to calculate the rank as it is the generators of an elliptic curve, we calculated the parity of the curve instead. If the parity was even, then the curve was definitely not of rank 1 so we could not do any further analysis with the above method. If the curve had odd parity, we assumed the curve was of rank 1, since curves of rank ≥ 3 are quite rare. For the curves of odd parity, we applied the above method by searching for a prime within the first 100 primes and checking $n = 1,2...,30$. For 92 out of 109 impressive examples where the curve had odd parity, we could not find a prime, p, or a value of n such that there was a point Q in the reduction of the curve modulo p where $nQ = P$. This provides evidence that most of the constructed curves in our examples had the point it was constructed around as a generator.

5.2 Method I: Hall s Conjecture

Let $(x,y) = (\frac{a}{b}, \frac{c}{d})$ for a,b,c,d **Z**. For any point on an elliptic curve it is required that $b^3 = d^2$. This has the benefit of putting the relatively large x^3 and y^2 terms in the long Weierstrass equation under a common denominator. One of our first worthwhile strategies for producing small curves was to make $c^2 - a^3$ small, thus reducing the size of of the generally large term in the `smallIntegerRelation` step of algorithm 1. Unfortunately, $c^2 - a^3$ is generally very large. This is formalized by Hall's conjecture, below:

Conjecture 1 ([5]). There exists a constant, $K(a) < 1$, depending on a, such that $K(a)$ 1 as a ∞ such that for all a,c **Z**, we have $K(a)$ $\overline{a} \leq$ $c^2 - a^3$.

Fortunately, Noam Elkies has computed a set of numbers (a,c) such that $\overline{a} >$ $c^2 - a^3$ [2]. These numbers are generally difficult to find. By using these values as the numerator of x and y respectively, and by trying various different numbers for b and d, we were able to generate some impressive examples.

The example with the highest value of $I(E,(x,y))$ given by this method was,

$$\begin{aligned}(a_1,a_2,a_3,a_4,a_5) &= \left(\frac{102797}{13724}, \frac{-12011}{3431}, \frac{-40}{3431}, 0, 0\right)\\ (x,y) &= \left(\frac{93844}{8581613769}, \frac{28748141}{794974954718853}\right)\\ F(E) &= 50.431085\\ I(E,(x,y)) &= 1.701445\\ U_1 &= 91.874877\\ \mathit{reduction} &= \mathit{True}\end{aligned}$$

where the a_i are the coefficients for E in long Weierstrass form, U_1 is the upper bound given by proposition 1, *reduction* is a boolean value that is *True* if E has parity 1 and passed the reduction test and is *False* if E has even parity or failed the reduction test. So, a value of *True* for *reduction* indicates that the point in the example is very likely to be a generator for its corresponding curve.

5.3 Method II: Only Using Algorithm

Using algorithm 1 and choosing $(x,y) = (\frac{a}{b}, \frac{c}{d})$ with $b^3 = d^2$ as $m_1 \leq a \leq n_1$, $m_2 \leq a \leq n_2$ $m_3 \leq a \leq n_3$ for m_i, n_i **Z** arbitrary, gave us some impressive examples. The one with the highest value of $I(E,(x,y))$ was,

$$\begin{aligned}(a_1,a_2,a_3,a_4,a_5) &= (0,-3057,-4192,870,2187)\\ (x,y) &= \left(\frac{9347693}{9345249},\frac{9347689}{28568426193}\right)\\ F(E) &= 30.824902\\ I(E,(x,y)) &= 2.343145\\ U_1 &= 83.647431\\ reduction &= False\end{aligned}$$

Here, the curve is of even parity, so the reduction test was not applied. It is significant that each of the coefficients of the curve are integers. This means that in the `smallIntegerRelation` step of the algorithm, the first of the 6 integers it generated divided each of the other 5.

5.4 Method III: Choosing a, b and c Close Together

We noticed that for $(x,y) = (\frac{a}{b},\frac{c}{d})$, many impressive examples had a, b and c close together. We choose $m_1 \leq a \leq n_1$ and then chose b and c such that $b-a \ \leq K$ and $b-c \ \leq K$ for some K such that $K < a$ and m and n arbitrary integers with $m \leq n$. Generally, K was chosen to be around one tenth of the size of a. As always, we have the condition that $b^3 = d^2$. The example with the highest value of $I(E,(x,y))$ was,

$$\begin{aligned}(a_1,a_2,a_3,a_4,a_5) &= \left(\frac{-4}{25},\frac{-511}{400},0,\frac{1}{16},0\right)\\ (x,y) &= \left(\frac{1000000}{815409},\frac{900250}{736314327}\right)\\ F(E) &= 19.605593\\ I(E,(x,y)) &= 3.139642\\ U_1 &= 71.202379\\ reduction &= False\end{aligned}$$

6 Conclusion

The theoretical results presented provide some framework to the question of finding small curves around given points. By establishing an upper bound on the smallest curve, and discussing other theoretical questions, we were able to give this problem some definition. Since we can get arbitrarily large points on any elliptic curve, this problem is only of interest if the point we construct the curve around has a chance of being a generator; somehow, this seems to have occurred frequently for our examples. More work needs to be done to understand this phenomenon. Furthermore, there is much more theoretical work that needs to be done to define this problem better. Specifically, it would be valuable to rigorously establish the "typical" size of the smallest elliptic curve around a given point. The computational aspect of this problem also has room for further research. Developing an optimal algorithm, and improving methods of choosing (x,y) so that a smaller curve can fit around it, would lead to more impressive examples. These computational aspects are very subtle problems and lend themselves to generalization. In particular, the problem of finding a small curve around a given point is very similar to finding a rational relation between an arbitrary set of numbers. Considerable work has been done on the problem of finding an integer relation, but this particular generalization has not been as well studied.

Acknowledgements: I would like to thank Henri Darmon for introducing me to this problem and for his help, guidance and financial support while working on it during the summer of 2011.

References

[1] Cremona, J.. mwrank and related programs for elliptic curves over **Q**. http://www.maths.nott.ac.uk/personal/jec/mwrank/, 2011.

[2] Elkies, N.. List of integers x, y with $x < 10^{18}$, $0 < x^3 - y^2 < x^{\frac{1}{2}}$. http://www.math.harvard.edu/ elkies/hall.html, 2011.

[3] Elkies, N.. Points of Low Height on Elliptic Curves and Surfaces I: Elliptic surfaces over $\mathbf{P_1}$ with small d. In "Algorithmic Number Theory," (F. Hess, S. Pauli and M. Pohst, eds.). Berlin: Springer Verlag, 2006.

[4] Goldfeld, D.. Conjectures on elliptic curves over quadratic fields. In "Number Theory Carbondale 1979," (M. Nathanson, ed). Carbondale: Springer, Berlin, 1979.

[5] Hall, M.. The Diophantine Equation $x^3 - y^2 = k$. In "Computers in Number Theory: Symposium Proceedings," (A.O.L. Atkin, B.J. Birch, eds.). Oxford: Academic Press Inc., 1971.

[6] Hastad, Helfrich, Lagarias and Schnorr. Polynomial Time Algorithms for Finding Integer Relations. In "STACS 86: 3rd Annual Symposium on Theoretical Aspects of Computer Science," Carbondale: Springer, 1979., 108-118.

[7] Hindry, M., Silverman, J.H. The canonical height and integral points on elliptic curves. Inventiones Mathematicae 93 (1988), 419-450.

DON'T PANIC: A CRASH COURSE IN SET THEORY FOR AN INCOMING U1.

Benjamin Lewis

The motivation for this article arises from the relative obscurity of set theory for most incoming U1 students, and its inversely proportionate importance in the study of Algebra and Analysis at the university level. As such, since naïve set theory is grasped rapidly, and leads naturally into axiomatic systems, some of the most relevant points of modern set theory are laid out here for any incoming undergraduates who care to read. Some practice in proof writing is also included, to get an idea of how to complete deductive proofs, which have often been left out of the curriculum.

1 A SET AND ITS ELEMENTS

One of the concepts at the core of modern mathematics starts with a. Really a is anything, but if you collect multiple as that are all similar in some aspect, you can call them a *set* A, where $a \quad A$ — a is in A, or is an *element* of A. For example, if we take the first ten integers, we would write that set as $\; 1,2,3,4,5,6,7,8,9,10 \;$. We might assign that set the name T, and then we can say that $4 \quad T$. The number of elements in a set A is written $\; A \;$. This doesn't mean that A needs to be finite though, noting that much of mathematics is based on a few very important infinite sets, at least a few of which you have probably already heard of.

Another important aspect to consider is the possibility of constructing another set that contains elements from a previously existing set. Now, suppose that we have a set $E = \; 2,4,6,8,10 \;$. Since $\; a \quad E, a \quad T$ (for each a in E, a is in T — the upside-down A is the symbol used to represent the term "for each", or sometimes "for all") we can say that E is a subset of T, which is written $E \subseteq T$. Since it's also possible in this instance to say that $\; a \quad T : a \quad E$, (there exists a in T such that a is not in E) we can say that $E \subset T$; the difference here is that there is no chance that $E = T$, whereas the first statement is less absolute — with the first, we say that it is a subset; with the second, a proper subset. A parallel that is instantly suggested is to ordering, with less-than and greater-than and their partial-ordering forms $(\leq, \geq)$.

