McGill Undergraduate Mathematics Journal

the δelta εpsilon

Winter 2011

Fifth Issue

McGill

The δelta-εpsilon

McGill Undergraduate Mathematics Journal

Contents

Letter from the Editors

Five is a unique number for many reasons, such as the fact that it is the only prime with two distinct twins. Similarly, the fifth issue of the Delta-Epsilon is unique. Not only did we try to put together a balanced and interesting issue, but we also attempted to standardize the editing process. One of the great things about mathematics and science is that it is not necessary to reinvent the wheel; as Newton once said, “If I have seen further it is by standing on the shoulders of giants.” By facilitating communication between editorial teams from year to year, we ensure a successful δelta-εpsilon in the future.

The dual nature of our role gave this project its challenging flavor. We sincerely hope that we have succeeded in our task and our efforts will be appreciated in years to come. (To next year’s editors: If you read this while completely discouraged, keep on going! The fun is just ahead of you!)

The δelta-εpsilon provides not only an incredible opportunity for mathematics students to be introduced to the publishing process, but also to think, share, and contribute to the rest of our undergraduate mathematical community. In order to take advantage of this wonderful opportunity, we need contributions from you, our undergraduate readers. Your help is always integral to the existence of the δelta-εpsilon. We strongly encourage every one of you to participate in next year’s journal, and to make it the best issue yet. If you are interested, do not hesitate to contact us by e-mail, or to talk to us in person. We hope you enjoy the fifth issue of the δelta-εpsilon, and if you have questions or comments just let us know.

François Séguin
Executive Editor
The δelta-εpsilon Editing Team
thedeltaepsilon@gmail.com

Letter from SUMS

What would mathematics be without research. Mathematical tools are used on a daily basis by everyone, yet mathematical research is what allowed these tools and much better ones to be developed. Research is invaluable and mathematicians have to start doing it as early as possible. The undergraduate level is a great place to start.

Publishing its fifth issue, the δelta-εpsilon continues to be a high-quality journal that allows undergraduates to showcase their work, and share their love of various mathematical topics. The Society of Undergraduate Mathematics Students (SUMS) is proud to see the efforts of the mathematics undergraduates of McGill pay off in this beautiful journal.

On behalf of SUMS, congratulations to the δelta-εpsilon team!

Sincerely,

Cyndie Cottrell
SUMS President
(On behalf of SUMS council)
`http://sums.math.mcgill.ca/`

Perfectly Matched

Cyndie Cottrell

In [2], Elkies et al. presented domino shuffling on a family of finite subgraphs of the square lattice. This shuffling provides us with an easy way to count perfect matchings on the family of subgraphs. Here, we develop a similar shuffling on the hexagonal lattice superimposed on its dual graph. We define two families of finite subgraphs and count perfect matchings on these subgraphs. We will be reproving Ciucu's results from [1] regarding one family of subgraphs. The results regarding the second family of subgraphs follow from this new shuffling.

1 Introduction

A mathematical article unequivocally begins with definitions. The topic of enumerating perfect matchings, explored here, combines the field of graph theory with that of combinatorics. Yet, what is a perfect matching? What is a graph?

Definition. A *graph*, G, is a set of vertices and edges. A *matching* is a set of vertex-disjoint edges in G. A matching is *perfect* when the matching covers every single vertex in G.

In layman's terms, a graph consists of two things: dots, and lines connecting these dots. When we choose some of these lines and they do not share endpoints, we have a matching. This matching is perfect when it includes all of the dots on the graph. See Figure 1.

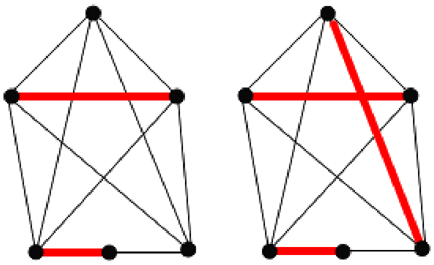


Figure 1: A matching on the left, and a perfect matching on the right

We are interested in counting the number of different perfect matchings in a graph. In 1992, Elkies et al. introduced a procedure called *domino shuffling* on the square lattice to count the number of perfect matchings on a family of graphs called *Aztec Diamonds* [2]. This shuffling inspired us to develop a similar shuffling algorithm to count the number of perfect matchings on certain subgraphs on the following more complicated lattice: the dP_3 lattice is a hexagonal lattice superimposed on its dual graph (see Figure 2).

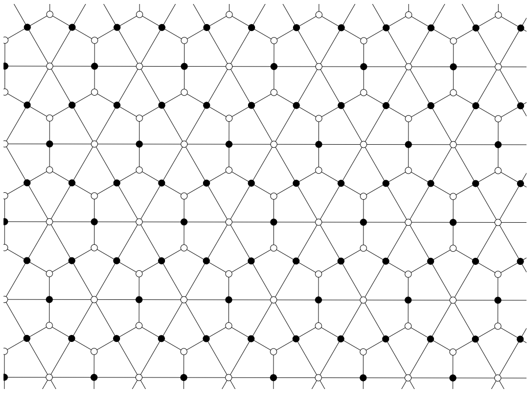


Figure 2: The dP_3 Lattice

We will study two different families of finite subgraphs of the lattice: whole diamonds and half diamonds. Let D_m be a diamond in one of these families with order m, for $m \in \frac{1}{2}\mathbb{N}$. If $m \in \mathbb{N}$, then D_m is a whole diamond. If $m + \frac{1}{2} \in \mathbb{N}$, then D_m is a half diamond. We will give a precise definition of both families of graphs in sections 4 and 5, but here we only give an intuitive definition. We cover the lattice with diamonds of order 1, as in Figure 3.

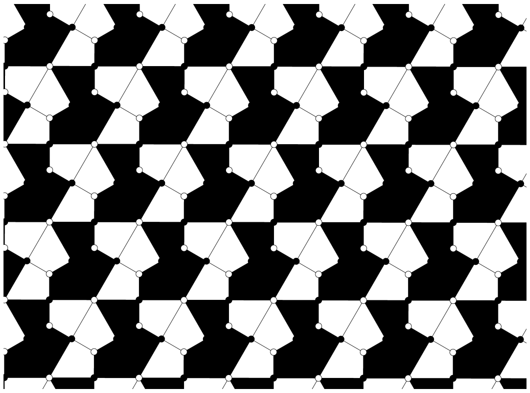


Figure 3: The dP_3 Lattice

We then select one diamond and call it the center. Let the ring of order m be the set of diamonds of order 1 directly surrounding the ring of order $m-1$, where the ring of order 1 is the center. Then, a whole diamond of order m is the set of rings of order n where n ranges from 1 to m.

The half diamonds of order m, defined as $D_{m+\frac{1}{2}}$, are more complicated. Here, we fix two diamonds of order 1 such that one is directly north of the other and call this the center, or the ring of order 1. Then, $D_{m+\frac{1}{2}}$ is the set of rings of order n where n ranges from 1 to m, as well as a few extra edges and vertices.

Now, our purpose here is to show the following theorem about the diamonds:

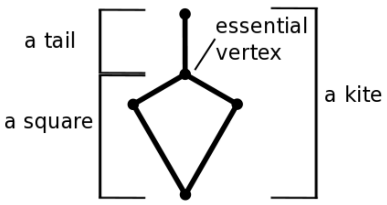
Theorem 1. The number of perfect matchings on a diamond of order m, where $n = \lfloor m \rfloor$, is

$$\begin{cases} 2^{n(n+1)} & m \in \mathbb{N} \\ 2^{(n+1)^2} & (m+\frac{1}{2}) \in \mathbb{N}. \end{cases}$$

The first part of the theorem related to the whole diamonds was proven by Ciucu in 2003 [1], while the second part is new. The proof is based on the application of our shuffling algorithm to a perfect matching on a diamond of order n. This will allow us to count the perfect matchings on a diamond of order $n+\frac{1}{2}$. Hence, by a simple induction we will show the theorem. Due to the tediousness of certain technical details, a mere sketch of the proof will be presented here. First, we give some more definitions.

2 More definitions

Definition. We define a *square* to be a face whose boundary has 4 edges. We also define the *tail* as the edge shown in the figure below; the tail depends on the orientation of the square. We define a *kite* to be a square and its tail. The *essential vertex* of a kite K is the unique vertex of K that is of degree 3.



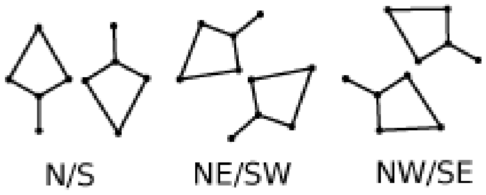


Figure 4: Orientations

This figure displays a N square. There are 6 possible orientations: N, S, NE, SE, NW, and SW. Further, when two squares have parallel tails, they have the same "pair of orientations". There are three such "pairs of orientations": N/S, NE/SW, and NW/SE. We will now abuse notation by using the term orientation in the place of the term pairs of orientations, unless clarity is absolutely necessary.

We define a *strip* to be a series of adjacent diamonds which share the same pair of orientations. Diamonds are adjacent if they share a common edge.

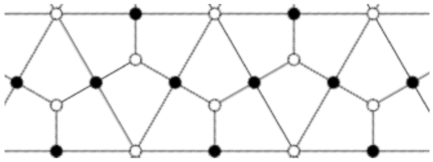


Figure 5: A strip

3 Double-Edge Contraction

Now, our shuffling is based on two graph transformations: urban renewal and double-edge contraction. Urban renewal is described by Propp in [3] and essentially consists of transforming the graph so that it has a predictable change in weight and number of perfect matchings. We describe double-edge contraction here. We consider a graph G, and will apply this transformation to a vertex b of degree 2. We can only apply double-edge contraction to vertices of degree 2 and obtain a new graph G'. We consider the two edges which share b as their endpoints and call them ab and bc. We will transform the graph by contracting the edges ab and bc into one vertex c'. We claim that G and G' have the same number of perfect matchings.

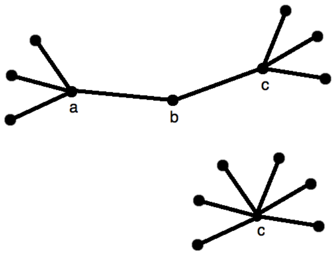


Figure 6: Double-Edge Contraction

We now show that our claim is true. Consider a perfect matching M on G. Then, since M is perfect, b must be matched. Hence, $ab \in M$ or $bc \in M$. Without loss of generality, let $ab \in M$. There must be some edge $c' \in M$ adjacent to c. When we apply double-edge contraction to the graph, a, b, and c become one vertex c'. Yet, all other edges are the same. We build a matching M' on the new graph G'. Then, let $M \backslash ab \in M'$, so that every vertex of G' remains matched. In particular, we know that a and b became a part of the vertex c and hence c' is in M'. So, M' is perfect, and for each matching M on G, we have exactly one matching of M' on G'. This process is completely reversible, so we have in fact given a bijection between matchings on G and matchings on G'.

4 The Diamonds

With a better understanding of matchings, we proceed to define the first family of subgraphs: whole diamonds. These diamonds are nontrivial to define rigorously, here we sketch an inductive construction. A diamond of order 1 is a subgraph of dP_3 consisting of three diamonds such that two are of the same pair of orientations, and the third has a different orientation. D_1s are shown below in Figure 7 and above in Figure 3. Here, we also define the *great vertex* of such a diamond to be its unique vertex of degree 4. The orientation of a diamond is defined as the orientation of the square which is the unique square of a pair of orientations. We use the convention that two diamonds which are reflections of each other along the vertical axis are the same.

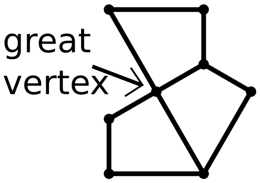
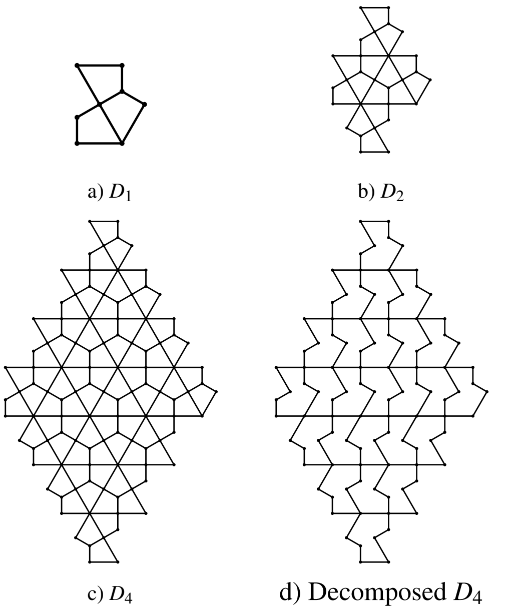


Figure 7: N D_1

Adjacent D_1s have at least one edge in common. We see that adjacent D_1s which lie on the same strip have opposite orientations. Further, D_1s that are adjacent, yet do not lie on the same strip, have opposite orientations. Here, we will solely be working with N D_1s and S D_1s. Now, given a diamond of order $n \in \mathbb{N}$ we build D_{n+1} by dividing D_n into D_1s. Then, we turn every N D_1 into a S D_1, and every N D_1 into a S D_1. We add a D_1 on the eastern boundary and one on the western boundary of each strip, as well as one above the northernmost, and one below the southernmost boundaries. We developed an intricate coordinate system to rigorously define these diamonds. Yet, rather than exploring this coordinate system, we proceed to consider the half diamonds.



a) D_1

b) D_2

c) D_4

d) Decomposed D_4

5 The Half Diamonds

In his work, Ciucu only mentioned whole diamonds [1]. We developed the half diamonds; they are closely related to the whole diamonds. These diamonds essentially consist of a northern half of D_n, and a 180° rotation of a northern half of D_n, plus two more squares, as shown in figure 8. Yet, $D_{\frac{1}{2}}$ does not agree directly with this definition as it is merely a N square.

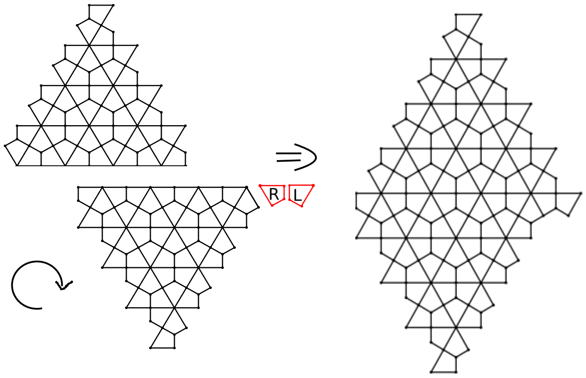


Figure 8: Constructing a half diamond

There exists an elaborate coordinate system very similar to that for the whole diamonds, yet we will not be using it here.