I alluded before to infinite sets; this is as good a place to introduce them as any other, since they are key to our study of numbers and functions. We begin with the set of all natural numbers, $\mathbb{N}$; this set is easily constructed as a consideration of anything that can be counted in the real world. As such, it is a set of all the positive integers, beginning with 1. To the natural numbers we add 0, forming the set $\mathbb{N}_0$. The next extension is to the integers, which may be thought of as the following, using set definition: $\mathbb{Z} = \; p : p \quad \mathbb{N}_0 \quad -p \quad \mathbb{N} \;$, that is, p is in $\mathbb{N}_0$ or $-p$ is in $\mathbb{N}$. The symbol is the logical term or, and is true if either or both of its elements is true. The notation used here is called *set definition* and is a short way of describing a general rule which defines all elements of a set. From the integers we describe the rationals, $\mathbb{Q} = \; p/q : p,q \quad \mathbb{Z} \quad q = 0 \;$; the rationals are, of course, all numbers which may be formed from the quotient of two integers p and q, and ( ) given that $q = 0$.

This is a good place to pause and notice something interesting; the rationals are an infinite set, and they are *everywhere dense*, that is to say, there is always an infinite number of rationals between any two rationals; however, they aren't complete; some numbers which are irrational include $\overline{2}$, ϕ, π, e, $\overline{5}$, etc. Although we may find a rational number that is arbitrarily close to any of these numbers, it will never be equal to that number; as such, we say that the rationals are not continuous, and therefore use the real numbers, $\mathbb{R}$, to fill in the cracks.

The next natural extension develops from the question, "What is the square root of negative one?" This seems absurd at first glance, but the definition of i, the imaginary number, opened the entire field of complex analysis, and has implications across electromagnetism (including everyday applications). So, defining $i^2 = -1$, we introduce the set $\mathbb{C} = \; a + bi : a,b \quad \mathbb{R}, i^2 = -1 \;$. Note that where $b = 0$, this set reduces to the real numbers.

Stepping back for a moment, it is a perfect moment to apply set relations, and see the following:

$$\mathbb{N} \subset \mathbb{N}_0 \subset \mathbb{Z} \subset \mathbb{Q} \subset \mathbb{R} \subset \mathbb{C}$$

2 SET OPERATIONS: HOW IS THIS THING LIKE ANOTHER?

As we have defined sets and subsets, one might consider what may be done with these sets; they are, after all, in many cases abstract concepts rather than numbers. There are operators that work on sets; all of the ones we consider here are binary (one may be considered to be unary; however, it always acts in relation to two sets. More on that later.)

The first operation to consider is the *intersection* of two sets, the set of elements shared between the two sets; using set definition notation, $A \setminus B$ (A intersect B) is the following: $A \setminus B = \quad x : x \quad A \quad x \quad B \quad$. Note that for logical-and to be true, both conditions must be met. The similarity between the intersection and logical-and signs works well to remember the requirements!

The next operation to consider is the *union* of two sets, all elements in either set: A union B may be written as the following: $A \quad B = \quad x : x \quad A \quad x \quad B \quad$. Again, the similarity between the set-theory and logical sign can be a strong mnemonic to remember how this set operation works.

Lastly, we have the *complement* of a set. Simply put, the complement is all elements that are not in the set, but are present in some other set. In the most abstract of cases, this other set is the set S, which is the universe of all possible elements. We write complement as $S - A = \quad x : x \quad S \quad x \quad A \quad$; it is alternately written $C_S(A)$ or $S \quad A$. In the case that we are looking at the universe of all elements as S, it can also be written $C(A)$ or A .

DeMorgan's Laws These laws relate to the interaction of set complements, where $A \subset S, B \subset S$:

$$C(A \quad B) = C(A) \setminus C(B)$$

$$C(A \setminus B) = C(A) \quad C(B)$$

. These follow from the definitions; $C(A \quad B) = \quad x : x \quad A \quad B \quad$ implies that if an element is in this complement, it is not in either A or B, therefore it is in the area of their complements that is overlapping; a similar logic applies to the second law, *mutadis mutandis*. (Incidentally, these have a direct mirror in logic; $\quad (p \quad q) = \quad p \quad \quad q$, and $\quad (p \quad q) = \quad p \quad \quad q$. (Margaris 71))

3 Products of sets

To begin the discussion of products of sets, we consider a motivating case; notably, plane geometry. To construct the *real plane*, we take the direct product $\mathbb{R} \times \mathbb{R}$; this is normally written $\mathbb{R}^2$, and in it may be drawn any plane shape; this product is called the Cartesian product, after René Descartes, whose geometry led to its development. More generally, the product of two sets A and B is a set of ordered pairs, $(a_i, b_j) : a_i \quad A, b_j \quad B$. It is possible for these sets to be anything; a favourite example is cards: ranking Ace as 1 up through King (13), we might show a standard playing card deck as the product of sets $S = \quad \bullet \, , \quad , | \, , \} \quad$ and $R = \quad 1,2,3,\ldots,12,13 \quad$; hence, the product of these sets is $S \times R = \quad (s,r) : s \quad S, r \quad R$ — some example elements would be $(\bullet\, ,1)$ and $(\quad ,11)$ (who, it is said, stole some tarts from $(\quad ,12)$.) Note, though, that $S \times R = R \times S$; although they would contain elements that are all the same size, the *order* would be different, making the elements different.

It should be noted that there are some key properties of products of sets; since for every element $a_i \quad A$, there are as many elements in $A \times B$ as there are $b_j \quad B$, $\quad A \times B \quad = \quad A \quad B \quad$. Notably, this means that if $A = \emptyset \quad B = \emptyset$, $A \times B = \emptyset$ as $\quad A \times B \quad = 0$. This carries over into products in another manner: unless $A = B$ or one or the other is the empty set, $A \times B = B \times A$, for reasons seen above. A and B *may* be of the same magnitude, but be different sets, so unless $\quad A \times B \quad = 0$, it cannot be taken as an indication of commutivity. Likewise, unless one of these conditions holds, $A \times (B \times C) = (A \times B) \times C$ (Cartesian products are not generally commutative nor associative).

Although the discussion here has been of products of two sets, that doesn't mean that Cartesian products are limited to two sets — one that we work in regularly is $\mathbb{R}^3$, real 3-space. This is extensible to $\mathbb{R}^n$, a given n-dimensional real space; in fact, any product of sets may be written

$$\prod_{i=0}^{n} X_i = \quad (x_0, x_1, \ldots, x_n) : x_i \quad X_i$$

(An index of 0 was used as an example here. Any index could be used, with a good reason.) When all X_i are identical, that product is often written X^n, as a particular n-dimensional space.

4 Indexed sets and their intersections and unions

It seems a natural extension of sets is to describe a *family* of sets; in this case, if we have a set X, we can define a family of subsets, $\quad X_i \quad _{i \quad I}$ where I is the indexing set, and $X_i = \quad x_{i_j} : x_{i_j} \quad X \quad$ are each *indexed sets*; as such, $X_i \subset X \quad i \quad I$; note that for $i, j \quad I$, most of the time $X_i = X_j$. The concept of indexed sets leads into an extension of the previous concepts of intersection and union.

Intersection of indexed sets The intersection of a family of indexed sets is taken over the whole family, that is to say, $X_0 \setminus X_1 \setminus \cdots \setminus X_n$; since this is clumsy notation, we write instead

$$\bigcap_{i \quad I} X_i.$$

This intersection has the property that

$$\bigcap_{i \quad I} X_i \subseteq X_i \quad i \quad I,$$

and the proof develops as follows: for any element $x_a \quad X_{i_1}$, if $x_a \quad X_i \;\; i \quad I$, then $x_a \quad \bigcap_{i \;\; I} X_i$; however, if there is an $x_b \quad X_{i_1} : x_b \quad X_{i_2}$, then $x_b \quad X_{i_1} \setminus X_{i_2}$, so $x_b \quad \bigcap_{i \;\; I} X_i$, and it is not possible for $\bigcap_{i \;\; I} X_i$ to be a superset of any X_i.

Union of indexed sets Similarly, to find the union of a family of indexed sets, the key is to find all elements in every indexed set:

$$\bigcup_{i \;\; I} X_i.$$

Compare now its property against the intersection, given that

$$\bigcup_{i \;\; I} X_i \supseteq X_i \;\; i \quad I,$$

which is much the opposite; the proof for this one is left to the reader, but it follows from a similar logic as the last one.

Cases where $I = \emptyset$ When one is indexing across the empty set, there are curious properties of these relations: (where S is the universe of the sets.)

$$\bigcup_{i \;\; \emptyset} X_i = \emptyset$$

$$\bigcap_{i \;\; \emptyset} X_i = S$$

DeMorgan's Laws It should be noted that DeMorgan's Laws apply over families of sets, in a similar manner to the original proofs. (The extensions are fairly elementary, and follow from the original proof. Have an exercise!)

5 Mapping sets to other sets

While sets are all well and good for making decks of cards and describing spaces that we think in, how can they be *applied*? That is where the mapping comes into focus. A *mapping*, what we also call a *function* in non-set theory parlance, is a way of taking an element from one set and, by transforming it in some fashion, attaches it to another element in another set, in a fashion which behaves similarly across elements in each set. For example, with two sets A and B, and a mapping f,

$$f : A \qquad B$$

$$f : a \qquad b$$

. There are two important properties that a function may have: if a function is *injective* (or one-to-one, in some texts) then for each $a \quad A \;\; !b \quad B : f(a) = b$. (There exists a *unique* $b \quad B$ such that $f(a) = b$.) The other important property is that f may be *surjective* (or onto.) If f is surjective, then $f(A) = B$; that is, there are no elements of B which are not the *image* of an element of a. A function which is both injective and surjective is called *bijective*.

As an example, $f : \mathbb{R} \qquad \mathbb{R}, y = x$ is an example of a bijective function, while if we define $f : \mathbb{R} \qquad \mathbb{R}, f(x) = e^x$, this function is injective but not surjective.

Note that this holds across products of sets, as well; if we define a function $f : \mathbb{R} \qquad \mathbb{R}^3, f : t \qquad (x,y,z)$ as the following,

$$\begin{pmatrix} f_1(t) \\ f_2(t) \\ f_3(t) \end{pmatrix} = \begin{pmatrix} 3\cos t \\ 3\sin t \\ 2t \end{pmatrix},$$

then this function is injective but not onto, *and* it maps from a one-dimensional space to a three-dimensional space. It is a small step to enhance this to n-dimensional spaces; try creating some functions that map from a given set to another set or product of sets!

6 References

Margaris, Angelo. *First Order Mathematical Logic*. New York, Dover. 1990.

Mendelson, Bert. *Introduction to Topology*. New York, Dover. 1990.

Jokes

Q: What is non-orientable and lives in the ocean?
A: Möbius Dick. □

"The number you have dialed is imaginary. Please, rotate your phone by 90 degrees and try again..." □

Interview with Professor Sergey Norin

Marie-Andrée B.Langlois

Professor Norin works in graph theory and combinatorics. He joined the McGill Mathematics Department this summer.

$\delta\varepsilon$: Tell us about your background both personal and academic:
I am from St. Petersburg. It is cold but not as cold as here. I did my undergraduate degree over there and afterwards I wasn't sure of what I wanted to do so I went to New Zealand for a year. I realized that there wasn't much math to do over there. Luckily, my old advisor was working in the United States so I went to work with him at Georgia Technology Institute in Atlanta. I obtained a PhD in Algorithms, Graph Theory and Combinatorics. After obtaining my degree I spent a year as a quantitative analyst. I quickly realized that working for a financial company wasn't for me. It was a really stressful environment and the job requires smart people but you don't necessarily use mathematics once you are working. So, I went back to academia and I prefer this environment. I prefer proving theorems rather than developing financial strategies. Once you have your proof, you know it is right and you have a permanent result. When finding a "good strategy" it is about 60%-70% "good" and it will only be useful for about a year. Research can also be stressful, it is very hard, but I think that it has a greater payoff in the end.

$\delta\varepsilon$: Why did you chose to study graph theory and combinatorics?
Since high school I knew that it was what I wanted to study. I did a lot of problem solving and I didn't like the idea that doing this was considered "useless" mathematics and was not the technique being taught. Combinatorics is a field that requires lots of thinking but much less background. You can understand really important proofs that have been discovered in the last thirty years, that stemmed from a beautiful idea, but that do not require a lot of mathematical knowledge to be understood. In my opinion, other branches of mathematics are detached from intuition, you must often assume theorems that you don't understand the proofs of in order to keep learning.

$\delta\varepsilon$: Do you have any computer science background?
I got my PhD through a program in joint mathematics and computer science, but I like to believe that what I do is purely mathematical.

$\delta\varepsilon$: Why did you decide to go back into academia after a year?
I knew finance wasn't for me and I had to go back quick enough to still have connections at universities. A lot of people who started at the same time as I did didn't stay long in finance. I spent a few years as a teaching assistant at Princeton and then I came to McGill in July.

$\delta\varepsilon$: Have you enjoyed McGill and Montreal so far?
I really love Montreal, it is a very cosmopolitan city and it has a European style to it. There is also extremely good food, I really like the Atwater market. I think that a certain city tends to attract a certain type of person. I feel that the people here are more relaxed and I really enjoy the Discrete Mathematics Group. I believe it's one of the strongest in the world and they are great people to work with.

$\delta\varepsilon$: What are you currently working on?
I am currently doing research on large discrete structures in order to describe what we can understand about them globally by looking only at local information. We can look at giant networks and sample random triples of nodes, then we must infer what the whole network looks like. Using statistics I try to explain from three nodes what characterizes a system as we let the number of nodes tend to infinity. We can also deduce similar things by looking at graphs. We can take a two-coloured cube and consider smaller subcubes to find the colouring of the larger one.

$\delta\varepsilon$: Do you think that mathematics is taught differently here than in Russia?
It is quite different here. In Russia, professors just give their classes and they don't care about being understood. It is more intense there and you learn a lot more but you might not remember much. Also, students do not choose their classes. They take common classes in their first couple of years and then they choose their area of study. However, even then they still do not choose their classes. Another thing is that all exams are oral. It's a good test to see if students understand but it is much harder psychologically.

How To Make Sense of Negative Probabilities

Samuel Perreault

Is it possible to toss a die for which some values have a "negative chance" of occurring? This is hard to imagine; however, Gábor J. Székely claims that there is a way to make sense of negative probabilites in his article *Half of a coin: Negative Probabilities* [Székely, 2005]. He is not the first person to introduce this idea: physicists such as [Dirac, 1942] and [Feynman, 1987] have done so in the past. In this article I will present some of the topics discussed in Székely's paper.

First of all, it is imperative to say that Székely does not claim it is possible to toss a die for which some values have a "negative chance" of occurring. To make sense of negative probabilities, he uses a half coin: an object with infinitely many sides numbered from 0 to infinity and for which we assign a negative probability to the faces with positive even numbers. This is a half coin in the sense that if we flip two half coins, then the sum of the outcomes is zero with a probability of $\frac{1}{2}$ and one with probability $\frac{1}{2}$, just as in the case of a regular fair coin (assuming, for instance, that 0 represents head and 1 represents tail.) For this to happen we first need to assign appropriate probabilities to each face.

The goal of the project is to construct a half coin which respects the case described above; namely, such that the sum of two half coin flips is 0 with probability $\frac{1}{2}$ and 1 with equal chances. Before attacking the half coin, a rough definition of key concepts and a quick analysis of the regular fair coin are necessary.

1 Concepts

We first define the probability of an event and generating function, the two main concepts used in the paper.

Formally, a probability function is defined on a sample space $(\Omega, \mathscr{S})$, which consists of:

(a) Ω, the set of all possible outcomes of the experiment

(b) $\mathscr{S}$, a σ-field of subsets of Ω.

Under these conditions, P is defined the following way:

(i) $P(A) \geq 0$ for all $A \quad \mathscr{S}$.

(ii) $P(\Omega) = 1$.

(iii) Let $\quad A_j \quad , A_j \quad \mathscr{S}$, $j = 1, 2, ...$, be a disjoint sequence of sets; that is, $A_j \bigcap A_k = \emptyset$ for $j = k$. Then we have that

$$P\left(\bigcup_{i=1}^{\infty} A_j\right) = \sum_{i=1}^{\infty} P(A_j)$$

However, for the purpose of this paper, the following characterization will suffice. $P(X = head)$ will represent the probability that the random variable X, which is the flip of a coin in this case, gives a head. The notation $P(X = 0)$ will be used to represent this case and $P(X = 1)$ will represent the case the flip gives a tail. Note that in the case of two flips, $P(X_1 = a, X_2 = b) = P(X_1 = a)P(X_2 = b)$. Also, $\sum_{i=0}^{\infty} P(X = i) = 1$ must be true. This is essentially equivalent to the statement: "There is 100% certainty that the coin flip will give *some* result". In the present case, $P(X = n) = 0$ for all $n \geq 2$, since a coin has only two faces.

The *generating function* of X consists of the sum

$$f(z) = \sum_n p_n z^n \ ,$$

where $p_n = P(X = n)$. In probability, the use of generating functions is common to gain insight on how the sequence of probabilities $P(X = n)$ behaves for all possible values of n. It allows one to use results for power series since $\sum_n p_n = 1 < \infty$. This will turn out to be very useful.

For more information or more formal definitions of these concepts, refer to [Rohatgi and Ehsanes Saleh, 2001].