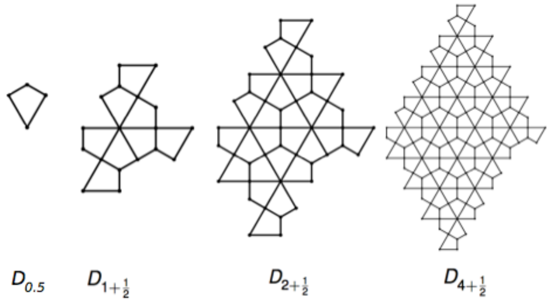


Figure 9: Some half diamonds

Now, using these diamonds' construction, it is simple but tedious to see that each subgraph has a perfect matching.

6 Counting edges

Having defined our diamonds, we proceed to count the number of edges in a perfect matching. Note that the number of edges in a perfect matching of any graph is half of the number of vertices. We will use this to see the effect of our shuffling algorithm on the number of edges in the matchings. We define the number of edges in a perfect matching on D_m to be M_m. We wish to show the following lemma by the number of vertices in D_m.

Lemma 2. Let $n = \lfloor m \rfloor$,

$$M_m = \begin{cases} n(3n+1) & m \in \mathbb{N} \\ 3n^2+4n+2 & (m+\frac{1}{2}) \in \mathbb{N}. \end{cases}$$

Proof. Now, let

- V be the number of vertices on D_m
- F be the number of faces on D_m
- E be the number of edges on D_m
- E_δ be the number of edges on the boundary of D_m
- E_{int} be the number of edges not on the boundary of D_m
- K be the number of squares on D_m.

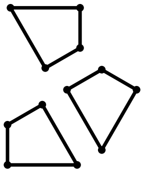


Figure 10: Decomposed diamond

We know that each square is associated with 4 edges and each edge in the interior of the diamond is associated with 2 distinct faces. Each edge on the boundary is associated to the infinite face and a face inside the subgraph, as shown in Figure 10. Hence, we have that $4K = 2E_{int} + E_\delta$. Further,

$$E = E_{int} + E_\delta \Rightarrow 4K = 2E - E_\delta \Rightarrow E = \frac{4K + E_\delta}{2}.$$

Now, we count the edges on the boundary of our diamond and find that

$$E_\delta = 16n - 8.$$

Next, we count the number of squares similarly by counting the number of diamonds on D_m and find that $K = 3(n^2 + (n-1)^2)$. Thus,

$$\begin{aligned} \Rightarrow E &= \frac{4 * 3(n^2+(n-1)^2) + 16n - 8}{2} \\ &= 6(n^2+(n-1)^2) + 8n - 4 \\ &= 6n^2 + 6(n-1)^2 + 8n - 4 \\ &= 12n^2 - 4n + 2. \end{aligned}$$

We use Euler's formula, and account for the infinite face by letting $F = K + 1$:

$$\begin{aligned} F + V &= E + 2 \\ (K+1) + V &= E + 2 \\ \Rightarrow V &= 1 + E - K \\ &= 1 + (12n^2 - 4n + 2) - (6n^2 - 6n + 3) \\ &= 6n^2 + 2n = 2n(3n+1), \\ \Rightarrow M_n &= n(3n+1). \end{aligned}$$

We do similar calculations for $m = n + \frac{1}{2}$ and find that

$$E_\delta = 16n + 2.$$

Also, there are $2n^2$ D_1s, and two extra squares in D_m $\Rightarrow K = 6n^2 + 2$.

We again use the above formula:

$$\begin{aligned} E &= \frac{4K + E_\delta}{2} \\ &= \frac{4(6n^2+2) + 16n + 2}{2} \\ &= 12n^2 + 4 + 8n + 1 \\ &= 12n^2 + 8n + 5, \end{aligned}$$

and since $V + F = E + 2$,

$$\begin{aligned} V &= E + 2 - F \\ &= 12n^2 + 8n + 5 + 2 - 6n^2 - 3 \\ &= 6n^2 + 8n + 4. \end{aligned}$$

Thus,

$$\Rightarrow M_m = \frac{V}{2} = 3n^2 + 4n + 2$$
$$= n(3n+1) + 3n + 2$$
$$= M_n + 3n + 2.$$

□

7 The Rules of Shuffling

We finally describe shuffling. It is the key to proving our main result. Given a perfect matching M on a diamond of order m, we let $n = \lfloor m \rfloor$. After applying shuffling to M, we will have a perfect matching M' on $D_{m+\frac{1}{2}}$. In essence, this algorithm comes from applying urban renewal and double-edge contraction to D_m.

This is how we shuffle:

1. Draw an oval surrounding the kite which has one and only one edge in the northernmost D_1.

2. Draw an oval surrounding all kites which have at least one edge in M and lie in the same pair of orientations as the kite circled in step 1.

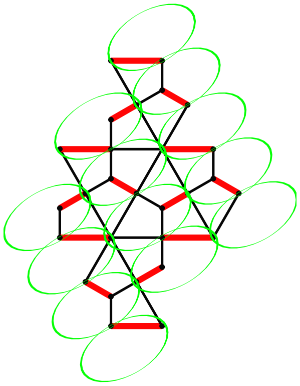


Figure 11: Steps 1 and 2

3. Ensure that the essential vertex of each circled kite is matched. If not, add the tail of that kite to M. We will add $2n+1$ tails.

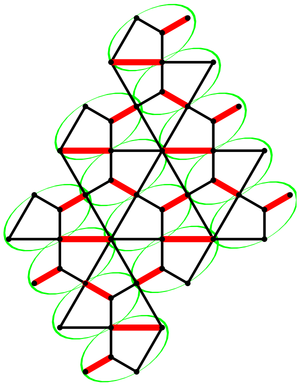


Figure 12: Step 3

4. Flip each kite in each oval so that it has an opposite orientation.

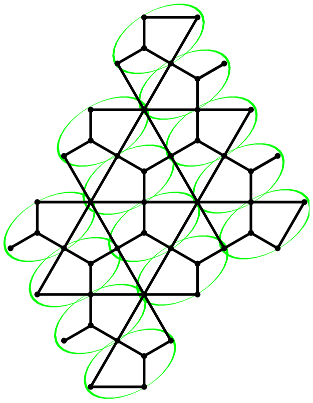
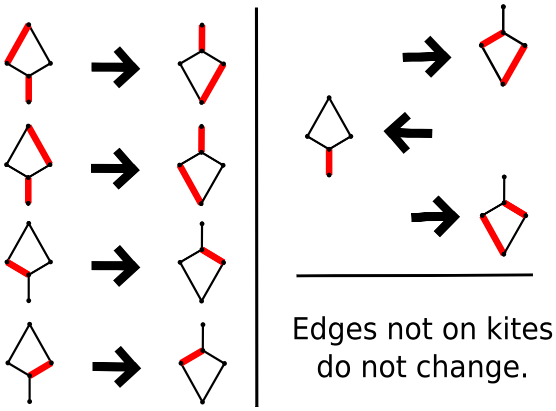


Figure 13: Step 4

5. Draw the new matching M' using the rules in Figure 14.



Edges not on kites do not change.

Figure 14: The Rules of domino shuffling

6. Drop the unmatched vertices on the boundary ovals.

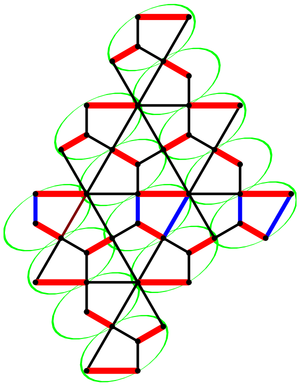


Figure 15: Steps 5 and 6

With these six steps we have completed the shuffling. Yet, we have not justified step 3. Let us now explain why we add $2n+1$ tails when we apply shuffling to M.

For each strip of D_m, we see that the easternmost and westernmost diamonds are either N diamonds or they are S diamonds. If they are both N diamonds, we circle two kites on the eastern boundary, and one on the western boundary. If they are both S diamonds, we circle two kites on the western boundary, and one on the eastern boundary. The tails of two of these kites are in D_m, while the other kite's tail is not in D_m. Hence, we will always have to add as many tails as strips to D_m, i.e., $2n-1$. We must also consider that there are two kites that do not lie on strips that contain diamonds in D_m. These two kites lie north and south of the northernmost and southernmost strips in D_m, respectively. Each of these kites only share one edge with D_m, hence their essential vertex must be matched by adding 2 more tails. Therefore, we add exactly $2n-1+2 = 2n+1$ vertices.

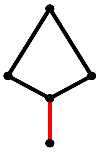


Figure 16: A creation

A *creation* is the case when the original kite had only its tail in the matching. Then, the output kite will have two of its edges in the matching, hence increasing the number of edges in the matching by one.

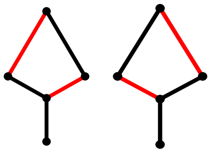


Figure 17: An annihilation

An *annihilation* contains two of the edges bounding the square. Its output is a kite with only one edge (the tail) matched. Hence, when an annihilation occurs, we decrease the number of edges in the matching by one.

Through a tedious yet simple case analysis, one can see that applying the shuffling to a perfect matching on D_m, we obtain a perfect matching on D_{m+1}.

8 Induction

Our final definition is that we let $PM(D_m)$ be the set of perfect matchings on D_m. We wish to create a map from $PM(D_m)$ to $PM(D_{m+\frac{1}{2}})$. We let $n = \lfloor m \rfloor$.

Applying shuffling to $M \in PM(D_m)$, by step 3, we add $2n+1$ tails, and we showed that $M_{m+\frac{1}{2}} = M_m + 3n + 2$. Hence, we must merely account for $n+1$ edges added to the matching. This must be the difference between the number of creations and annihilations.

Suppose that M has k annihilations, then by the last paragraph we must have that (#of annihilations)$+n+1 = k+n+1$ creations. Yet, for each specific set of k kites, there are exactly 2^k possible ways of having k annihilations on this set of specific kites, assuming that the rest of the matching is fixed. This is because for each kite, there are 2 possible ways of having an annihilation.

Similarly, M has $k+n+1$ creations on $k+n+1$ kites. Hence, there are 2^{k+n+1} ways of matching these $k+n+1$ kites in $D_{m+\frac{1}{2}}$ since for each kite there are two ways of appropriately matching the vertices in the output kite. Hence, the 2^k matchings with k annihilations map to exactly 2^{k+n+1} matchings on $PM(D_{m+\frac{1}{2}})$. This implies that $|PM(D_{m+\frac{1}{2}})| = 2^{n+1}|PM(D_m)|$. Having shown the inductive step leading to our final result, we show our base cases:

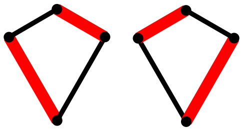


Figure 18: Case $m = \frac{1}{2}$

Case $m = \frac{1}{2}$

- $D_{\frac{1}{2}}$ has 4 edges and 4 vertices. It is clear that there exist exactly 2 possible perfect matchings.

Case $m = 1$

- To find the number of perfect matchings on D_1 we use the graph transformation called urban renewal, which is described by Propp in [3]. This gives us that D_1 has 4 perfect matchings.

Thus,

$$|PM_(D_m)| = \begin{cases} 2^1 2^1 2^2 \ldots 2^{n+1} 2^{n+1} & m \in \mathbb{N} \\ 2^1 2^1 2^2 \ldots 2^n 2^{n+1} & (m+\frac{1}{2}) \in \mathbb{N} \end{cases}$$

$$= \begin{cases} 2^{\Sigma_{i=1}^{n+1} 2i} & m \in \mathbb{N} \\ 2^{n+1+\Sigma_{i=1}^{n} 2i} & (m+\frac{1}{2}) \in \mathbb{N} \end{cases}$$

$$= \begin{cases} 2^{n(n+1)} & m \in \mathbb{N} \\ 2^{(n+1)^2} & (m+\frac{1}{2}) \in \mathbb{N}. \end{cases}$$

9 Conclusion

This method gives us a simple formula to count perfect matchings; the significance of these results lies in the development of the shuffling itself. The transformations were basic: urban renewal and double-edge contraction. Yet, they allowed us to develop a powerful tool to count the matchings. The question is then, can we develop similar shufflings in order to count perfect matchings on other lattices? It appears so, and this merits further exploration. Any takers?

10 Acknowledgements

This is joint work with Benjamin Young. The project was supported in part by an ISM Summer Scholarship, for undergraduate research supervised by post-doctoral students, and in part by Jacques Hurtubise, to whom we are deeply grateful. An extension and more formal version of this research is in preparation and will appear soon.

References

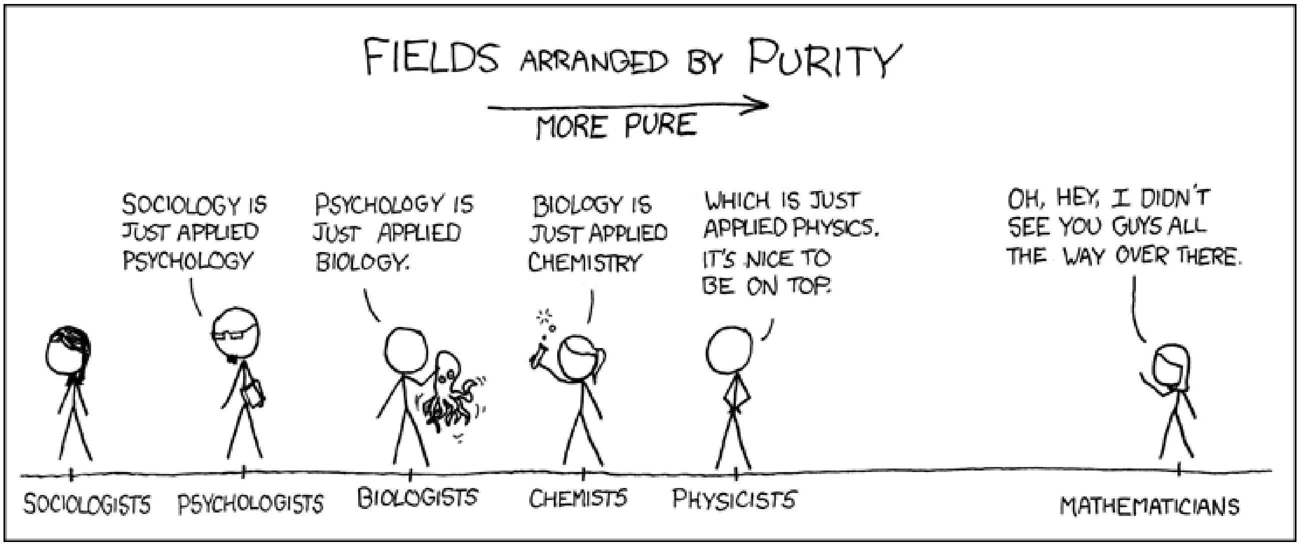
[1] Mihai Ciucu. Perfect matchings and perfect powers. *Journal of Algebraic Combinatorics*, 17(3):335–375, 2003. arXiv:math/0501521.