2 The fair coin

Suppose X is a regular fair coin, then

$$\begin{cases} P(X = 0) = \frac{1}{2} \\ P(X = 1) = \frac{1}{2} \\ P(X = n; n = 0, 1) = 0 \ . \end{cases}$$

In the present case, the generating function f of X is found from computing the finite series. We get that $f(z) = 1/2 + z/2$ and so $f(1) = 1$. This value of $f(1)$ is precisely what we would expect since $z = 1$ implies f is simply the sum of all probabilities.

3 Half of a coin

In the case of the half coin, we need

$$\sum_n p_n = 1 \text{ and } \sum_n \quad p_n \quad < \infty$$

in order to have everything well-defined and to work with power series. The probability that our half coin takes the value k is p_k, but note that interpreted as a classical random variable this probability would be $p_k\ /\sum_n\ p_n$ since negative probabilities are typically not allowed. [Feller, 1968] showed that to get the generating function of the sum of two independent random variables, one needs to multiply the two original ones. Using the definition of the half coin (the sum of two flips is one) and the previous fact, it seems plausible to set

$$\sqrt{\frac{1+z}{2}} = \sum_{n}^{\infty} p_n z^n$$

as the generating function of the half coin. The generating function of the sum of two independent flips of a half coin is then the same as the generating function of a flip of a regular coin. Applying the binomial theorem gives

$$\sqrt{\frac{1+z}{2}} = \frac{1}{\overline{2}} \sum_{n}^{\infty} \binom{1/2}{n} z^n$$

It turns out that something interesting happens here. The sequence of numbers 1, 1, 2, 5, 14, 42, 132, 429,... defined by

$$C_n = \frac{\binom{2n}{n}}{n+1}, \qquad n = 0, 1, ...$$

(where C stands for Catalan) allows one to rearrange the terms in the following way:

$$\begin{aligned}\binom{1/2}{n} &= \frac{(1/2)(-1/2)(-3/2)\cdots(-(2n-1)/2)}{n!} \\ &= \frac{(-1)^{n-1}2C_{n-1}}{4^n}\ .\end{aligned}$$

Hence, for $n = 1, 2, \ldots$, we get $p_n = (-1)^{n-1}\ \overline{2}\frac{C_{n-1}}{4^n}$, where we define $C_{-1} := -\frac{1}{2}$.

Does this satisfy the required conditions that $\sum_n p_n = 1$ and $\sum_n\ p_n\ < \infty$? The formula $\sqrt{\frac{1+z}{2}} = \sum_n^{\infty} p_n z^n$ with $z = 1$ and $z = -1$ confirms that it does. The first condition is satisfied since

$$1 = \sum_{n=0}^{\infty} p_n\ .$$

To confirm that the second condition is satisfied, note that

$$0 = \sum_{n=0}^{\infty} (-1)^n p_n$$

implies that

$$p_0 = -\sum_{n=1}^{\infty} (-1)^n p_n\ .$$

Now, since $p_n < 0$ for all even n and $(-1)^n$ is negative for all odd n, we have that

$$p_0 = \sum_{n=1}^{\infty}\ p_n$$

Therefore,

$$\sum_{n=0}^{\infty}\ p_n\ = 1/\ \ \overline{2} + 1/\ \ \overline{2} = \ \ \overline{2} < \infty\ ,$$

and the second requirement is satisfied.

So the half coin is well-defined, and the last thing to verify is that it respects the definition of half coin given at the beginning of the article, namely that there is equal probability for heads and for tails. The sum of two flips is 0 only if both flips give 0. Hence,

$$\begin{aligned}P(X+Y=0) &= P(X=0, Y=0) \\ &= P(X=0)P(Y=0) = p_0^2 = \frac{1}{2}\end{aligned}$$

The sum is 1 only when the first flip is 0 and the second 1 or vice versa. Therefore,

$$\begin{aligned}&P(X+Y=1) \\ &= P(X=1)P(Y=0) + P(X=0)P(Y=1) \\ &= p_1p_0 + p_0p_1 = 2p_1p_0 = 2\frac{1}{\overline{2}}\frac{\overline{2}}{4} = \frac{1}{2}\end{aligned}$$

Hence, it does respect the definition: there is a probability of $\frac{1}{2}$ of getting heads and $\frac{1}{2}$ for tails.

4 Fundamental Theorem

From the very definition of the half coin, someone familiar with probability theory and the following theorem could have seen that the example was meant to work out well.

Theorem 1. *For every generalized (in the sense of extended to signed probabilities) generating function f of a signed probability distribution there exist two probability distribution functions g and h of ordinary non-negative probability distributions such that the product $fg = h$. [Ruzsa and Székely, 1983] and [Ruzsa and Székely, 1988]*

Just as the generating function of the sum of two independent random variables is the product of each of the original ones, if f is the generating function of a half coin, then there exists two ordinary coins such that if we flip the half coin and one of the ordinary coins, their sum will be the result of the remaining coin.

5 Conclusion

After all, does it make sense to talk about negative probabilities? [Dirac, 1942] said once "Negative energies and probabilities should not be considered as nonsense. They are well-defined concepts mathematically, like a negative of money." In fact, the presentation above, according to Gábor Székely, justifies the use of negative probabilities in the same sense as we use negative numbers. It does not make sense in daily life to lose 80 pounds when one weighs 65 pounds. However, it does not prevent one from subtracting 80 from 65.

References

[Dirac, 1942] Dirac, P. A.M. (1942). The physical interpretation of quantum mechanics. *Proc. Roy. Soc. London. Ser. A.*, 180:1–40.

[Feller, 1968] Feller, W. (1968). *An introduction to probability theory and its applications. Vol. I.* Third edition. John Wiley & Sons Inc., New York.

[Feynman, 1987] Feynman, R.P. (1987). Negative probability. In *Quantum implications*, pages 235–248. Routledge & Kegan Paul, London.

[Rohatgi and Ehsanes Saleh, 2001] Rohatgi, V.K. and Ehsanes Saleh, A. K.M. (2001). *An introduction to probability and statistics*. Wiley Series in Probability and Statistics: Texts and References Section. Wiley-Interscience, New York, second edition.

[Ruzsa and Székely, 1983] Ruzsa, I.Z. and Székely, G.J. (1983). Convolution quotients of nonnegative functions. *Monatsh. Math.*, 95(3):235–239.

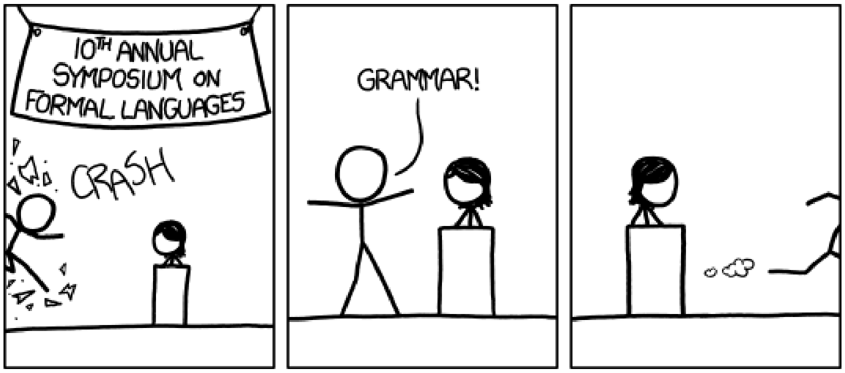
[Ruzsa and Székely, 1988] Ruzsa, I.Z. and Székely, G.J. (1988). *Algebraic probability theory*. Wiley Series in Probability and Mathematical Statistics: Probability and Mathematical Statistics. John Wiley & Sons Ltd., Chichester.

[Székely, 2005] Székely, G.J. (2005). Half of a coin: negative probabilities. *Wilmott Magazine*, pages 66–68.

Jokes

A mathematician going through the American border for a group theory conference is interrogated by the customs officer.
"What exactly is the purpose of your visit to the United States?"
After thinking a while of the most concise comprehensible answer, she responds simply "Free groups."
The officer replies "Exactly which groups do you want to liberate?" □

An engineer, a physicist and a mathematician are driving through the high country in Scotland. Atop a hill, they see a black sheep.
The engineer says: "All sheep are black!" The physicist says: "No, no, some sheep are black." The mathematician: "At least one sheep is black on at least one side." □



[audience looks around] What just happened?'
There must be some context we're missing.'

Certain Infinite Products with a View Toward Modular Forms

Catherine Hilgers

In this paper, we will discuss two infinite products, one studied by Bressoud and the other by Fine and Evans. These two infinite products are closely related to the famous Rogers–Ramanujan identities and the Rogers–Ramanujan continued fraction. We first revisit these two functions with a view toward modular forms, especially as quotients of Dedekind eta functions. Then we revisit one of the Rogers–Ramanujan forty identities in terms of these functions. Finally, we derive a congruence identity satisfied by the Rogers–Ramanujan continued fractions.

1 Introduction

The well known Rogers-Ramanujan functions are defined for $q < 1$, where here and throughout this paper, we always assume that $q := e^{2\pi iz}$ and $z \quad \mathscr{H}$, where $\mathscr{H}$ denotes the upper half plane. We have that

$$G(q) := \sum_{n=0}^{\infty} \frac{q^{n^2}}{(q;q)_n}$$

and

$$H(q) := \sum_{n=0}^{\infty} \frac{q^{n(n+1)}}{(q;q)_n}, \tag{1.1}$$

where for any complex number a, $(a;q)_0 = 1$ and $(a;q)_n = \prod_{k=1}^{n}(1-aq^{k-1})$ for $n \geq 1$.

These functions satisfy the famous Rogers-Ramanujan identities [17, pp. 214–215]

$$G(q) = \prod_{n=0}^{\infty} \frac{1}{(1-q^{5n+1})(1-q^{5n+4})},$$
$$H(q) = \prod_{n=0}^{\infty} \frac{1}{(1-q^{5n+2})(1-q^{5n+3})}. \tag{1.2}$$

At the end of his brief communication [16], [17, p. 231] announcing his proofs of the Rogers-Ramanujan identities (1.2), Ramanujan remarks, "I have now found an algebraic relation between $G(q)$ and $H(q)$, viz.:

$$H(q) \;\; G(q) \;\; ^{11} - q^2 G(q) \;\; H(q) \;\; ^{11}$$
$$= 1 + 11q \;\; G(q)H(q) \;\; ^{6}. \tag{1.3}$$

Each of these formulae is the simplest of a large class." In a manuscript of Ramanujan, published with his Lost Notebook [18], there are forty identities involving the Rogers-Ramanujan functions. After work of many people, only one of the forty identities has not been proven (see for details [4]).

In his thesis [5], Bressoud proved fifteen from the list of forty by using the following function:

$$g_{\alpha}^{(p,n)}(q)$$
$$= (q^{\alpha})^{\nu} \prod_{r=0}^{\infty} \frac{(1-(q^{\alpha})^{pr+\frac{p-2n+1}{2}})(1-(q^{\alpha})^{pr+\frac{p+2n-1}{2}})}{\prod_{k=1}^{p-1}(1-(q^{\alpha})^{pr+k})}, \tag{1.4}$$

where α is a natural number, p is an odd positive integer, n is an integer, and V_n is $\frac{12n^2-12n+3-p}{24p}$. Note that if $p = 5$, the functions $g_{\alpha}^{(5,1)}$ and $g_{\alpha}^{(5,2)}$ recover the Rogers-Ramanujan functions, namely

$$g_{\alpha}^{(5,1)}(q) = q^{\frac{-\alpha}{60}} G(q^{\alpha})$$

and

$$g_{\alpha}^{(5,2)}(q) = q^{\frac{11\alpha}{60}} H(q^{\alpha}). \tag{1.5}$$

To study congruence properties of the partition function, Atkin and Swinnerton-Dyer [2] introduced the following infinite product:

$$W_{\ell,j}(z) = q^{\frac{6j^2}{\ell}-j} \prod_{n=1}^{\infty} \frac{(1-q^{\ell(n-1)+4j})(1-q^{\ell n-4j})}{(1-q^{\ell(n-1)+2j})(1-q^{\ell n-2j})}, \tag{1.6}$$

where $1 \leq j \leq \frac{\ell-1}{2}$ and ℓ is an integer greater than or equal to 3. Later, Fine [9] proved that "cyclic" functions involving $W_{\ell,j}(z)$ satisfy invariant properties on certain level ℓ congruence subgroup, and Evans [8] considered certain combinations of $W_{\ell,j}(z)$ as modular functions on $\Gamma_1(\ell)$ (see 2 for the definition). Also the sum of functions $W_{\ell,j}(z)$ weighted by the partition function $p(\ell n + j)$ was studied in [6].

The goal of this paper is to revisit the infinite products $g_{\alpha}^{(p,j)}$ and $W_{p,j}(z)$ by using eta-quotients, and to recover the identity (1.3) by using the properties given by these two functions then derive a congruence identity satisfied by the Rogers-Ramanujan continued fraction. More specifically, in 2, we summarize some basic facts on modular forms. In 3, we examine $g_{\alpha}^{(p,j)}$ and $W_{p,j}(z)$ with eta-quotients. In 4, we recover the proof of the identity (1.3) by these two functions. Finally in 5 we derived the recurrence relation and the congruence identity satisfied by the Rogers-Ramanujan continued fraction.

2 Preliminaries

In this section, we follow the expositions of [15, 13]. Note that $\gamma := \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \quad \mathrm{SL}_2(\mathbb{Z})$ acts on the upper half plane $\mathscr{H}$ by the fractional linear transformation

$$\gamma z = \frac{az+b}{cz+d}.$$

Let N be a positive integer. Then the *l*evel N congruence subgroups $\Gamma_1(N)$ and $\Gamma_0(N)$ of $\mathrm{SL}_2(\mathbb{Z})$ are defined by

$$\Gamma_1(N) = \left\{\gamma \quad \mathrm{SL}_2(\mathbb{Z}) : \gamma \equiv \begin{pmatrix}1 & *\\ 0 & 1\end{pmatrix} \pmod{N}\right\}$$

$$\Gamma_0(N) = \left\{\gamma \quad \mathrm{SL}_2(\mathbb{Z}) : \gamma \equiv \begin{pmatrix}* & *\\ 0 & *\end{pmatrix} \pmod{N}\right\}.$$

We say that a meromorphic function f on $\mathscr{H}$ is a *m*eromorphic modular form of weight k for a congruence subgroup Γ if

$$f\Big(\frac{az+b}{cz+d}\Big) = (cz+d)^k f(z)$$

for all $z \quad \mathscr{H}$ and $\left(\begin{smallmatrix}a & b\\ c & d\end{smallmatrix}\right) \quad \Gamma$, and f is meromorphic at the cusps. If $k=0$, then f is known as a *modular function* on Γ. Further, we say that f is a *holomorphic modular form* if f is holomorphic on $\mathscr{H}$ and holomorphic at cusps. A holomorphic modular form is said to be a *cusp form* if it vanishes at the cusps of Γ. Denote by $M_k(\Gamma)$ (resp. $S_k(\Gamma)$) the space of holomorphic modular forms (resp. cusp forms) of weight k for Γ. Moreover denote by M_k^{∞} the space of weakly holomorphic modular forms on Γ (i.e. holomorphic on $\mathscr{H}$ but not necessarily at the cusps). If Γ has a cusp at ∞ with width h, then each $f \quad M_k^{\infty}(\Gamma)$ has a Fourier expansion at infinity:

$$f(z) = \sum_{n=n_0}^{\infty} a_n q_h^n, \quad q_h := e^{2\pi i z/h}, \quad n_0 \quad \mathbb{Z}. \tag{2.1}$$

Note that a modular form can be identified with its q-expansion. For example, the Dedekind-eta function $\eta(z)$ defined by

$$\eta(z) = q^{\frac{1}{24}} \prod_{n=1}^{\infty}(1-q^n) \tag{2.2}$$

is essentially a nonvanishing half integral weight modular form.

If χ is a Dirichlet character modulo N, we say that a form $f \quad M_k(\Gamma_1(N))$ has *Nebentypus character* χ if

$$f\Big(\frac{az+b}{cz+d}\Big) = \chi(d)(cz+d)^k f(z)$$

for all $z \quad \mathscr{H}$ and all $\left(\begin{smallmatrix}a & b\\ c & d\end{smallmatrix}\right) \quad \Gamma_0(N)$. The space of such modular forms is denoted by $M_k(\Gamma_0(N),\chi)$.

A function $f(z)$ of the form

$$f(z) = \prod_{\delta \; N} \eta(\delta z)^{r_\delta}$$

where $N \geq 1$ and each r_δ is an integer, is known as an *eta-quotient*. Recall the following general result of Gordon, Hughes, and Newman [11, 14] on eta-quotients:

Theorem 1. *If $f(z) = \prod_{\delta \; N} \eta(\delta z)^{r_\delta}$ is an eta-quotient with $k = \frac{1}{2}\sum_{\delta \; N} r_\delta \quad \mathbb{Z}$, with the following additional properties that*

$$\sum_{\delta \; N} \delta r_\delta \equiv 0 \pmod{24} \quad \textit{and} \quad \sum_{\delta \; N} \frac{N}{\delta} r_\delta \equiv 0 \pmod{24},$$

then $f(z)$ satisfies

$$f(\gamma z) = \chi(d)(cz+d)^k f(z)$$

for all $\gamma = \left(\begin{smallmatrix}a & b\\ c & d\end{smallmatrix}\right) \quad \Gamma_0(N)$. The character χ is defined by $\chi(d) = \big(\frac{(-1)^k s}{d}\big)$ and $s = \prod_{\delta \; N} \delta^{r_\delta}$.

Suppose that k is a positive integer and that $f(z)$ is an eta-quotient satisfying the conditions of Theorem 1. If $f(z)$ is holomorphic at all the cusps of $\Gamma_0(N)$, then $f(z) \quad M_k(\Gamma_0(N),\chi)$. Since $\eta(z)$ is analytic and never vanishes on $\mathscr{H}$, it suffices to check that the orders at the cusps are nonnegative. The following theorem is the necessary criterion for determining orders of an eta-quotient.