[2] Noam Elkies, Greg Kuperberg, Michael Larsen, and James Propp. Alternating-Sign Matrices and Domino Tilings (Part II). *Journal of Algebraic Combinatorics*, 1(3):219–234, 1992. arXiv:math/9201305.

[3] James Propp. Generalized domino-shuffling. *Theoretical Computer Science*, 303(2-3):267–301, 2003. arXiv:math/0111034.

[4] Benjamin Young. Computing a pyramid partition generating function with dimer shuffling. *Journal of Combinatorial Theory, Series A*, 116(2):334–350, 2009. arXiv:0802.3948.

Jokes


FIELDS ARRANGED BY PURITY
MORE PURE
SOCIOLOGY IS JUST APPLIED PSYCHOLOGY
PSYCHOLOGY IS JUST APPLIED BIOLOGY.
BIOLOGY IS JUST APPLIED CHEMISTRY
WHICH IS JUST APPLIED PHYSICS. IT'S NICE TO BE ON TOP.
OH, HEY, I DIDN'T SEE YOU GUYS ALL THE WAY OVER THERE.
SOCIOLOGISTS
PSYCHOLOGISTS
BIOLOGISTS
CHEMISTS
PHYSICISTS
MATHEMATICIANS

xkcd 435: *Purity*

□

Constructing Cryptographic Hash Functions

François Séguin

We will describe how we can use walks on Cayley expander graphs to construct cryptographic hash functions in an attempt to show that abstract algebra can sometimes be useful for real-life applications.

1 Introduction

"That's very nice but, what is it useful for?"

Mathematicians are asked this question countless times, usually following an explanation of some mathematical concept or research paper. Although the question is clearly rhetorical most of the time, it is indeed frustrating despite its potential legitimacy.

The goal of this paper is to demonstrate how branches of mathematics that are often considered "useless" play an important role in our lives, how the fundamental concepts and ideas of mathematics are not only developed to give jobs to mathematicians. We will do so through the concrete example of the process of constructing cryptographic hash functions using walk on Cayley expander graphs. We will then see how abstract algebra, in particular the theory of group representation, plays a crucial role in this development.

2 Cryptographic Hash Functions

We should begin by explaining exactly what a hash function is, as well as the difference between a standard hash function and a cryptographic hash function. Different applications of these algorithms will then be outlined.

2.1 What Is A Hash Function?

Given a set Σ called the alphabet, a *string* is an element of the set Σ^N for some $N \in \mathbb{N}$.

A hash function is a function h defined on an alphabet Σ that maps arbitrarily long strings to strings of a fixed length $n \in \mathbb{Z}$, i.e.

$$\begin{aligned} h : \Sigma^* &\longrightarrow \Sigma^n \\ x &\longmapsto y. \end{aligned}$$

Here, x is the message to hash and y is called the *hash value* or the *digest* of the message x. We will also call $|\Sigma|^n$ the *size* of the hash function. Now according to this definition, we clearly see that a hash function cannot be injective, by the pigeon hole principle. Thus, we expect to have several messages associated to every element of Σ^n, and this is why it is common to call these different possible values *buckets*. We also say that a certain bucket contains a message m if the bucket is the hash value of m. Ideally, a standard hash function should map elements of Σ^* to Σ^n as uniformly as possible. That is, every bucket should contain sensibly "the same amount" of messages. Formally, we could say that the ideal hash function is such that the probability of a randomly chosen string to be in any bucket is of $|\Sigma|^{-n}$.

Typically, we can also require standard hash functions to have a very small sensitivity to changes in the message. It is not rare to use a hash function that maps *similar* messages to *close* buckets. For example, in the case where, given a string s in a bucket B, we are interested to find a similar string s' in a text, we could hash the strings of the text and look at those falling in buckets close to B.

2.2 Cryptographic Hash Functions

Since we will exclusively be working with a special kind of hash functions called cryptographic hash functions, we should make the distinction with the other types of hash functions very clear.

The first major difference is the sensitivity to change. Ideally, a good cryptographic hash function would by highly sensitive to changes in the messages for the attribution of hash values. Thus, a very small change in a certain string should result in a hash value very far from the digest of the original string. Also, it is very important for a cryptographic hash function h to be a one-way function, i.e. that we can easily compute $h(x) = y$ but that it is very hard to compute $h^{-1}(y)$. One example of a one-way function could be to take $f(x) = \gamma^x$ for γ a generator of a large cyclic group, and x an integer. Then, for some appropriately chosen group, the problem of finding $f^{-1}(y)$ is called the discrete logarithm problem and is known to be a hard problem.

To formally present the characteristics we require for a cryptographic hash functions, we introduce the following concepts:

Definition. A hash function h is called *preimage resistant* if given a hash value y, it is infeasible to find a message x such that $h(x) = y$.

We notice that this concept is directly related with the concept of one-way function.

Definition. A *collision* of the hash function h is a pair $(x, x') \in (\Sigma^*)^2$ such that $x \neq x'$ but $h(x) = h(x')$.

We remind the reader that these collisions are bound to exists as h is not injective.

Definition. The function h is called *weak collision resistant* if, given $x \in \Sigma^*$, it is infeasible to compute a collision (x, x').

This property is also called *second preimage resistance*. We notice that it is somewhat stronger than preimage resistance as, if we have x, we can also easily find $y = h(x)$ and so weak collision resistance implies preimage resistance.

Definition. The function h is called *(strong) collision resistant* if it is infeasible to compute any collisions (x,x').

N.B. The above definitions are not completely rigorous as we have not defined what it means to be *infeasible*. For our purposes, it is sufficient to say that something is infeasible if it would require too much time or space to be carried out with the available technology.

Fact 1. A (strong) collision resistant function h is one-way.

N.B. For any function h that we consider, we will assume that $h(x)$ is easy to compute.

Proof. Suppose that h is not one-way. We choose an arbitrary string $x \in \Sigma^*$ and we let $y = h(x)$. Now, we compute $h^{-1}(y) = x'$, which can easily be done as h is not one-way. Since x is arbitrary, we can repeat the process until we find $x' \neq x$. We remind that this has to happen as h cannot be injective. We thus found the collision (x,x'). □

We conclude that we only have to require a cryptographic hash function to be collision resistant. This way, if two given messages have the same hash value, we can be confident that they are the same message. This is the key property used in cryptography.

2.3 Applications of Cryptographic Hash Functions

The reason for requiring the collision resistant property becomes apparent when looking at applications of cryptographic hash functions.

We should say first of all that, according to Kerckhoff's principle, the hash function itself should never be a secret in any applications.

Fingerprinting

The first application we will describe here is called fingerprinting. This is used whenever we want to quickly verify the integrity of some data without actually having to look at all the data to notice changes. The idea is to apply the cryptographic hash function to the original data and store this digest of the data somewhere safe. At a later time, to verify that the data has not been altered, we can recompute the hash value of the data and compare this relatively small value to the digest of the original data. If the data was changed even by a single digit (or character), we should be able to see a significant difference in the hash value. Collision resistance is important here so that no one can alter the data without changing the hash value.

Example: Suppose that Alice owns a bank in which Bob has a bank account. She is responsible for verifying that the amount of money everyone has in the morning is the same as they had at the end of the previous day; however, as there are large amount of data to be checked, comparing the original files with archives would be too time consuming. Thus, at the end of every day, she instead computes the hash value of the document containing the customer's names, account numbers and balances. During the night, Mallory intrudes in the bank's computer and wants to change Bob's account balance. If the hash function used was not collision resistant, then Mallory could find a way to change the document while keeping the same hash value and thus Alice would never notice that changes were made; however, since Alice uses a cryptographic hash function, she can easily know if changes were made in the record.

Message Authentification

The second important application of cryptographic hash functions is data authentification. In the process of sending a secret message between two people, there are procedures preventing the message from being read by an eavesdropper during the transmission process, but there is no way to prevent the message from being intercepted and replaced by another message. The way to notice that a malicious attacker has done this is through data authentification. This is best seen through an example:

Example: Suppose that Alice wants to send a message m to Bob. Alice encrypts her message and sends it to Bob as m_e. However, Mallory intercepts the message. Even though this message is totally incomprehensible to her, she can still decide to prevent the message from reaching Bob and substitute it for her own message m'_e. Now, Bob receives a message m'_e duly encrypted, but cannot know if Alice really sent this message. To prevent this, we suppose that Alice and Bob share a common secret K. Then, Alice sends Bob her encrypted message m_e along with a *message authentification code* (MAC) that she computes using a cryptographic hash function h as $h(K \circ m)$ where $K \circ m$ denotes a (public) way to combine K and m (e.g. if $a||b$ denotes concatenation and $\oplus$ the bitwise XOR, it could be $K||m$, $K \oplus m$, $h(K||m)$, etc.). Now, as Bob receives the message, he can decrypt it, then compute $h(K \circ m)$ himself and compare it with the MAC he received. If Mallory had intercepted the message, she could replace it with her own but would then have to compute the MAC of her own message. Since h is one-way, she could neither recuperate K from Alice's MAC nor figure some message m' that would have the same MAC as the original one. Thus, if Bob receives a message m and MAC a such that $a = h(K \circ m)$, he could be very confident that the message truly comes from Alice.

2.4 Importance of Research

Because of all the previously cited applications of cryptographic hash functions to different areas of cryptography, it should be clear that these hash functions are truly important. However, it does not directly imply that it is important for us to try to come up with new such functions. After all, if we already have some of these functions working properly, why should we bother finding more?

The answer to this is simply that a cryptographic system's worst enemy is the cryptographer her/himself. Indeed, for your cryptosystem to be safe, you have to be convinced as a cryptographer that anyone attacking it will fail. This is why cryptographers spend so much time designing attacks on the very cryptosystems they developed: If those systems are flawed, even slightly, then we have to find something better.

It is also true that, as of now, only a few cryptographic hash functions exist that have not been broken. As those functions are so useful, we essentially rely on only a small number of cryptographic hash functions. This means that if ever someone finds a breach in these particular functions, we would be deprived of this useful tool, hence we have to start thinking about developing new cryptographic hash functions.

2.5 A New Hope

This is where the study of abstract structure comes to the rescue of cryptography. The cryptographic hash functions in use right now use what is called a compression function among other procedures that make the function collision resistant. Compression functions basically work by compressing chunks of information (say N characters) into smaller chunks of information (say n characters) and repeating the process until the given result is small enough to be a digest of the function.

Graph theory provides us with a totally different approach to cryptographic hash functions. We view the function as a walk on a graph. Before going into more details, we should explain the particular notions from graph theory we are going to be using.

3 Cayley Expander Graphs

3.1 What Is A Graph?

A *graph* G is a set of *vertices* $\mathrm{V}(G)$ along with a set of *edges* $\mathrm{E}(G)$ such that every $e \in \mathrm{E}(G)$ is of the form (u,v) for $u,v \in V$, $u \neq v$, called the *endpoints* of e. We also require that $(u,v) \in E \Rightarrow (v,u) \in E$ so that the graph is *undirected*. We say that two vertices are *adjacent* if there exists an edge containing both of them. A *path* P in G is a sequence of edges of G such that the second endpoint of any edge is the first endpoint of the next edge in the sequence. Similarly, a $x-y$ path in G is a path in G with endpoints x and y. We say that a graph is *connected* if for any two vertices $x,y \in \mathrm{V}(G)$, there exists a $x-y$ path.

The subgraph of G generated by $S \subseteq V$, denoted $G[S]$, is the graph with vertex set S and edge set $\mathrm{E}(G[S]) = \{(u,v) : u,v \in S, (u,v) \in \mathrm{E}(G)\}$.

Also, we define the neighborhood of a vertex v in a graph G to be $N(v) := \{u \in \mathrm{V}(G) : (u,v) \in \mathrm{E}(G)\}$. Similarly, if $S \subseteq V$, then $N(S) := \{u \in V : (u,v) \in E \text{ for some } v \in S\}$.

Finally, we say that a graph is *d-regular* if, for any vertex $v \in V$, $|N(v)| = d$, i.e. every vertex is adjacent to exactly d other vertices.

Any graph can also be completely defined by its adjacency matrix. The *adjacency matrix* of a graph G is defined by the $(|V| \times |V|)$-matrix $A_G = (a_{i,j})$ where, if we index the vertices of G by $V = \{v_k\}_{k=1,\dots,|V|}$, then

$$a_{i,j} = \begin{cases} 1 \text{ if } (v_i, v_j) \in \mathrm{E}(G) \\ 0 \text{ if } (v_i, v_j) \notin \mathrm{E}(G) \end{cases} .$$

It is clear from this definition that the adjacency matrix of any graph is symmetric, that is that $A_G^T = A_G$. Also, as we do not allow an edge from a vertex to itself, all the diagonal entries of A_G are 0. Finally, as the indexing of the vertices of G are not unique, we see that the adjacency matrix of a graph is not unique either. Actually, it is unique up to interchanging of rows and columns, more specifically up to conjugation by $E_{i,j}$ where

$$E_{i,j} := \begin{array}{cc} & \begin{array}{cccc} \quad & i & j & \quad \end{array} \\ \begin{array}{c} \\ i \\ j \\ \\ \end{array} & \begin{pmatrix} 1 & & & \\ & 0 & 1 & \\ & 1 & 0 & \\ & & & 1 \end{pmatrix} \end{array},$$

the elementary matrix interchanging rows.

3.2 Cayley Graphs

Let now H be a group and $S \subseteq H$ be a generating set for H. Here, we will require that S is symmetric, that is $g \in S$ implies $g^{-1} \in S$ as well. Then, we have that the *Cayley graph* $\Gamma(H,S)$ is the graph having the vertex set H and such that $(u,v) \in \mathrm{E}(\Gamma(G,H))$ if $s \cdot u = v$ for some $s \in S$. We note that these are undirected edges as if $(u,v) \in \mathrm{E}(\Gamma(H,S))$, then $v = s \cdot u$ and $s^{-1} \cdot v = u$ so $(v,u) \in \mathrm{E}(\Gamma(H,S))$. It should be thus clear that any Cayley graph $\Gamma(G,S)$ is a connected $|S|$-regular graph.

We first define an *automorphism of a graph* Γ to be a permutation π of all its vertices that preserves the edges, that is that (h,g) is an edge if and only if $(\pi(h), \pi(g))$ is. It is interesting to note that Cayley graphs are always *vertex transitive*, i.e. that for any $u,v \in \mathrm{V}(\Gamma)$, there exists an automorphism π taking u to v. Indeed, given the ordered pair u,v, we can have the automorphism of the graph

$$\pi : g \longmapsto gu^{-1}v$$

such that $\pi(u) = v$, and if $(g,h) \in \mathrm{E}(\Gamma)$, then $sg = h$ and so $sgu^{-1}v = hu^{-1}v$ giving $s\pi(g) = \pi(h)$ implying that $(\pi(g), \pi(h)) \in \mathrm{E}(\Gamma)$.

3.3 Expansion Property of A Graph

For any graph G, we can define for $S,K \subseteq \mathrm{V}(G)$, $\mathrm{E}(S,K) := \{(u,v) : u \in S, v \in K, (u,v) \in \mathrm{E}(G)\}$. For example, $\mathrm{E}(V,V) = E$, $\mathrm{E}(S,S) = \mathrm{E}(G[S])$, etc.

Now, we can also define the *edge boundary of a set* $S \subseteq V$ to be $\partial S := \mathrm{E}(S, V \setminus S)$. We notice that $|\partial S| = |N(S) \setminus S|$.

Finally, for Γ a d-regular connected graph with n vertices, the *expansion constant* h_Γ of Γ is defined as

$$h_\Gamma := \min_{\{S \subseteq V : 0 < |S| \leq \frac{n}{2}\}} \frac{|\partial S|}{|S|}.$$

There is a strong connection between the expansion property of a Cayley graph and spectral analysis of its adjacency matrix. Let A be this adjacency matrix and $\lambda_1 \geq \lambda_2 \geq \ldots \geq \lambda_n$ the eigenvalues of A.

Claim 2. $\lambda_1 = d$

Indeed, we can take vector v with 1 for every entry, and it is clear that $Av = dv$.

Then, we have a very interesting property of the spectral gap of A, that is $\lambda_1 - \lambda_2$.

Theorem 3 (Alon-Milman).

$$h_\Gamma \geq \frac{2d - 2\lambda_2}{3d - 2\lambda_2}.$$

Therefore, we can build a graph with very good expansion property by finding a graph with minimal λ_2.

3.4 Construction of the Hash Function

We want to use these Cayley graphs to construct a cryptographic hash function. Let's assume that we want a function $f : \Sigma^* \longrightarrow X \subseteq \Sigma^n$.

Let G be a finite group with $|G| \leq |\Sigma|^n$ and S be a generating set for G such that $|S| \geq |\Sigma|$. Let also $\tilde{S}$ be the symmetric completion of S, i.e. the set obtained by $S \cup S^{-1}$. Let now $\Gamma(G, \tilde{S})$ be the Cayley graph of G using $\tilde{S}$. We then choose a vertex $v_0 \in \mathrm{V}(\Gamma)$. Finally, we fix the following two functions of sets :

$$\tau : \Sigma \hookrightarrow S$$

and

$$\phi : G \hookrightarrow \Sigma^n.$$

Indeed, we let $X = \phi(G)$ and notice by the previous cardinality requirements that such injective maps exist.

Now in order to evaluate the function on a certain message $e_0e_1e_2\ldots e_N$ for $e_i \in \Sigma$, we split the message characterwise. We then perform a walk on the graph starting at v_0 and then going across $\tau(e_0)$, then $\tau(e_1)$, and so on until we go across $\tau(e_N)$. We then define the hash value of the message as the image of the final vertex under ϕ. We can define this algorithm in a more mathematical way as

$$f(e_0e_1\ldots e_N) = \phi\left(\tau(e_N) \cdot \ldots \cdot \tau(e_1) \cdot \tau(e_0) \cdot v_0\right)$$

where the multiplication "$\cdot$" is taken in G. It is easy here to see how any message of any finite length gets mapped to an element of Σ^n as G is closed under multiplication. Notice also that as we can also define f recursively as, for $e \in \Sigma$

$$f(e) = \phi(\tau(e) \cdot v_0)$$

and for $e_i \in \Sigma$ for $i = 1, \ldots, N$,

$$f(e_0e_1\ldots e_N) = \phi\left(\tau(e_N) \cdot \phi^{-1}\left(f(e_0e_1\ldots e_{N-1})\right)\right)$$

as the injectivity of ϕ guarantees that $\phi^{-1}\left(f(e_0e_1\ldots e_{N-1})\right)$ is well-defined.

3.5 f Being Cryptographic

We have now proven that f is a hash function of size n, but not that f is actually a cryptographic hash function. For this, we still need that f is one-way.

For reasons that would be beyond the scope of this article, we know that the quality of the collision resistance of f is directly related to the expansion property of the graph $\Gamma(G, \tilde{S})$. We can have an intuitive feeling of how those concepts are related by remembering what f being one-way implies in this specific case. Given a hash value g_0, we want it to be very difficult to compute a message m such that $f(m) = g_0$. Notice that this implies that it must be infeasible to efficiently perform a search algorithm in the Cayley graph of G using $\tilde{S}$ as otherwise, we could perform this located a v_0 to find the path to g_0. We thus know that we have to use a very big group. Also, the generating set has to be such that it uses as much as possible this size of Γ, the Cayley graph. Suppose that Γ were to have a very low expansion constant. Then we could have a message m' taking its hash value in the subset of vertices where the minimum is attained. Thus, the concatenation of this message and some extra characters would most probably have an image staying in this significantly smaller subgraph of Γ, and we therefore increase significantly our chances of finding a collision.

Since it must also be difficult to determine what Γ looks like as a whole, we must determine the expansion property of Γ differently. We know by section 3.3 that the expansion property of a graph is directly related to its adjacency matrix. Because here we are dealing with a Cayley graph, we expect to find some property of the adjacency matrix following from the group structure itself. Fortunately this is exactly what the Kazhdan constant of representation theory provides us with.

4 Representation Theory

4.1 Basic Definitions and Results

Definition. Let G be a finite group . Then, a *representation of* G is a pair (V,ρ) such that V is a vector space over $\mathbb{C}$ and ρ is the homomorphism

$$\rho : G \longrightarrow GL(V)$$

where $GL(V)$ is the set of linear bijective maps from V to V.

That is, every element of the group G is represented as a linear transformation of V homomorphically, that is for any $g,h \in G$, the transformation $\rho(gh) = \rho(g)\rho(h)$.

Another way to understand the representation of a group is to understand the group through its action on a vector space V. Indeed, every group element $g \in G$ acts on any vector $v \in V$ as $\rho(g)v$ and ρ being homomorphic implies that this satisfies all the properties of group action.

Now, given that V is finitely generated, we have that $GL(V) \cong GL_n(\mathbb{C})$, the general linear group of $n \times n$ invertible matrices with entries in $\mathbb{C}$, for n the dimension of V. Hence, ρ maps every element of G to such a matrix. We also call n the dimension of the representation ρ.

We now have to introduce the concept of irreducible representation, as it is key for our purposes:

Definition. A representation $\rho : G \to GL(V)$ is called *irreducible* if, whenever $W \leq V$ is invariant under all $\rho(g)$, $g \in G$, then either $W = \{0\}$ or $W = V$.

Also, we will use the following fact:

Fact 4. For G a group, the number of irreducible representations of G is the number of conjugacy classes of G.

In particular, we notice that there are finitely many irreducible representations for any group G. We now present one of the very important results in representation theory which tells us exactly how the different irreducible representations can be found using a special representation called the regular representation. We first need some preliminaries.

Definition. The *character* χ of the representation of G, (ρ,V) is the function

$$\begin{aligned} \chi : G &\longrightarrow \mathbb{C} \\ g &\longmapsto \operatorname{Tr}(\rho(g)) \end{aligned}$$

Definition. For any two characters χ,Ψ of two representations of G,

$$\langle \chi, \Psi \rangle := \frac{1}{\#G} \sum_{g\in G} \chi(g)\overline{\Psi(g)}.$$

Theorem 5. Let V be any representation of G, and let χ_V be its character. Now, let $\chi_1,\dots,\chi_r$ be the respective characters of $V_1,\dots,V_r$, the irreducible representations of G. Then,

$$V \cong V_1^{a_1} \oplus \cdots \oplus V_r^{a_r}$$

where

$$a_i = \langle \chi_V, \chi_i \rangle .$$

Definition. Let G be any finite group. Let V be the $\#G$-dimensional vector space with the basis $\{e_g : g \in G\}$. Then, define the action of G on the basis elements to be

$$\rho(h) : e_g \longmapsto e_{hg}.$$

The representation (V,ρ) is called the *regular representation* of G.

Theorem 6. The decomposition into irreducible representations of the regular representation of any group G contains all irreducible representations of G.

4.2 The Kazhdan Constant

Now, we finally introduce the last definition necessary: the Kazhdan constant of a group G.

Definition. Let G be a finite group, S a generating set for G and let r be the regular representation of G. Then, we define the *Kazhdan constant* of G using S to be

$$K(G,S) = \min_{v\perp 1} \max_{h\in S} \frac{\|r(h)v - v\|^2}{\|v\|^2}.$$

We presented all of the above results in order to simplify the problem of computing the Kazhdan constant through the following fact:

Fact 7. Let G be a finite group, S a generating set for G. Then,

$$K(G,S) = \min_{\rho} \min_{v\in V} \max_{h\in S} \frac{\|\rho(h)v - v\|^2}{\|v\|^2}$$

where (ρ,V) ranges over all non-trivial irreducible representations of G.

We can see this result through Theorems 5 and 6.

It is known that there is a strong connection between the adjacency matrix of $\Gamma(G,S)$ and the regular representation of G, which is reflected in the following bound:

Consequence 8.

$$\frac{K(G,S)}{2|S|} < 1 - \lambda_2(G,S) < \frac{K(G,S)}{2}.$$

Now, using Theorem 3 from section 3.3, we get a bound between the Kazhdan constant of a group G using a generating set S and the expansion constant of the Cayley graph $\Gamma(G,S)$.

Hence, we get a way to characterize the expansion constant of a Cayley graph using only the Kazhdan constant of this same group. Since representation theory is a well known branch of abstract algebra, such constants are known (or at least bounded) for several interesting groups. We could study the Kazhdan constant of these groups in order to decide which one to pick, along with which generating set, in order to get the best cryptographic hash function.

5 Conclusion

Abstract algebra was key here in the process of developing new cryptographic hash functions. Indeed, we saw that representation theory helped us determine the Kazhdan constant of a group, the use of this constant to determine the expansion property of the associated Cayley graph, and finally the potential use of these Cayley graphs and walks on them in order to construct the cryptographic hash functions we were looking for.

In conclusion, asking what abstract algebra is useful for is a legitimate question, but there is also legitimate answer to it.

6 Acknowledgements

I learned most of the above during a NSERC USRA project under the supervision of professor Eyal Z. Goren, who invested a lot of time working with me on this project. I would thus like to thank him very much for his supervision.

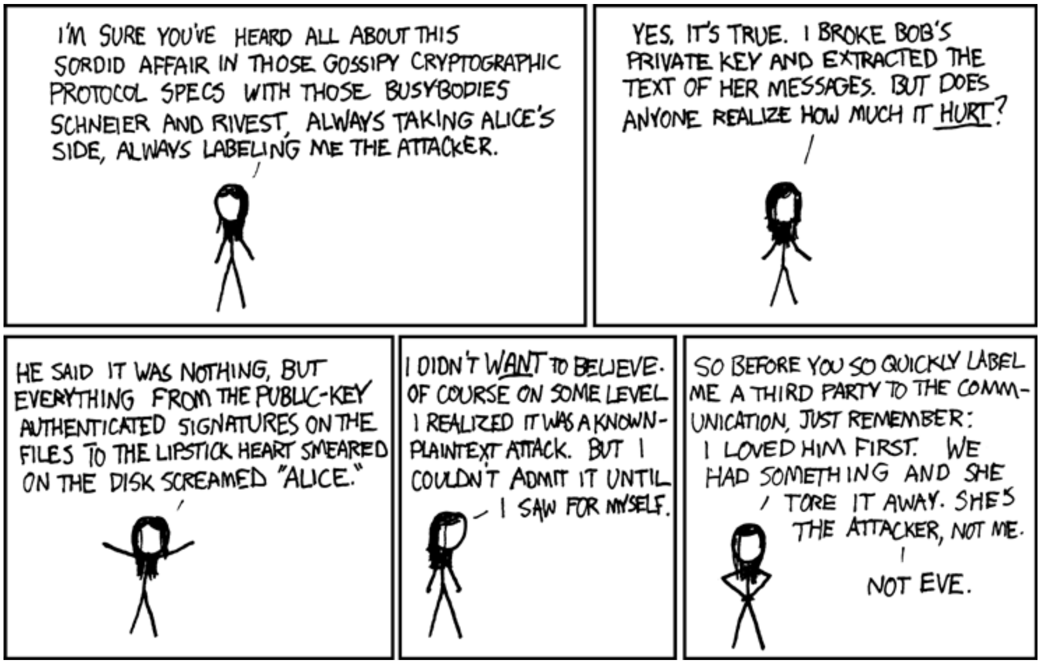
References

[1] Hoory, Shlomo, Nathan Linial and Avi Wigderson.“Expander Graphs and their Applications.”*Bulletin (New Series) of the American Mathematical Society* Volume 43, Number 4, October 2006, pp.439–561.

[2] Naimark, M.A., and A.I. Štern. *Theory of Group Representation*. New York: Springer-Verlag, 1982.

[3] Buchmann, Johannes A. *Introduction to cryptography*. 2^{nd} ed. New York: Springer, 2004.