Theorem 2. *Let c, d and N be positive integers with $d \; N$ and $\gcd(c,d)=1$. If $f(z)$ is an eta-quotient satisfying the conditions of Theorem 1 for N, then the order of vanishing at the cusp $\frac{c}{d}$ is*

$$\frac{N}{24}\sum_{\delta \; N} \frac{\gcd(d,\delta)^2 r_\delta}{\gcd(d,\frac{N}{d})d\delta}.$$

3 The functions $g_\alpha^{(p,j)}(q)$ and $W_{p,j}(z)$

In this section, we revisit the functions $g_\alpha^{(p,j)}(q)$ and $W_{p,j}(z)$ with a view toward modular forms. We start this section by proving a basic result on result on $g_\alpha^{(p,j)}(q)$.

Proposition 3. *If $g_\alpha^{(p,n)}(q)$ is defined as in* (1.4)*, then we obtain that*

$$\prod_{j=1}^{\frac{p-1}{2}} g_\alpha^{(p,j)}(q) = \frac{\eta(\alpha p z)^{\frac{p-1}{2}-1}}{\eta(\alpha z)^{\frac{p-1}{2}-1}}, \tag{3.1}$$

where α is a natural number, and p is an odd positive integer.

Proof. From the definition on $g_\alpha^{(p,j)}(q)$, we have that

$$\begin{aligned}
&g_\alpha^{(p,1)} g_\alpha^{(p,2)} \cdots g_\alpha^{(p,\frac{p-1}{2})}\\
&= (q^\alpha)^{\sum_{n=1}^{\frac{p-1}{2}} V_n} \prod_{r=0}^{\infty} \frac{\prod_{k=1}^{p-1}(1-(q^\alpha)^{pr+k})}{\prod_{k=1}^{p-1}(1-(q^\alpha)^{pr+k})^{\frac{p-1}{2}}}\\
&= (q^\alpha)^{\sum_{n=1}^{\frac{p-1}{2}} V_n} \prod_{r=0}^{\infty} \frac{1}{\prod_{k=1}^{p-1}(1-(q^\alpha)^{pr+k})^{\frac{p-1}{2}-1}}
\end{aligned}$$

$$= (q^{\alpha})^{\Sigma_{n=1}^{\frac{p-1}{2}} V_n} \prod_{r=1}^{\infty} \frac{(1-(q^{\alpha})^{pr})^{\frac{p-1}{2}-1}}{(1-(q^{\alpha})^{r})^{\frac{p-1}{2}-1}}$$

$$= (q^{\alpha})^{\Sigma_{n=1}^{\frac{p-1}{2}} V_n} (q^{\alpha})^{\frac{-p^2+4p-3}{48}} \frac{\eta(\alpha pz)^{\frac{p-1}{2}-1}}{\eta(\alpha z)^{\frac{p-1}{2}-1}},$$

where in the last equality, we used the definition of $\eta(z)$. A simple calculation shows that

$$\sum_{n=1}^{\frac{p-1}{2}} (12n^2 - 12n + 3 - p) = \frac{p(p-1)(p-3)}{2}$$

and hence

$$(q^{\alpha})^{\frac{\Sigma_{n=1}^{\frac{p-1}{2}} 12n^2-12n+3-p}{24p}} = (q^{\alpha})^{\frac{p(p-1)(p-3)}{48p}} = (q^{\alpha})^{\frac{p^2-4p+3}{48}}$$

so we cancel out the powers of q^{α} in front of the eta quotient in the last equality. □

Note that the eta functions in the quotient (3.1) are taken to the same power. Thus one suspects that for certain p, it will be a weakly homomorphic modular function on the level p congruence subgroup with a character.

For convenience, for odd positive integer ℓ, denote by

$$f_{\ell,\alpha}(z) := \prod_{j=1}^{\frac{\ell-1}{2}} g_{\alpha}^{(\ell,j)}(q). \tag{3.2}$$

Theorem 4. *Let $p \geq 3$ be a prime satisfying*

$$(p-1)\left(\frac{p-1}{2}-1\right) \equiv 0 \pmod{24}. \tag{3.3}$$

Then $f_{p,1}(z)$ is a weakly homomorphic modular function on $\Gamma_0(p)$ such that

$$f_{p,1}\left(\frac{az+b}{cz+d}\right) = \chi(d) f_{p,1}(z), \quad \begin{pmatrix} a & b \\ c & d \end{pmatrix} \quad \Gamma_0(p), \tag{3.4}$$

where $\chi(d) = \left(\frac{s}{d}\right)$ and $s := p^{\frac{p-1}{2}-1}$.

Proof. We apply Theorem 1 for an odd prime p. Then $r_1 = \frac{1-p}{2} + 1$, and $r_p = \frac{p-1}{2} - 1$. So the weight k will be always zero. Now we want to check the conditions of Theorem 1, namely

$$p\left(\frac{1-p}{2}+1\right) + \frac{p-1}{2} - 1 =$$

$$-(p-1)\left(\frac{p-1}{2}-1\right) \equiv 0 \pmod{24}$$

which is our assumption on p. Therefore we have the transformation (3.4). Since $\eta(z)$ is analytic and is never zero on $\mathscr{H}$, we now need to check that $f_{p,1}(z)$ is meromorphic at the cusps of $\Gamma_0(p)$. Note that $\Gamma_0(p)$ has two cusps 0 and ∞.

By our assumption on p, let

$$(p-1)\left(\frac{p-1}{2}-1\right) = 24m$$

for some nonnegative integer m. Then by Theorem 2 it is easy to check that $f_{p,1}(z)$ has a pole of order m at the cusp at 0 and vanishes at ∞. Therefore $f_{p,1}(z)$ is a weakly holomorphic modular function on $\Gamma_0(p)$ associated with the character χ. □

One of the important results on $W_{\ell,j}(z)$ as an eta-quotient is due to Atkin and Swinnerton-Dyer [2].

Theorem 5 ([2]). *Let $\ell = 6\lambda \pm 1$ (not necessarily prime). Then*

$$(-1)^{\lambda} \frac{\eta(z/\ell)}{\eta(\ell z)} = 1 + \sum_{j=1}^{(\ell-1)/2} W_{\ell,j}(z), \tag{3.5}$$

where $\eta(z)$ is the Dedekind eta function.

The functions $W_{\ell,j}(z)$ were studied by Fine [9] with a theory of modular forms and some of the properties were discussed by Garvan [10] and Evans [8]. We close this section by observing that we can rewrite $W_{\ell,j}(z)$ as a quotient of $g_1^{(\ell,j)}(q)$ for any given odd integer $\ell > 1$. As an example, we have the following result.

Proposition 6. *Let $g_{\alpha}^{(\ell,j)}(q)$ and $W_{\ell,j}(\alpha z)$ be defined as in* (1.4) *and* (1.6) *respectively. Then for $\alpha \quad \mathbb{N}$ and ℓ an odd positive integer we have the following relations*

$$W_{\ell,j}(\alpha z) = \frac{g_{\alpha}^{(\ell,n)}(q)}{g_{\alpha}^{(\ell,m)}(q)}$$

for any combination of n and m, where

$$n \quad \left\{\frac{1}{2}(\ell-8j+1), \frac{1}{2}(-\ell+8j+1)\right\},$$

$$m \quad \left\{\frac{1}{2}(\ell-4j+1), \frac{1}{2}(-\ell+4j+1)\right\}.$$

Proof. We have that

$$W_{\ell,j}(\alpha z) =$$

$$(q^{\alpha})^{\frac{6j^2}{\ell}-j} \prod_{r=0}^{\infty} \frac{(1-(q^{\alpha})^{\ell r+4j})(1-(q^{\alpha})^{\ell r+\ell-4j})}{(1-(q^{\alpha})^{\ell r+2j})(1-(q^{\alpha})^{\ell r+\ell-2j})}.$$

Equating coefficients above, we obtain the following equalities to be satisfied:

$$\frac{n^2-n-m^2+m}{2} = 6j^2 - j\ell \qquad (3.6)$$

$$\begin{aligned} \ell r + \frac{\ell-2n+1}{2}, \ell r + \frac{\ell+2n-1}{2} &\quad , \\ = \ \ell r + 4j, \ell r + \ell - 4j &\quad , \qquad (3.7) \\ \ell r + \frac{\ell-2m+1}{2}, \ell r + \frac{\ell+2m-1}{2} &\quad , \\ = \ \ell r + 2j, \ell r + \ell - 2j &\quad . \qquad (3.8) \end{aligned}$$

Solving in (3.7) and (3.8), we obtain that

$$n \quad \left\{\frac{1}{2}(\ell-8j+1), \frac{1}{2}(-\ell+8j+1)\right\},$$

$$m \quad \left\{\frac{1}{2}(\ell-4j+1), \frac{1}{2}(-\ell+4j+1)\right\}.$$

Simple calculations show that these satisfy (3.6) in any combination. □

4 Recover identity (1.3) using $g_\alpha^{(\ell,j)}(q)$ and $W_{\ell,j}(z)$

In this section, we will sketch a proof of the identity (1.3). This identity is one of two identities stated by Ramanujan without proof [16] and it is the only identity among the forty in which powers of $G(q)$ or $H(q)$ appear. Many proofs of (1.3) are known (see [7] the first published proof, for example).