Jokes


I'M SURE YOU'VE HEARD ALL ABOUT THIS SORDID AFFAIR IN THOSE GOSSIPY CRYPTOGRAPHIC PROTOCOL SPECS WITH THOSE BUSYBODIES SCHNEIER AND RIVEST, ALWAYS TAKING ALICE'S SIDE, ALWAYS LABELING ME THE ATTACKER.
YES, IT'S TRUE. I BROKE BOB'S PRIVATE KEY AND EXTRACTED THE TEXT OF HER MESSAGES. BUT DOES ANYONE REALIZE HOW MUCH IT HURT?
HE SAID IT WAS NOTHING, BUT EVERYTHING FROM THE PUBLIC-KEY AUTHENTICATED SIGNATURES ON THE FILES TO THE LIPSTICK HEART SMEARED ON THE DISK SCREAMED "ALICE."
I DIDN'T WANT TO BELIEVE. OF COURSE ON SOME LEVEL I REALIZED IT WAS A KNOWN-PLAINTEXT ATTACK. BUT I COULDN'T ADMIT IT UNTIL I SAW FOR MYSELF.
SO BEFORE YOU SO QUICKLY LABEL ME A THIRD PARTY TO THE COMMUNICATION, JUST REMEMBER: I LOVED HIM FIRST. WE HAD SOMETHING AND SHE TORE IT AWAY. SHE'S THE ATTACKER, NOT ME.
NOT EVE.

xkcd 177: *Alice and Bob*

□

Interview with Axel Hundemer

Cathryn Supko

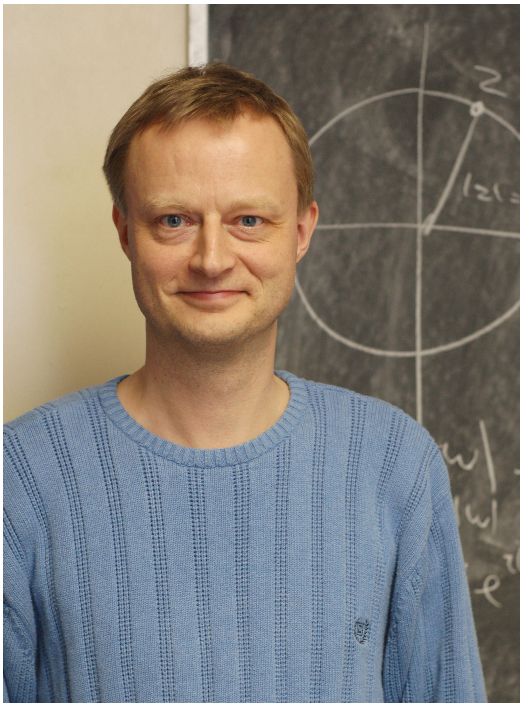
$\delta\varepsilon$: What is your background, both personal and academic?
I was born and raised in Germany, which is where I attended school. For my undergraduate degree, I studied both Math and Computer Science. I did my Ph.D. at the Technical University in Munich, focusing on several complex variables. I then did two years as a post doc at the University of Michigan. After that, I came to McGill, where I have been for 12 years.

$\delta\varepsilon$: What are your favourite things about McGill and Montreal?
The environment at McGill is very different from both Munich and Michigan because here there is a truly international community. Students from many different cultures and nations work together very well on a regular basis, which is really unique. This diversity is also what is so great about Montreal in general. It's also a very beautiful, almost European city, and I don't mind the winters too much.

$\delta\varepsilon$: Have you always known you wanted to be a professor?
Yes, I think I'm very lucky because I've known I wanted to have this job since I was in high school. I was always very good at math when I was growing up, so this was a very natural path for me to take. The students here are willing to learn and hardworking, which makes teaching here very enjoyable. I teach a wide variety of courses here, including Calculus, Complex Analysis, and Linear Algebra. One of the great things about the math department is that you do not teach the exact same material year after year, which helps to keep things dynamic and interesting.

$\delta\varepsilon$: What are your research interests?
I've always enjoyed most fields of pure mathematics. In particular, I really like algebra and complex analysis. I find that I like complex analysis more than real analysis because complex analysis tends to be a bit less cumbersome.

$\delta\varepsilon$: When did you start taking on administrative duties, and what are you primarily responsible for?
When I was hired initially as a faculty lecturer, it was primarily for the purpose of developing the WebWork system. I did most of the programming, administrative tasks, and debugging behind this system, which is now used in many 100, 200, and 300 level math courses. Three years ago, I also took on the position of Undergraduate Program Director.



Picture 1: Faculty Lecturer Axel Hundemer

$\delta\varepsilon$: What information about the program do you think students are most unaware of?
The descriptions of the requirements for the programs offered by the department are fairly straight-forward. Problems arise, however, when students decide to make substitutions for classes without asking permission. Another difficulty is that students have only one semester to decide if they are to follow the honors or the majors track, which may not be enough. This is potentially a problem because switching programs can be difficult. Depending on the student's academic advisor, it can be very difficult to make the switch from the majors into the honors program. Students typically switch from honors into majors because their grades are poor, and many students don't realize that McGill's policy on poor marks is very unforgiving and there is no way to replace a fail on your transcript.

$\delta\varepsilon$: What advice can you offer undergraduates looking to pursue math further?
Summer research is a great opportunity for undergraduates, they usually have very good experiences. If you are interested in working on a project, you should look into applying for funding before the deadlines in mid-February.

THE ORDER OF THE MORDELL-WEIL TORSION SUBGROUP AND RANKS FOR A ONE-PARAMETER FAMILY OF ELLIPTIC CURVES OVER THE RATIONAL NUMBERS

Dieter Fishbein

We present an introduction to elliptic curves and some important results associated with them. We study a one-parameter family of elliptic curve over the rational numbers, with a point of order 5 and present orginal results that characterize the Mordell-Weil torsion subgroup of this family. We present results from [1] regarding the rank of this family and a table, computed as a part of the project, showing the number of curves of certain rank found for values of the parameter within a height bound.

1 PREFACE

This report is the culmination of research done in the summer of 2010, supported by an undergraduate research scholarship from the Institut des Sciences Mathématiques in Montréal and supervised by Dr. Bryden Cais of the University of Wisconsin-Madison.[1]

2 INTRODUCTION TO ELLIPTIC CURVES AND THEIR TORSION SUBGROUPS

This section is loosely based on Chapters 1 through 3 of [5] and is intended to give the reader sufficient background to understand the main results in this paper.

2.1 Introduction

We define an elliptic curve over $\mathbf{Q}$ as a smooth curve of genus 1 equipped with a specified rational point. It can be shown that every such curve can be written as a locus of points of a cubic equation in $\mathbf{P}^2$. If we take our given rational point as $\mathscr{O}$=(0,1,0), after scaling the X, Y and Z axes appropriatley, and setting $x = X/Z$ and $y = Y/Z$ we obtain the following equation for the curve on the Euclidean plane in so called *Weierstrass form*,

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

By rational transformations, the above equation can be further put into *Weierstrass normal form*,

$$y^2 = f(x) = x^3 + ax^2 + bx + c.$$

Two curves are said to be *birationally equivalent* if there exists a bijective mapping between them that maps rational points to rational points. Since only rational transformations are used to transform a curve from Weierstrass form to Weierstrass normal form, we that the above two forms for an elliptic curve are birationally equivalent.

The above discussion glazes over many interesting details, see III.3 in [4] for a rigorous discussion. For the purposes of this paper, it is sufficient to know that any smooth curve that is birationally equivalent to a curve in Weierstrass normal form or Weierstrass form is an elliptic curve.

For an elliptic curve in Weierstrass normal form we define its *discriminant* in the usual way:

Definition. (see [5] p.47). For an elliptic curve of the form

$$y^2 = f(x) = x^3 + ax^2 + bx + c,$$

the discriminant *is,*

$$0 \neq D = -4a^3c + a^2b^2 + 18abc - 4b^3 - 27c^2.$$

2.2 Group Structure

Rational points on elliptic curves form an abelian group, $E(\mathbf{Q})$, under addition of points. We take the given rational point on the curve, $\mathscr{O}$ as the zero element for our group.

For two distinct points P and Q, we define the group law 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, $P + Q = (P * Q) * \mathscr{O}$.

We now explain why the addition of points is well defined. Since we are dealing with a cubic curve we know that any line through the curve, that does not intersect it at a point of tangency or inflection, will intersect the curve at three distinct points. In order to guarantee that a line through any two points, not necessarily distinct (points), will intersect the curve three times, we need to observe the convention that a line through a point of tangency intersects the curve twice at that point and a line through a point of inflection intersects the curve three times at that point.

[1] Computations done in this project were made possible through computing resources funded by National Science Foundation Grant No. DMS-0821725

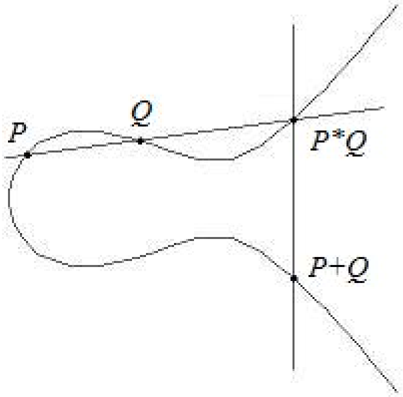


Figure 1: Adding points on a Weierstrass cubic

Commutativity is clear since the line given by joining two points is independent of the order in which we join the two points. Hence, $(P*Q)*\mathscr{O} = (Q*P)*\mathscr{O}$. So we need to verify that our zero element works, that each element has an additive inverse and that associativity holds for our group structure to be valid.

If we join P to $\mathscr{O}$ we get $P*\mathscr{O}$ as our third intersection. So, now we must join $P*\mathscr{O}$ to $\mathscr{O}$ to obtain the result of our addition. Clearly the third intersection of this line will be P. Hence, $\mathscr{O}$ is the zero element.

For a given Q, it is actually quite simple to calculate $-Q$. One need only take the reflection of Q in the X axis. So $Q=(x,y) \implies -Q=(x,-y)$. This is easily verified. The third intersection of the line through Q and $-Q$ and our curve is $\mathscr{O}$. The line connecting $\mathscr{O}$ to $\mathscr{O}$ meets the curve at $\mathscr{O}$ since $\mathscr{O}$ intersects our curve at a point of inflection. Hence $Q+(-Q)=\mathscr{O}$, as required. (See Figure 2).

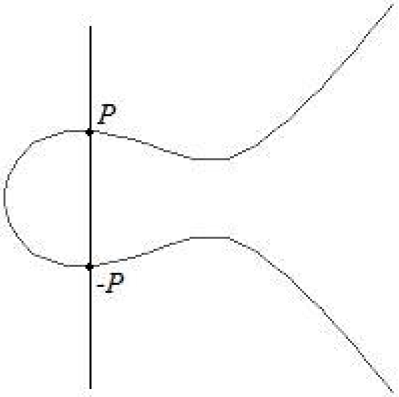


Figure 2: Additive Inverse of a Point

One can verify associativity directly by using explicit formulae for the group law, to be given in the next section, for curves in Weierstrass normal form. This is elementary but tedious as there are a great number of special cases. Associativity is best proven as a consequence of the Riemann-Roch Theorem, since one can show that for a given elliptic curve, E, $E \cong \text{Pic}^{\circ}(\text{E})$ (see III.3.4e in [4]).

2.3 Explicit Formulae for Group Law

By determining explicit formulae for the lines joining each point in our group law, and doing some algebra (see [5] p.29), we are able to derive explicit formulae for the group law on a Weierstrass cubic. Let,

$$P_1 = (x_1,y_1),\ P_2 = (x_2,y_2),\ P_3 = (x_3,y_3) = P_1 + P_2.$$

We find,

$$x_3 = \lambda^2 - a - x_1 - x_2, \qquad y_3 = \lambda x_3 + \upsilon,$$

where,

$$\lambda = \frac{y_2 - y_1}{x_2 - x_1} \qquad \upsilon = y_1 - \lambda x_1 = y_2 - \lambda x_2.$$

λ represents the slope of the line connecting P_1 and P_2. In cases where P_1=P_2 we must take λ to be the slope of the tangent line at that point. In this case, using implicit differentiation, we find,

$$\lambda = \frac{3x^2 + 2ax + b}{2y}.$$

2.4 Torsion Points

In this section we will be looking at points, P, that satisfy

$$P + ... + P \text{ (m times) } = mP = \mathscr{O}$$

for some $m \in \mathbf{N}, m \neq 0$. We call the least such m, if it exists, the *order* of P. If no such m exists, m is said to have *infinite order*. A point with finite order is known as a *torsion point*. The set of torsion points form a subgroup of the group of rational points, denoted $E(\mathbf{Q})_{\text{tors}}$. As $\mathscr{O}$ is often difficult to work with for computational purposes, one can use the equivalent condition $(m-1)P = -P$. This is a computationally easier condition since, if the curve is in Weierstrass normal form, $P=(u_0,v_0) \Rightarrow -P=(u_0,-v_0)$.

Here we will present three important theorems, without proof, that will give us greater insight into $E(\mathbf{Q})_{\text{tors}}$.

It turns out that the collection of torsion points for a given elliptic curve is finite. A result of Nagell and Lutz allows us to calculate a set of points that contains all torsion points for a given elliptic curve. Moreover, it tells us that all torsion points have integer coordinates:

Theorem 1 (Nagell-Lutz Theorem). *Let,*

$$E: y^2 = f(x) = x^3 + ax^2 + bx + c$$

be a non-singular cubic curve with integer coefficients and let D be the discriminant of E. Let $P = (x, y)$ be a rational torsion point on E. Then x and y are integers; and either $y = 0$, in which case case P has order two, or else y^2 divides D.

We are now able to calculate a finite set of points which contains all of our torsion points. One can then use the explicit formulae for the group law to determine the order of each point, and thus completely determine the subgroup $E(\mathbf{Q})_{\text{tors}}$.

The following theorem of Mazur gives an explicit list of groups which occur as $E(\mathbf{Q})_{\text{tors}}$:

Theorem 2 (Mazur's Theorem (see [2])). *Let E be an elliptic curve over* $\mathbf{Q}$*, and suppose that* $E(\mathbf{Q})$*, the group of rational points on the curve, contains a point of finite order m. Then either*

$$1 \leq m \leq 10 \quad or \quad m = 12.$$

Furthermore, the subgroup, $E(\mathbf{Q})_{\text{tors}}$*, must have one of the following forms:*

- *A cyclic group of order N with 1≤N≤10 or* $N = 12$,
- *The product of a cyclic group of order two and a cyclic group of order 2N with 1≤N≤4.*

2.5 Mordell's Theorem

Now we know that the torsion points of an elliptic curve over $\mathbf{Q}$ form either a cyclic group or are the product of two cyclic groups. We still must try to understand the points of infinite order.

Theorem 3 (Mordell's Theorem, see [5] p.63). *The group of rational points of an elliptic curve is finitely generated.*

Mordell's Theorem tells us the group of rational points is generated by a finite number of points, so there must be a finite number of independent points of infinite order. By the structure theorem for finitely generated abelian groups,

$$E(\mathbf{Q}) \cong \mathbf{Z}^r \otimes E(\mathbf{Q})_{tors}.$$

We call r the rank of E.

For proofs of the Nagell-Lutz Theorem and Mordell's Theorem, one can consult a variety of sources, including [5].

3 A Family of Elliptic Curves with a Point of Order 5

We follow [3] and construct a one-parameter family of elliptic curves over $\mathbf{Q}$, with each curve having a rational point of order 5.

Let E be an elliptic curve with a point, P, of order 5. Embed E in $\mathbf{P}^2$ with coordinates X, Y, Z and let $x = \frac{X}{Z}$ and $y = \frac{Y}{Z}$. Let $P = (0,0,1)$ and $\mathscr{O} = (0,1,0)$. Let the tangent line to E at P be $y = 0$. This forces E to have the form below, (see [3] p.8).

$$E : y^2 + a_1xy + a_3y = x^3 + a_2x^2.$$

By applying the transformations $x \to \lambda^2 x$ and $y \to \lambda^3 y$ where $\lambda = \dfrac{a_3}{a_2}$, we obtain,

$$y^2 + \alpha xy + \beta y = x^3 + \beta x^2$$

where $\alpha = \dfrac{a_1a_2}{a_3}$ and $\beta = \dfrac{(a_2)^3}{(a_3)^2}$. Using the group law, it is easy to determine that on E, we have

$$2P = (-\beta, \beta(\alpha - 1)) \qquad 3P = (1-\alpha, \alpha - \beta - 1).$$

We know P has order 5 or $P = \mathscr{O}$ if and only if $3P = -2P$. Hence, if $P \neq \mathscr{O}$, P has order exactly 5 if and only if $\alpha = 1 + \beta$. Letting $t = \alpha = 1 + \beta$, we have,

$$E_t : y^2 + (1+t)xy + ty = x^3 + tx^2. \tag{1}$$

Also, the discriminant of E_t is

$$D = -t^5(t^2 + 11t - 1).$$

We see that $D = 0 \Leftrightarrow t \in \{0, \frac{-11\pm5\sqrt{5}}{2}\}$. Hence, our cubic is smooth, which means it is an elliptic curve, for any $t \neq \{0, \frac{-11\pm5\sqrt{5}}{2}\}$. We now have our one-parameter family of elliptic curves defined over $\mathbf{Q}$ with a point, $P = (0,0,1)$, of order exactly 5.

We wish to put E_t into Weierstrass normal form as this will allow us to use the explicit formulae for the group law that we defined earlier. We apply the transformation $y \to y - \frac{1}{2}[(1+t)x + t]$ and we get,

$$E'_t : y^2 = x^3 + \left(\frac{1}{4}t^2 + \frac{3}{2}t + \frac{1}{4}\right)x^2 + \left(\frac{1}{2}t^2 + \frac{1}{2}t\right)x + \frac{1}{4}t^2. \tag{2}$$

It is easy to see that our transformation preserves rational points and irrational points, so E'_t and E_t are birationally equivalent over $\mathbf{Q}$. We note that on E'_t, we now have two points of order 5, $P = (0, \pm\frac{t}{2})$.

4 The Mordell-Weil Torsion Subgroups of E_t

We would like to have a better understanding of the torsion subgroup, $E_t(\mathbf{Q})_{\text{tors}}$, for this family of curves. Since each curve necessarily contains a point of order 5, by Mazur's Theorem, we know

$$E_t(\mathbf{Q})_{tors} \cong \mathbf{Z}/10\mathbf{Z} \textit{ or } \mathbf{Z}/5\mathbf{Z}.$$

We wish to characterize those values of t for which $E_t(\mathbf{Q})_{\text{tors}}$ has order 10. In order to do this, the Propositions 4.1 and 4.2 were proved during the course of the project.

Proposition 4. Let $t \in \mathbf{Q}$. Then $E_t(\mathbf{Q})_{\text{tors}}$, has order 10 if and only if there exists $s \in \mathbf{Q}$ with:

(1) $\sqrt{s^2+6s+1} \in \mathbf{Q}$

(2) $t = -\frac{1}{2}s - \frac{1}{2} \pm \frac{1}{2}\sqrt{s^2+6s+1}$.

Proof. First, assume $E_t(\mathbf{Q})_{\text{tors}}$ has order 10 and $t \in \mathbf{Q}$. Then, we know there must exist a point, (u,v) such that $2(u,v) = (0, \pm\frac{t}{2})$ and (u,v) is a point of order 10. Since E_t' and E_t are birationally equivalent, we perform calculations with E_t'.

Using our explicit formulae for the group law, we calculate $2(u,v) = (0, \pm\frac{t}{2})$ and solve for t. We obtain two solutions:

$$t = -u \qquad (3)$$

$$t = -\frac{1}{2}u - \frac{1}{2} \pm \frac{1}{2}\sqrt{u^2+6u+1}. \qquad (4)$$

Looking at equation (4.1), we find that $(u,v) = (-t, \pm\frac{t^2}{2})$. By doing a simple computation, using Sage for example, we find that $(-t, \pm\frac{t^2}{2})$ is necessarily a point of order 5. Clearly, if t is rational, then $(-t, \pm\frac{t^2}{2})$ is also rational. Thus we have found two rational points of order 5 on E_t'. Also, by construction, $(0, \pm\frac{t}{2})$ are two rational points of order 5 on E_t'. We now have 4 points of order 5 on E_t'.

Each of $\mathbf{Z}/10\mathbf{Z}$ and $\mathbf{Z}/5\mathbf{Z}$ have exactly 4 points of order 5. Since we have assumed $E_t(\mathbf{Q})_{\text{tors}}$ has order 10, equation (4.2) must give us exactly 2 rational points that induce a point of order 10. Since t is rational, and can be defined by equation (4.2), we know (1) and (2) must hold.

Second, assume (1) and (2) hold. Then, by a reverse argument, we can find a rational point, (u,v), of order 10. Hence, $E_t(\mathbf{Q})_{\text{tors}}$ has order 10 and $t \in \mathbf{Q}$.

□

We now present a simple way of determining if a given rational parameter forces $E_t(\mathbf{Q})_{tors} \cong \mathbf{Z}/10\mathbf{Z}$.

Proposition 5. *Let* $t \in \mathbf{Q}$ *then* $E_t(\mathbf{Q})_{tors} \cong \mathbf{Z}/10\mathbf{Z}$ *if and only if*

$$x^3 + \left(\frac{1}{4}t^2 + \frac{3}{2}t + \frac{1}{4}\right)x^2 + \left(\frac{1}{2}t^2 + \frac{1}{2}t\right)x + \frac{1}{4}t^2 \qquad (5)$$

has a rational root.

Proof. Again, we work with E_t'. Note that the above equation is E_t' where $y = 0$. Since E_t' is in Weierstrass normal form, we know that (u,v) is a point of order 2 if and only if $v = 0$, by Theorem 2.3. So if equation (4.3) has a rational root, this means we have found a rational point, (u,v), of order 2. Since $\mathbf{Z}/10\mathbf{Z}$ has a point of order 2 and $\mathbf{Z}/5\mathbf{Z}$ does not, we have the required result. □

Definition. We define the height of a rational number, $\frac{a}{b}$, *as* height$(\frac{a}{b})$=$|max(a,b)|$.

One can see that there are only finitely many rational numbers with height less than a fixed constant.

Remark. Looking at all rational numbers in lowest terms, with height $\leq 10^3$ *we find only 70, out of several hundred thousand where* $E_t(\mathbf{Q})_{\text{tors}}$ *has order 10.*

5 The Rank of E_t

In [1], Fisher establishes an upper bound for the rank of E_{-t} (see [1] (13)). Notice that he uses $-t$ in place of t, so we will limit our discussion to E_{-t}. We will use this bound to partially classify curves based on rank for certain values of t.

5.1 An Upper Bound for the Rank of E_{-t}

We follow [1] and give an upper bound for the rank of E_{-t}. We begin by defining $\beta(t)$,

$$\beta(t) = t^2 - 11t - 1.$$

Definition. We define the p-adic order of t , *written as* $ord_p(t)$ *as the highest exponent, k, such that* p^k *divides t.*

We also define disjoint sets of rational primes depending on t,

$$\mathscr{A} = \left\{ p \text{ prime} \;\middle|\; ord_p(t) < 0 \text{ or } \lambda \equiv 0 \; (mod\, p) \right\}$$

$$\mathscr{B} = \left\{ p \text{ prime} \;\middle|\; \begin{array}{c} \beta(t) \equiv 0 \; (mod\, p) \text{ and } p \equiv 1 \; (mod\ 5) \\ \text{or} \\ p = 5 \text{ and } t \equiv 18 \; (mod\ 25) \end{array} \right\}.$$

For $\mathscr{S}$, a set of rational primes, we write $[\mathscr{S}]$ for the subspace of the vector space $\mathbf{Q}^\times/(\mathbf{Q}^\times)^5$ generated by $\mathscr{S}$. We can then define a pairing of $(\mathbf{Z}/5\mathbf{Z})$-vector spaces, $\Xi : [\mathscr{A}] \times [\mathscr{B}] \to \mathbf{Z}/5\mathbf{Z}$.

Theorem 6 (see [1] p.178). For each $q \in \mathscr{B}$, we fix a non-trivial character, $\chi_q : (\mathbf{Z}/q\mathbf{Z})^\times \to \mathbf{Z}/5\mathbf{Z}$. Then Ξ is represented by the matrix, $(\chi_q(p))_{p \in \mathscr{A}, q \in \mathscr{B}}$. The upper bound for the Mordell-Weil rank of E_{-t} is

$$\text{rank}(E_{-t}) \leq |\mathscr{A}| + |\mathscr{B}| - 1 - 2\,\text{rank}(\Xi).$$

5.2 The Rank of E_{-t} for Certain Values of t

We first try to find values of t where E_{-t} will necessarily have rank 0.

$$|\mathscr{A}|+|\mathscr{B}|-1-2\,\mathrm{rank}(\Xi)\leq 0 \Rightarrow |\mathscr{A}|+|\mathscr{B}|\leq 1+2\,\mathrm{rank}(\Xi).$$

In order to easily classify values t that will cause E_{-t} to have rank 0, we assume $\mathrm{rank}(\Xi)=0$. This still will give us sufficient, but not necessary, conditions on t to cause E_{-t} to have rank 0. So we have,

$$|\mathscr{A}|+|\mathscr{B}|\leq 1.$$

One can see that this requires $-t$, and therefore t, to be a power of a prime for all $t\neq 1$. This is because $\mathscr{A}$ will contain all the prime factors of t, and if $t\neq 1$, it will necessary have a prime factor. Since $|\mathscr{A}|+|\mathscr{B}|\leq 1$, and $\mathscr{A}$ and $\mathscr{B}$ are disjoint, $\mathscr{B}=\emptyset$.

Of course, there are substantially more curves in E_t that have rank 0, but this allows us to easily identify the ranks of a small number of curves solely based on their parameter, t.

Proceeding in this same fashion, we find,

$$|\mathscr{A}|+|\mathscr{B}|\leq 2 \Rightarrow \mathrm{rank}(E_{-t})\leq 1$$
$$|\mathscr{A}|+|\mathscr{B}|\leq 3 \Rightarrow \mathrm{rank}(E_{-t})\leq 2$$
$$|\mathscr{A}|+|\mathscr{B}|\leq 4 \Rightarrow \mathrm{rank}(E_{-t})\leq 3$$
$$\vdots$$

While this gives us a convenient way to better understand the rank of E_{-t} solely based on the parameter t, it is generally only useful for values of t with few prime factors relative to rank. Since t can have arbitrarily large height, and we do not know of many curves with high rank, this method will not give us much useful information about rank for most values of t.

We now present some examples of applying this bound for certain values of t, letting $\lambda=-t$.

Example. Let $\lambda=-t=2$. We see that $\beta(2)=-19$. One can compute $\mathscr{A}=\{2\}$ and $\mathscr{B}=\emptyset$. In this case, Ξ has rank 0, but even if it had positive rank, we have $|\mathscr{A}|+|\mathscr{B}|\leq 1$, so E_{-2} is necessarily a curve of rank 0.

Example. Let $\lambda=-t=76$. We see that prime factorization of $\beta(76)=11*449$ and the prime factorization of $\lambda=76=2^2*19$. We have, $\mathscr{A}=\{2,19\}$ and $\mathscr{B}=\{11\}$. One can show that Ξ has rank 1, so we see that $\mathrm{rank}(E_{-76})=0$.

In the preceding two examples, we were able to calculate the exact rank of E_{-t} because it was zero. Often, especially for parameters of large height, our bound is much less useful, as in the following example:

Example. Let $\lambda=-t=4290$. We see that $\beta(4290)=18356909$, which is prime, and the prime factorization of $\lambda=(4290)=2*3*5*11*13$.We have, $\mathscr{A}=\{2,3,5,11,13\}$ and $\mathscr{B}=\emptyset$. Ξ has rank 0, so $\mathrm{rank}(E_{-4290})\leq 4$. A calculation using Sage reveals that $\mathrm{rank}(E_{-4290})=0$. We see that here, our upper bound is not very precise.

In this example, we must use Dirichlet characters to calculate our bound for the rank:

Example (see [1] p.199)**.** Let $\lambda=-t=-56$. We see that $\beta(-56)=3751=11^2*31$. The prime factorization of λ is $\lambda=-2^3*7$. We have, $\mathscr{A}=\{2,7\}$ and $\mathscr{B}=\{11,31\}$. Furthermore, we see that Ξ is given by

$$\Xi=\begin{pmatrix}\chi_{11}(2) & \chi_{11}(7)\\ \chi_{31}(2) & \chi_{31}(7)\end{pmatrix}.$$

Choosing $\chi_{11}(p)=p\ (mod\ 5)$ and $\chi_{31}(p)=p\ (mod\ 5)$, both non-trivial characters that satisfy our requirements, we see that Ξ has rank 1. Hence, $\mathrm{rank}(E_{-56})\leq 1$. A calculation using Sage gives us, $\mathrm{rank}(E_{-56})=1$.

5.3 Rank Distribution

We computed the ranks of elliptic curves, E_t, for all t such that height(t) $\leq$ 700. We assumed the Birch and Swinnerton-Dyer conjecture and used the `analytic_rank()` method in Sage. This method uses the Buhler-Gross algorithm, as implemented in GP by John Cremona and Tom Womack.

A summary of the results we found is below. The values in the second row indicate the upper bound on height and the values in row 3 to 7, column 2 to 4 indicate the percentage of curves with the respective rank and height bound.

Rank Distributions			
Rank	10	10^2	700
0	0.634921	0.392640	0.387439
1	0.349206	0.499096	0.492672
2	0.015873	0.103992	0.112306
3	0	0.004271	0.007102
4	0	0	0.000081

Remark. Looking at the preceding table, it appears that with parameters of larger height*, we get more curves of higher rank. In particular, the few curves of rank 4 that do occur, occur only when* height(t) >400*. This is consistent with the tendency for curves of higher rank to have coefficients of very large height in the Weierstrass equation, as a parameter of large height would cause the coefficients in the equation to also have large height.*

References

[1] Fisher, Tom. *Some Examples of 5 and 7 descent for elliptic curves over Q*. Journal of the European Mathematical Society, 3 (2001): 169-212.