By a simple calculation, we rewrite the identity as follows:

Lemma 7. *The identity* (1.3) *is equivalent to*

$$\left(\frac{G(q)}{H(q)}\right)^5 - 11q - q^2\left(\frac{H(q)}{G(q)}\right)^5 = q\frac{\eta^6(z)}{\eta^6(5z)}. \quad (4.1)$$

Proof. From (1.4), we have that

$$g_1^{(5,1)}(q) = q^{\frac{-1}{60}} G(q) \quad \text{and} \quad g_1^{(5,2)}(q) = q^{\frac{11}{60}} H(q)$$

and hence

$$G(q)H(q) = q^{-1/6} g_1^{(5,1)} g_1^{(5,2)} .$$

Therefore by Theorem 3.1, we have that

$$G^6(q)H^6(q) = \frac{\eta^6(5z)}{q\eta^6(z)}.$$

Dividing both sides of (1.3) by $G^6(q)H^6(q)$, we obtain the result. □

One thus obtains the following identity.

Proposition 8. *We have that*

$$q^{-\frac{1}{5}}\frac{G(q)}{H(q)} - q^{\frac{1}{5}}\frac{H(q)}{G(q)} = 1 + \frac{\eta(z/5)}{\eta(5z)} . \qquad (4.2)$$

Proof. Setting $\ell = 5$ and $\lambda = 1$, it is immediate from Theorem 5 that

$$-\frac{\eta(z/5)}{\eta(5z)} = 1 + W_{5,1}(z) + W_{5,2}(z).$$

On the other hand, we have that

$$\begin{aligned} W_{5,1}(z) &= q^{\frac{1}{5}} \prod_{n=0}^{\infty} \frac{(1-q^{5n+4})(1-q^{5n+1})}{(1-q^{5n+2})(1-q^{5n+3})} \\ &= q^{\frac{1}{5}} \frac{H(q)}{G(q)}, \\ W_{5,2}(z) &= q^{\frac{14}{5}} \prod_{n=0}^{\infty} \frac{(1-q^{5n+8})(1-q^{5n-3})}{(1-q^{5n+4})(1-q^{5n+1})} \\ &= q^{\frac{14}{5}} \frac{(1-q^{-3})}{(1-q^3)} \prod_{n=0}^{\infty} \frac{(1-q^{5n+2})(1-q^{5n+3})}{(1-q^{5n+4})(1-q^{5n+1})} \\ &= -q^{-\frac{1}{5}} \frac{G(q)}{H(q)} \end{aligned}$$

which completes the proof. □

Berndt [3] proved Proposition 8 by using certain q series identity and then derived the identity (4.1) from (4.2) by rewriting (4.1) using the fifth root of unity and multiplying all five terms.

5 Congruence identity of the Rogers-Ramanujan continued fraction

The famous Rogers-Ramanujan continued fraction is defined by

$$R(q) = \frac{q^{1/5}}{1 + \frac{q}{1 + \frac{q^2}{1 + \cdots}}}, \qquad q < 1, \qquad (5.1)$$

which first appeared in a paper by Rogers [19]. Using the Rogers-Ramanujan identity (1.1), Rogers proved that

$$R(q) = q^{1/5}\frac{H(q)}{G(q)}. \qquad (5.2)$$

This was independently discovered by Ramanujan [1]. Therefore we can rewrite (4.2) as

$$\frac{1}{R(q)} - R(q) = 1 + \frac{\eta(z/5)}{\eta(5z)}. \qquad (5.3)$$

The first result is the recurrence formula on (5.3).

Theorem 9. *For any positive integer n, we have*

$$\begin{aligned}&\frac{1}{R^n(q)}+(-1)^nR^n(q)\\&=C_n+\left(1+\frac{\eta(z/5)}{\eta(5z)}\right)^n\\&-\sum_{k=1}^{n/2}(-1)^k\binom{n}{k}\left(\frac{1}{R^{n-2k}(q)}-R^{n-2k}(q)\right),\end{aligned}$$

where the constant $C_n=0$ if n is odd and $C_n=(-1)^{n/2+1}\binom{n}{n/2}$ if n is even.

Proof. From (5.3), we have that

$$\begin{aligned}&\left(1+\frac{\eta(z/5)}{\eta(5z)}\right)^n\\&=\left(\frac{1}{R(q)}-R(q)\right)^n\\&=\frac{1}{R^n(q)}+(-1)^nR^n(q)+\sum_{k=1}^{n-1}\binom{n}{k}\frac{(-1)^k}{R^{n-2k}(q)}.\end{aligned}$$

If n is odd,

$$\begin{aligned}&\sum_{k=1}^{n-1}\binom{n}{k}\frac{(-1)^k}{R^{n-2k}(q)}\\&=\sum_{k=1}^{\frac{n-1}{2}}\binom{n}{k}\frac{(-1)^k}{R^{n-2k}(q)}+\sum_{k=\frac{n-1}{2}+1}^{n-1}\binom{n}{k}\frac{(-1)^k}{R^{n-2k}(q)}\\&=\sum_{k=1}^{\frac{n-1}{2}}(-1)^k\binom{n}{k}\left(\frac{1}{R^{n-2k}(q)}-R^{n-2k}(q)\right).\end{aligned}$$

If n is even,

$$\begin{aligned}&\sum_{k=1}^{n-1}\binom{n}{k}\frac{(-1)^k}{R^{n-2k}(q)}\\&=\sum_{k=1}^{\frac{n}{2}-1}\binom{n}{k}\frac{(-1)^k}{R^{n-2k}(q)}+\sum_{k=\frac{n-1}{2}+1}^{n-1}\binom{n}{k}\frac{(-1)^k}{R^{n-2k}(q)}\\&+\binom{n}{n/2}(-1)^{\frac{n}{2}+1}\\&=\sum_{k=1}^{n/2}\binom{n}{k}(-1)^k\left(\frac{1}{R^{n-2k}(q)}-R^{n-2k}(q)\right)\\&+\binom{n}{n/2}(-1)^{\frac{n}{2}+1}.\end{aligned}$$

This completes the proof. □

Moreover, if n is prime, then we can obtain the congruence:

Corollary 10. *For a prime $p\geq 3$, one has*

$$\frac{1}{R^p(q)}-R^p(q)\equiv 1+\frac{\eta^p(z/5)}{\eta^p(5z)}\pmod{p}.$$

Proof. We have

$$\begin{aligned}&\frac{1}{R^p(q)}-R^p(q)=\sum_{j=0}^{p}\binom{p}{j}\left(\frac{\eta(z/5)}{\eta(5z)}\right)^j\\&-\sum_{j=1}^{p/2}(-1)^j\binom{p}{j}\left(\frac{1}{R^{p-2j}(q)}-R^{p-2j}(q)\right).\end{aligned}$$

Since we have $0<j<p$, $p\ \binom{p}{j}$ it follows that

$$\frac{1}{R^p(q)}-R^p(q)\equiv 1+\frac{\eta^p(z/5)}{\eta^p(5z)}\pmod{p}.$$

□

6 Acknowledgement

I would like to thank my supervisor Heekyoung Hahn for suggesting to me this project as a summer undergraduate research experience.

References

[1] G. E. Andrews, B. C. Berndt, L. Jacobsen, and R. L. Lamphere, *The Continued Fractions Found in the Unorganized Portions of Ramanujan s Notebooks*, Memoirs of the AMS, Providence, 1992.

[2] A. O. L. Atkin and P. Swinnerton-Dyer, *Some properties of partitions*, Proc. London Math. Soc. **3** No. 4 (1954), 84–106.

[3] B. C. Berndt, *Number theory in the spirit of Ramanujan*, Student Mathematical Library **34** AMS, Providence, 2006.

[4] B.C. Berndt, G. Choi, Y-S. Choi, H. Hahn, B. Yeap, A. J. Yee, H. Yesilyurt, J. Yi, *Ramanujan s forty identities for the Rogers-Ramanujan functions*, Memoirs of the AMS, **188** No. 880, Providence RI, 2007.

[5] D. Bressoud, *Proof and Generalization of Certain Identities Conjectured by Ramanujan*, Ph. D. Thesis, Temple University, 1977.

[6] H.H Chan, H. Hahn, R.P Lewis, and S.L. Tan, *New Ramanujan-Kolberg Type Partition Identities*, Mathematical Research Letters, **92** (2002), 801–811.

[7] H. B. C. Darling, *Proofs of certain identities and congruences enucated by S. Ramanujan*, Proc. London Math. Soc. (2) **19** (1921), 350–372.