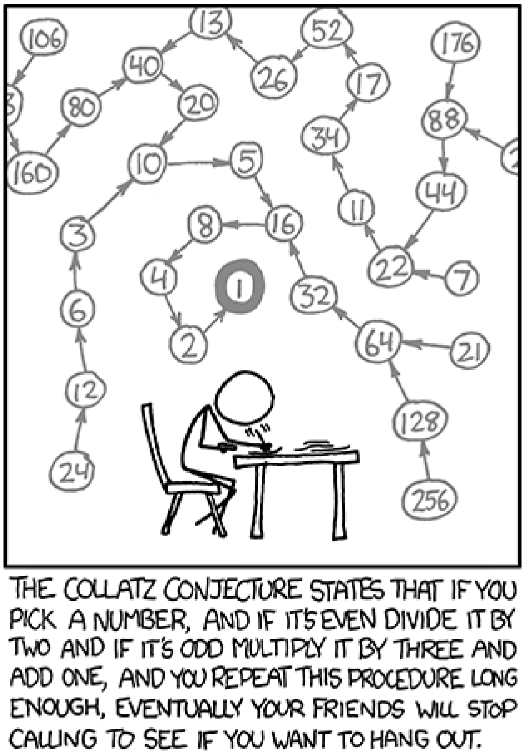
[2] Mazur, B. *Modular Curves and the Eisenstein Ideal*. IHES Publ. Math., 47 (1977): 33-186.

[3] Silverberg, A. *Open Questions in Arithmetic Algebraic Geometry. In "Arithmetic Algebraic Geometry," (B. Conrad and K. Rubin, eds)*. Park City: American Math. Soc. IAS/Park City, 1999.

[4] Silverman, J.H. *The Arithmetic of Elliptic Curves*. New York: Springer, 1986.

[5] Silverman, J.H., and Tate, J. *Rational Points on Elliptic Curves*. New York: Springer-Verlag, 1955.

Jokes


106
13
52
176
40
26
17
80
20
88
34
160
10
5
44
11
3
8
16
22
7
4
1
32
6
64
21
2
12
128
24
256
THE COLLATZ CONJECTURE STATES THAT IF YOU PICK A NUMBER, AND IF IT'S EVEN DIVIDE IT BY TWO AND IF IT'S ODD MULTIPLY IT BY THREE AND ADD ONE, AND YOU REPEAT THIS PROCEDURE LONG ENOUGH, EVENTUALLY YOUR FRIENDS WILL STOP CALLING TO SEE IF YOU WANT TO HANG OUT.

xkcd 710: *Collatz Conjecture*

□

An engineer hears that a famous mathematician will be giving a public lecture, and always having a soft spot for math, he attends. The mathematician then talks at length about all sorts of amazing phenomena that happen in some 17 dimensional space. The engineer, amazed at this mathematician's intuition for 17 dimensional space, goes up to him afterwards and asks "How do you picture 17 dimensions?", to which the mathematician answers "Oh, its easy. Just imagine n-dimensional space, and set n equal to 17." □

A mathematics professor was lecturing to a class of students. As he wrote something on the board, he said to the class "Of course, this is immediately obvious." Upon seeing the blank stares of the students, he turned back to contemplate what he had just written. He began to pace back and forth, deep in thought. After about 10 minutes, just as the silence was beginning to become uncomfortable, he brightened, turned to the class and said, "Yes, it IS obvious!" □

Singularly Perturbed Multiple State Dependent Delay Differential Equations

Daniel Bernucci

Delay differential equations (DDEs) are generalizations of ordinary differential equations used in modeling systems from economics to biology. This article deals with a class of DDEs wherein the delay is state-dependent. The one delay case will give us some insight on the stability of the solutions that will then be applied to construct periodic orbits to singularly perturbed DDEs with two delays. Conditions for the existence and stability of the solutions are then discussed.

1 Introduction

There is no doubt as to the usefulness of differential equations in the study of various physical phenomena. Differential equations are used to build models that are used in a number of fields, such as chemistry and engineering. However, in reality one often encounters delays as a result of the time it takes to react to an observed measurement. For this reason many models benefit by being described in terms of *delay differential equations* (DDE).

A DDE is an equation wherein the derivative of an unknown function depends of the values of the function at past times. Whereas to solve an ordinary differential equation one only needs to specify the value of the solution at a given time, to solve a DDE one needs to know the value of the solution on an interval of length equal to the delay. Thus a *history function* must be given as opposed to a simple *initial condition*. This history function describes the trajectory of the solution at past times. Hence an infinite-dimensional set of initial conditions must be given to solve even one linear DDE, thereby making DDEs infinite-dimensional problems. In this article we are interested in solving DDEs of the form

$$\dot{u}(t) = f(t, u(t), u(t-\tau_1(t,u(t))), u(t-\tau_2(t,u(t)))).$$

2 Single Delay Differential Equations

Consider the following DDE with delay $a + cu(t)$:

$$\varepsilon\dot{u}(t) = -\gamma u(t) - \kappa u(t-a-cu(t)), \tag{1}$$

where $\varepsilon, \gamma, \kappa, a,$ and c are positive constants.

Theorem 1. Any solution $u(t)$ to equation (1) remains bounded. More precisely, let $\phi(t)$ represent the history function and let $M = \max\{\frac{\kappa a}{\gamma c}, \phi(0)\}$. Then if $\phi(t) \geq -\frac{a}{c}$ for $t \in [-a-cM, 0]$, then

$$u(t) \in \left[-\frac{a}{c}, M\right]$$

for all $t > 0$.

Proof. First of all to find $\dot{u}(t)$ we need to know $u(t-a-cu(t))$ and in particular we should have that $t-a-cu(t) \leq t$ which in turn implies that

$$u(t) \geq -\frac{a}{c}.$$

If $u(t) = -\frac{a}{c}$ then we find that $t-a-cu(t) = t$ and

$$\varepsilon\dot{u}(t) = -\gamma\left(-\frac{a}{c}\right) - \kappa\left(-\frac{a}{c}\right) > 0.$$

So $\dot{u}(t) > 0$ hence u is increasing from $-a/c$. Thus $-a/c$ is indeed a lower bound. For an upper bound we note that when $u(t)$ has a local maximum, say B, then $\dot{u}(t) = 0$. So

$$\begin{aligned} 0 = \varepsilon\dot{u}(t) &= -\gamma B - \kappa u(t-a-cB) \\ &< -\gamma B - \frac{\kappa a}{c} \end{aligned}$$

and in particular

$$B < \frac{\kappa a}{\gamma c}.$$

Let now T be such that $u(T) > \frac{\kappa a}{\gamma c}$ and let $u(t) \in \left[-\frac{a}{c}, u(T)\right]$ for all $t \leq T$. Then

$$T - a - cu(T) < T - a\left(1 + \frac{\kappa}{\gamma}\right).$$

So

$$u(T-a-cu(T)) \in \left[-\frac{a}{c}, u(T)\right].$$

Hence

$$\varepsilon\dot{u}(t) < -(\gamma+\kappa)u(T) < 0.$$

So $\dot{u}(T) < 0$, which is a contradiction since we assumed $u(T) > \frac{\kappa a}{\gamma c}$ and we had that any local maximum satisfied $B < \frac{\kappa a}{\gamma c}$. Thus

$$u(t) \in \left[-\frac{a}{c}, \frac{\kappa a}{\gamma c}\right],$$

which completes the proof. □

Consider equation (1) with $\varepsilon \to 0$ (i.e., take $1 \gg \varepsilon > 0$.) Equation (1) becomes

$$\dot{u}(t) = \frac{1}{\varepsilon}[-\gamma u(t) - \kappa u(t-a-cu(t))]. \tag{2}$$

In particular,

$$\begin{aligned} -\gamma u(t) - \kappa u(t-a-cu(t)) &> 0 \Rightarrow \dot{u} \gg 0 \\ -\gamma u(t) - \kappa u(t-a-cu(t)) &< 0 \Rightarrow \dot{u} \ll 0 \end{aligned}$$

and so the solution tries to evolve with $-\gamma u(t) - \kappa u(t-a-cu(t)) = 0$, that is,

$$u(t) = -\frac{\kappa}{\gamma}u(t-a-cu(t)). \tag{3}$$

We construct a periodic solution to (1) with period T, with $t-a-cu(t) = (k-n)T$ for $t \in (kT, (k+1)T)$ as in Figure 1. We see that in this case

$$u(t) = \frac{-a+nT}{c} + \frac{t}{c}, \quad t \in (0,T). \tag{4}$$

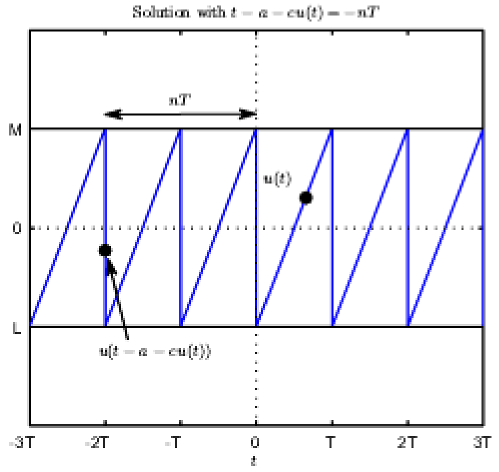


Figure 1: Solution of (1) with $t-a-cu(t)=-nT$, $t\in(0,T)$.

In this case we define the delay to be $\alpha(t,u(t)) = t-a-cu(t)$ and then the delayed term of the solution becomes $u(\alpha)$. Note that the delay in the above case is always between nT and $(n+1)T$, so $u(t)$ is always bounded away from $-\frac{a}{c}$. We find that

$$L := u(0) \quad = \quad \frac{-a+nT}{c} \tag{5}$$

$$M := u(T) \quad = \quad \frac{-a+(n+1)T}{c}. \tag{6}$$

So $u(t)\in\left[\frac{-a+nT}{c},\frac{-a+(n+1)T}{c}\right]$. Also note that the slope of $u(t)$ is $1/c$ for $t\in(kT,(k+1)T), k\in\mathbb{Z}$.

Now we need that

$$u(t) = -\frac{\kappa}{\gamma}u(t-a-cu(t)).$$

But $t-a-cu(t)=-nT$ and $u(t)=\frac{-a+nT}{c}+\frac{t}{c}$, so

$$\frac{-a+nT}{c}+\frac{t}{c} = -\frac{\kappa}{\gamma}u(\{-nT\})$$

where $u(\{-nT\})$ is set-valued, that is, can take any value in $[L,M]$.

Remark. A function $f:A\to B$ is said to be *set-valued* if it associates to every point in A one or more points in B. As such, f is not quite a function in the traditional sense since it is not single-valued. For instance, the function assigning to every nonzero complex number its square roots is set-valued, because every such number has two square roots, so $f(4)=\{-2,2\}$. In our case u associates to the value $-nT$ a whole range of values between L and M.

Thus

$$u(\{-nT\}) = \frac{\gamma}{\kappa c}(a-nT-t).$$

When $t=0$, we need $u(\{-nT\}) = \frac{\gamma}{\kappa c}(a-nT)$. Also $u(\{-nT\})\geq\frac{-a+nT}{c}$ and so

$$\frac{\gamma}{\kappa c}(a-nT-t)\geq\frac{-a+nT}{c} \quad \text{so}$$
$$t\leq\left(1+\frac{\kappa}{\gamma}\right)(a-nT).$$

But $0<t<T$ and so

$$T+\left(1+\frac{\kappa}{\gamma}\right)nT = a\left(1+\frac{\kappa}{\gamma}\right) \quad \text{so}$$
$$T=\frac{a(\gamma+\kappa)}{\gamma+n(\gamma+\kappa)}.$$

Using this value for T we can compute L and M independently of T using (5) and (6). We find

$$\begin{aligned} T &= \frac{a(\gamma+\kappa)}{\gamma+n(\gamma+\kappa)} \\ L &= \frac{-a\gamma}{c(\gamma+n(\gamma+\kappa))} \\ M &= \frac{a\kappa}{c(\gamma+n(\gamma+\kappa))}. \end{aligned}$$

We also can compute the amplitude $A=M-L$ of the solution $u(t)$, and we find it to be

$$A=\frac{T}{c}=\frac{a(\gamma+\kappa)}{c(\gamma+n(\gamma+\kappa))}.$$

From these computations we can draw the following conclusions:

Proposition 2. As $n\to\infty$ the previously constructed solution $u(t)$ to equation (1) approaches the solution $u(t)=0$ by oscillating about the t-axis.

Proof. As $n\to\infty$ we see that $M\downarrow 0$, $L\uparrow 0$, and $A\to 0$. The period T also approaches zero, but the slope of $u(t)$ for $t\in(kT,(k+1)T)$ remains constant. The proposition follows easily. (Figure 2 illustrates the behavior of the solutions as n varies.) □

Finally we find that for $k\in\mathbb{Z}$

$$u(t)=\frac{-a+nT+(t-kT)}{c}$$

for $t\in(kT,(k+1)T)$. For $t=kT$ the solution $u(t)$ is set-valued and can take any value in $[L,M]$,

$$u(\{kT\})=\left[\frac{-a\gamma}{c(\gamma+n(\gamma+\kappa))},\frac{a\kappa}{c(\gamma+n(\gamma+\kappa))}\right].$$

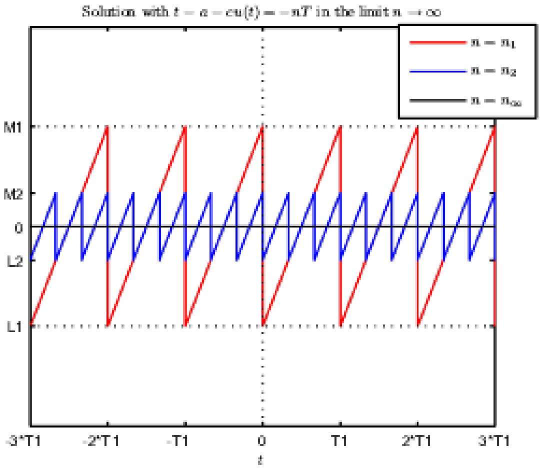


Figure 2: Solution of (1) with $t - a - cu(t) = -nT$ as $n \to \infty$. Mi, Li, Ti refer to the maxima, minima and period respectively of the solution corresponding to n_i. In this graph $n_1 < n_2 < n_\infty$.

We must just check that for $t = kT$ the solution stops increasing and decreases instantaneously. Without loss of generality take $k = 1$. At $t = kT = T$ let

$$u(T) = \frac{-a + (n+\theta)T}{c}, \qquad \theta \in [0,1].$$

For $\theta = 1, u(T) = M$. For $\theta = 0, u(t) = L$ and the solution restarts with $k = 2$.