[8] R. J. Evans, *Theta function idenities*, J. Math. Anal. Appl. **147** (1990), 97–121.

[9] N.J. Fine, *On a system of modular functions connected with the Ramanujan identities,* Tôhoku Math. J. (2) **8** (1956), 149-164

[10] F.G. Garvan, *Some congruences for partitions that are p-cores,* Proc. London Math. Soc. (3) **66** (1993), 492-520.

[11] B. Gordon and K. Hugues, *Multiplicative properties of η- products II*, A tribut to Emil Grosswald: Number theory and related analysis, Cont. Math. of the AMS **143** (1993), 415–430.

[12] H. Hahn, *On Zeros of Eisenstein Series for Genus Zero Fuchsian Groups*, (Rochester University, date unknown), pp. 1

[13] N. Koblitz, *Introduction to Elliptic Curves and Modular Forms*, Springer-Verlag, New York, 1984.

[14] M. Newman, *Construction and applications of certain class of modular functions*, Proc. London Math. Soc. (3) **7** (1956), 334–350.

[15] K. Ono, *The web of modularity: Arithmetic of the coefficients of modular forms and q-series*, CBMS No. 102, AMS, Providence, 2004.

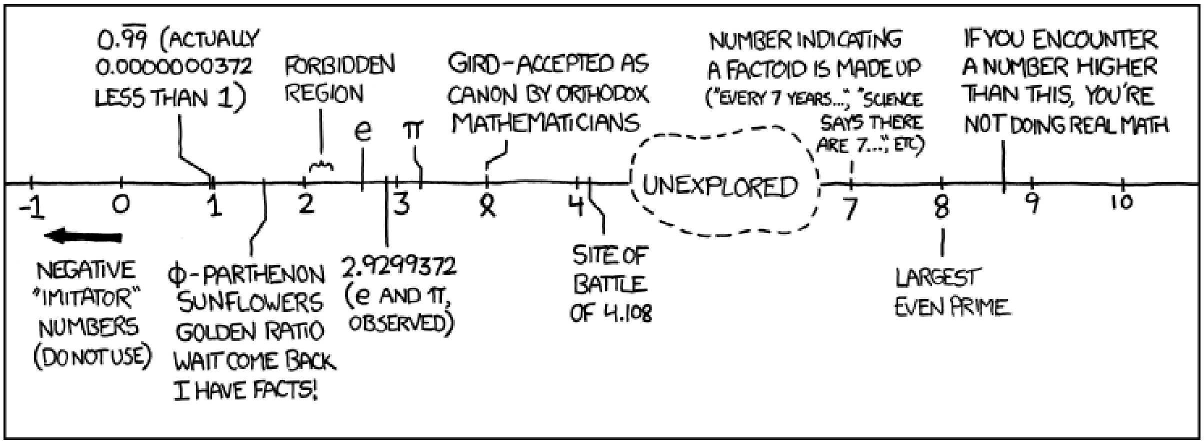
[16] S. Ramanujan, *Algebraic relations between certain infinite products*, Proc. London Math. Soc. **2** (1920), p. xviii.

[17] S. Ramanujan, *Collected Papers*, Cambridge University Press, Cambridge, 1927; reprinted by Chelsea, New York, 1962; reprinted by the American Mathematical Society, Providence, RI, 2000.

[18] S. Ramanujan, *The Lost Notebook and Other Unpublished Papers*, Narosa, New Delhi, 1988.

[19] L. J. Rogers, *Second memoir on the expansion of certain infinite products*, London. Math. Soc. **25** (1894), 318–343.

Jokes

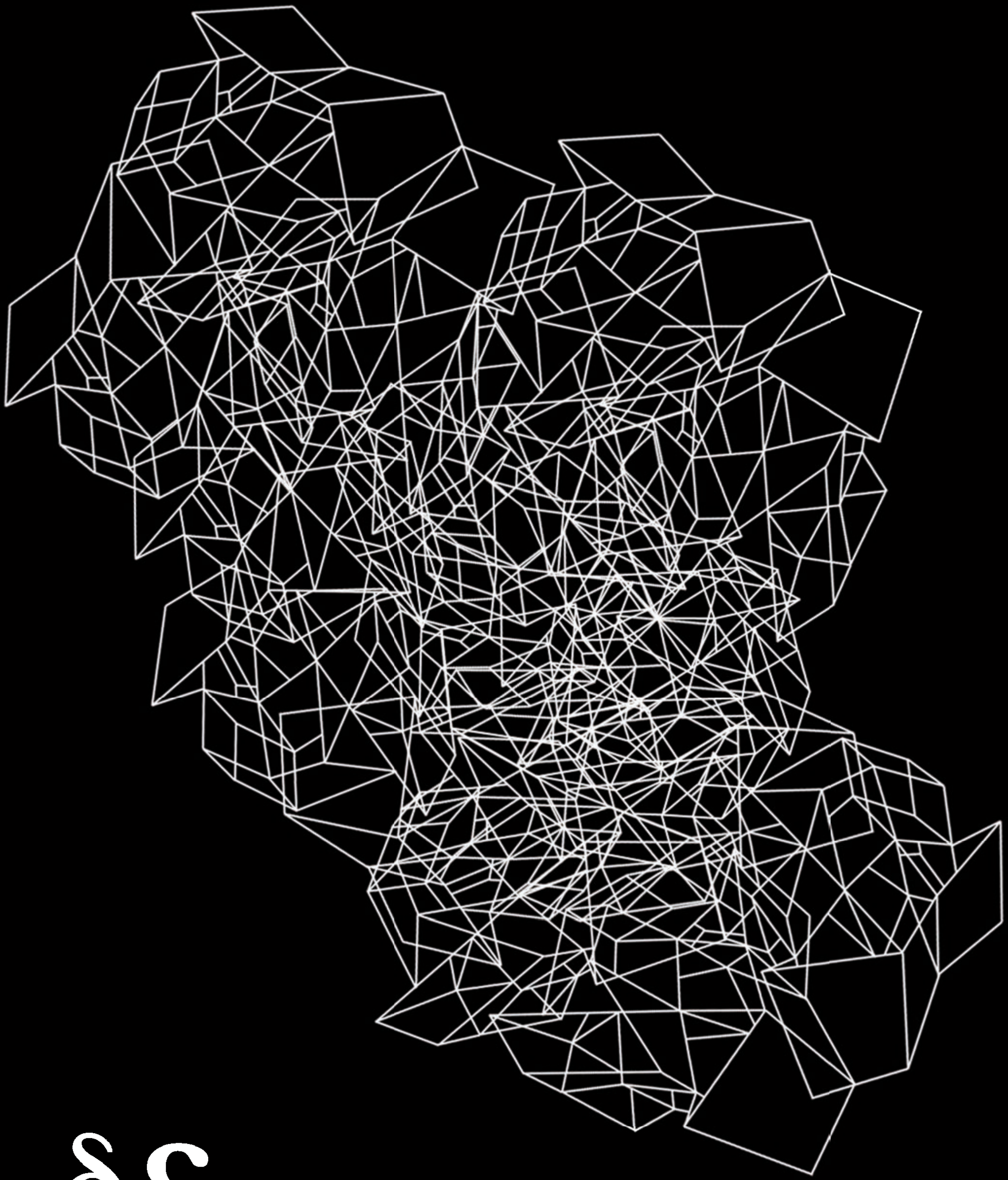

0.$\overline{99}$ (ACTUALLY 0.0000000372 LESS THAN 1)
FORBIDDEN REGION
e
π
GIRD-ACCEPTED AS CANON BY ORTHODOX MATHEMATICIANS
NUMBER INDICATING A FACTOID IS MADE UP ("EVERY 7 YEARS..."; "SCIENCE SAYS THERE ARE 7..."; ETC)
IF YOU ENCOUNTER A NUMBER HIGHER THAN THIS, YOU'RE NOT DOING REAL MATH
-1
0
1
2
3
ꝗ
4
UNEXPLORED
7
8
9
10
NEGATIVE "IMITATOR" NUMBERS (DO NOT USE)
ϕ-PARTHENON SUNFLOWERS GOLDEN RATIO WAIT COME BACK I HAVE FACTS!
2.9299372 (e AND π, OBSERVED)
SITE OF BATTLE OF 4.108
LARGEST EVEN PRIME

Q: How can you tell that Harvard was planned by a mathematician?
A: The div school is right next to the grad school. □

Q: What is gray and huge and has integer coefficients?
A: An elephantine equation. □

ACKNOWLEDGEMENTS

The production of this issue would not have been possible without our team of editors and peer reviewers. In addition, we would like to thank the Science Undergraduate Society as well as the Society of Undergraduate Mathematics Students for their generous financial support. We would like to thank Professor Robert Seiringer and Professor Sergey Norin for taking the time to speak to us and for all of the great advice that they have sent out to the undergraduates. We would like to thank François Séguin for his continued help with assembling the journal and cover. And finally, e would like to thank the contributors and the readers of this journal, without whom this publication would not exist.



δε.