Now we have $\varepsilon\dot{u}(T) = -\gamma u(T) - \kappa u(T - a - cu(T))$ and so we need

$$-\gamma u(T) - \kappa u(T - a - cu(T)) < 0 \tag{7}$$

for $\theta \in (0,1)$ since we want u to be decreasing. At $\theta = 0, 1$, (7) is already satisfied and in fact we get equality; so the solution stops increasing ($\theta = 1$) or decreasing ($\theta = 0$). In general, using the expression for $u(T)$ above we find

$$T - a - cu(T) = (1 - n - \theta)T.$$

By the periodicity of the solution,

$$u(T - a - cu(T)) = u(-\theta T).$$

But $-\theta T \in (-T, 0)$ and so

$$u(-\theta T) = \frac{-a + (n + 1 - \theta)T}{c}.$$

Then (7) becomes

$$-\gamma u(T) - \kappa u(T - a - cu(T)) = -\frac{a(\gamma+\kappa)}{c(\gamma + n(\gamma+\kappa))}(\theta - 1)(\gamma - \kappa).$$

Thus (7) is satisfied for $\theta \in (0,1)$ when $\kappa > \gamma$, which can be shown to be a necessary condition for the fixed point to be unstable, so holds in any case.

3 Multiple Delay Differential Equations with $c_1 = c_2$

In this section we study the DDE with two delays

$$\varepsilon\dot{u}(t) = -\gamma u(t) - \sum_{i=1}^{2} \kappa_i u(t - a_i - c_i u(t)) \tag{8}$$

where $\varepsilon, \gamma, \kappa_1, \kappa_2, a_1, a_2, c_1, c_2 > 0$.

Let $\alpha_i(t) = t - a_i - c_i u(t), i = 1, 2$. In the case where $c_1 = c_2 = c$ we have that

$$\alpha_1 - \alpha_2 = a_2 - a_1 = \text{constant}.$$

We further assume without loss of generality that $a_2 > a_1$. This then implies that

$$\alpha_2 < \alpha_1 < t.$$

In section 3.2, we will construct period orbits of period T where for $t \in (kT, (k+1)T)$ the delayed times will satisfy $\alpha_1 = kT$ and $\alpha_2 = (k - \theta)T$ where $\theta \in (0,1)$ is defined below.

3.1 Properties of Multiple Delay Differential Equations with $c_1 = c_2$

The following results are taken from Felicia Magpantay's thesis and are stated here for completeness.

Theorem 3. If $\gamma \geq \kappa_2$ and the history function $\phi(t) \in \left[-\frac{a_1}{c}, \frac{a_1(\kappa_1+\kappa_2)}{c\gamma}\right]$ for all $t \in \left[-a_2 + \frac{a_1(\kappa_1+\kappa_2)}{\gamma}, 0\right]$ then $u(t) \in \left[-\frac{a_1}{c}, \frac{a_1(\kappa_1+\kappa_2)}{c\gamma}\right]$ for all $t > 0$.

Theorem 4. The condition that $\kappa_1 + \kappa_2 > \gamma$ is a necessary but not a sufficient condition for the instability of the fixed point.

3.2 Singularly Perturbed Solutions

We will now construct a general solution in the limit $\varepsilon \to 0$ in which for $t \in (kT, (k+1)T)$ $\alpha_1 = kT$ and $\alpha_2 = (k - \theta)T$ where T is again the period. Such a solution is depicted in Figure 3.

Theorem 5. Let $\kappa_1 > \gamma > \kappa_2$,

$$a_2 > a_1 \left[1 + \frac{\kappa_2}{\gamma + \kappa_2}\right], \tag{9}$$

$$T = \frac{a_1(\gamma + \kappa_1) + \kappa_2 a_2}{\gamma + \kappa_2} \tag{10}$$

and

$$\theta = \frac{a_2 - a_1}{T}. \tag{11}$$

Then when the parameters $a_1, a_2, \gamma, \kappa_1, \kappa_2$ are chosen so that $\theta \in \left(\frac{\kappa_2}{\kappa_1+\kappa_2-\gamma}, 1\right)$, equation (8) has a periodic solution $u(t)$ of period T in the limit $\varepsilon \to 0$ where

$$u(t) = \frac{-a_1 + (t - kT)}{c} \qquad \text{for } t \in (kT, (k+1)T),$$

the solution is set-valued for $t = kT$ and can take any value in $\left[-\frac{a_1}{c}, \frac{-a_1+T}{c}\right]$, and for all t, $\alpha_1 - \alpha_2 = a_2 - a_1 = \theta T$.

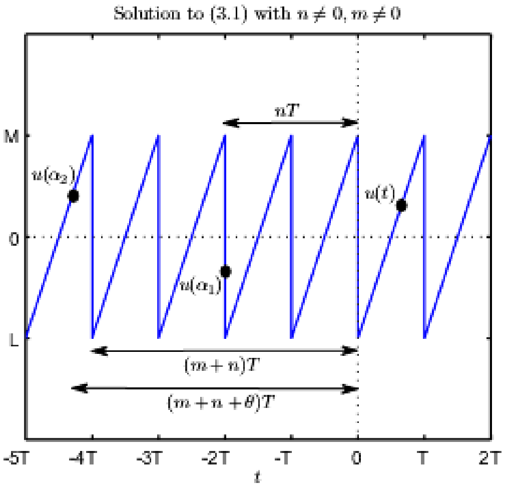


Figure 3: Setup for the solution of (8) with $\alpha_1 = -nT, \alpha_2 = -(m+n+\theta)T$, $t \in (0,T)$. We are considering $n = m = 0$.

Proof. Generalizing the work done in section 2 we find that for $0 < t < T$ the solution $u(t)$ can be described as

$$\begin{aligned} u(t) &= \frac{-a_1+t}{c} \\ u(\alpha_1) &= \left[-\frac{a_1}{c}, \frac{-a_1+T}{c}\right] \qquad (12) \\ \alpha_1(t) &= t - a_1 - cu(t) = 0 \\ \alpha_2(t) &= t - a_2 - cu(t) = a_1 - a_2 < 0 \end{aligned}$$

where we then choose $\theta \in (0,1)$ to satisfy (11) and $u(\alpha_1)$ is set-valued. It now follows that

$$u(\alpha_2) = \frac{-a_2+T}{c}.$$

Our next step is finding an expression for T and verifying that

$$0 = \gamma u(t) - \kappa_1 u(\alpha_1) - \kappa_2 u(\alpha_2) \qquad (13)$$

holds for $t \in (0,T)$. To this end we use (12), keeping in mind that as $t \to T^-, u(\alpha_1) \to -\frac{a_1}{c}$. The expression for T in (10) is simply found by substituting the expressions for $u(T), u(\alpha_1)$ and $u(\alpha_2)$ into (13) and solving for T. For $t \in (0,T)$, $u(\alpha_1)$ is set-valued, so we can write

$$u(\alpha_1) = \frac{-a_1+\mu_1 T}{c}$$

where $\mu_1 \in [0,1]$. For $\mu_1 = 1$, the left-hand side of (13) is negative while for $\mu_1 = 0$ it is positive. The intermediate value theorem therefore guarantees that there is some $\mu_1 \in [0,1]$ such that (13) holds.

We must now consider how the solution behaves when $t = T$. We will have that $u(T) \in \left[-\frac{a_1}{c}, \frac{-a_1+T}{c}\right]$ and so we can set

$$u(T) = \frac{-a_1+\mu T}{c} \qquad \text{for } \mu \in [0,1].$$

Once again we need that for $\mu \in (0,1)$

$$-\gamma u(T) - \kappa_1 u(\alpha_1(T)) - \kappa_2 u(\alpha_2(T)) < 0 \qquad (14)$$

where we find that

$$\alpha_1(T) = (1-\mu)T.$$

Therefore

$$u(\alpha_1) = \frac{-a_1+(1-\mu)T}{c}.$$

By a similar computation we get

$$\alpha_2(T) = (1-\mu-\theta)T.$$

Hence $\alpha_2(T) = 0$ when $\mu = 1-\theta$.

We get three cases.

Case 1: $\mu \in (1-\theta, 1)$
In this case

$$-\theta < 1-\mu-\theta < 0$$

We then have that

$$u(\alpha_2) = \frac{-a_1+(2-\mu-\theta)T}{c}.$$

Using these values we verify (14).

$$\begin{aligned} -\gamma u(T) - &\kappa_1 u(\alpha_1) - \kappa_2 u(\alpha_2) \\ &= \frac{T}{c}((1-\mu)(\gamma-\kappa_1-\kappa_2)). \end{aligned}$$

This implies that we need $\kappa_1 + \kappa_2 > \gamma$, an already necessary condition to ensure the instability of the fixed point.

Case 2: $\mu \in (0, 1-\theta)$
We deduce that

$$0 < 1-\mu-\theta < 1-\theta.$$

This then implies that

$$u(\alpha_2) = \frac{-a_1+(1-\mu-\theta)T}{c}.$$

We now put the values of $u(T), u(\alpha_1), u(\alpha_2)$ and T into (14) and get

$$\begin{aligned} -\gamma u(T) - &\kappa_1 u(\alpha_1) - \kappa_2 u(\alpha_2) \\ &= \frac{T}{c}((\gamma-\kappa_1)(1-\mu)+\mu\kappa_2). \end{aligned}$$

We find that

$$0 < \frac{\mu}{1-\mu} < \frac{\kappa_1-\gamma}{\kappa_2}$$

must be satisfied for all $\mu \in (0, 1-\theta)$ therefore $\kappa_1 > \gamma$ and

$$1 > \theta > \frac{\kappa_2}{\kappa_1+\kappa_2-\gamma} > 0.$$

Writing θ in terms of the parameters using (11) we are able to deduce condition (9).

Case 3: $\mu = 1-\theta$
We know that $\alpha_2 = 0$ and that $u(\alpha_2)$ is set-valued,

$$u(\alpha_2) = \left[-\frac{a_1}{c}, \frac{-a_1+T}{c}\right].$$

We compute $u(T)$ and $u(\alpha_1)$ and find

$$\begin{aligned} u(T) &= \frac{-a_2+T}{c} \\ u(\alpha_1) &= \frac{a_2-2a_1}{c} \end{aligned}$$

Imposing (14) gives

$$\begin{aligned} -\gamma&\left(\frac{-a_2+T}{c}\right) \qquad (15) \\ &-\kappa_1\left(\frac{a_2-2a_1}{c}\right) - \kappa_2 u(\alpha_2) < 0. \end{aligned}$$

First we put $u(\alpha_2) = -\frac{a_1}{c}$ in (15) and we find a condition equivalent to $\theta > \frac{\kappa_2}{\kappa_1+\kappa_2-\gamma}$ found in Case 2. Now if we let $u(\alpha_1) = \frac{-a_1+T}{c}$ in (15), we once again obtain the condition $\kappa_1+\kappa_2 > \gamma$. By the linearity of $u(\alpha_2)$ in (15), the fact that the equation holds at both extremes of the interval $\left[-\frac{a_1}{c}, \frac{-a_1+T}{c}\right]$ implies that it holds for all values in between as well. This completes the proof. □

The conditions $\theta \in \left(\frac{\kappa_2}{\kappa_1+\kappa_2-\gamma}, 1\right)$ for the existence of the periodic orbit in Theorem 3.3 can be translated into explicit inequalities that must be satisfied by the parameters. Using (11) and (10) we can express θ in terms of the parameters. Enforcing the bounds on θ we find two lower bounds on κ_1, where either of them may be greater than the other, depending on the values of κ_2, γ, a_1 and a_2. Together all these conditions tell us where these periodic orbits are defined as well as their stability.

Of interest now is to know what happens when κ_1 is chosen to be small, or when (9) fails. This leads us to study where Hopf bifurcations may occur. Also we are interested in finding periodic orbits in other regions as well, which we achieve by taking $n \neq 0$ and/or $m \neq 0$. Results obtained in those cases are analogous to the ones presented here and are omitted.

4 Applications of State-Dependent DDEs

In many models involving feedback control mechanisms, DDEs are frequently used to model the time required to react to a change in the state of the system. In this section we explain how DDEs, and in particular state-dependent DDEs, occur in practice by considering an example from biology. We will consider an equation first proposed by Mackey [2] to study an autoimmune disease that causes periodic drops in red blood cell (RBC) levels in the blood. As a result of the negative feedback control, the Mackey equation (also known as the Mackey-Glass equation) shows limit cycle oscillations.

The way the delay occurs is as follows. When RBC levels are low, the body produces a hormone, erythropoeitin, that ramps up the production of cells responsible for generating RBCs. When the RBCs are fully matured after a few days, erythropoeitin production is slowed. Hence the maturation time of RBC causes the delay in the negative feedback mechanism. Mackey modeled the situation as

$$\dot{E}(t) = FE(t'-\tau') - \gamma E$$

where E is the density of RBCs, F describes the influx of RBCs, and τ' and γ are constants describing the maturation time and the loss rate of RBCs, respectively. These parameters can be estimated experimentally. In turn F can be written as

$$F = F_0 \frac{\theta^p}{E^p(t'-\tau')+\theta^p}$$

where again the parameters carry biological significance. Appropriate changes of variables can turn this equation into the dimensionless form

$$\dot{u}(t) = \frac{1}{1+u(t-\tau)^p} - bu$$

which is a delay differential equation.

Furthermore, it has been observed that in periods of deficit, production of cells is not only ramped up, but the maturation time is actually *shorter*. This suggests that the delay is not constant, but rather state-dependent, in that the delay changes depending on the cell density at the present time.

5 Conclusion

In most scientific models and mathematical theory, the delay time of DDEs is assumed to be fixed, but in applications there is much evidence that these delays are actually state-dependent. However, the lack of mathematical theory of such equations motivates this article's discussion of multiple delay nonlinear differential equations with linearly state-dependent delays.

After briefly outlining some basic properties of single delay equations, we constructed a periodic solution to a singularly perturbed equation with two delays, where we noticed the important role the parameters play in both the existence and stability of the periodic orbits. The next generalization of these results comes from studying the behavior of the solutions when the second delay "gets stuck" in the vertical transition layer. It has been observed that the solutions then bifurcate to other solutions exhibiting a double spike. The analysis of these solutions is in progress and should prove to be very interesting.

6 Acknowledgements

I would firstly like to thank Professor Tony Humphries, with whom this project was completed, for his guidance and patience in introducing this and other topics to me. My thanks also go to Felicia Magpantay for allowing me to use some of her results in this article, as well as to NSERC and McGill University for funding.

References

[1] Bellman, Richard, and Kenneth L. Cooke. *Differential-Difference Equations*. New York: Academic Press, 1963.

[2] Erneux, Thomas. *Applied Delay Differential Equations*. New York: Springer, 2009.

[3] Strogatz, Steven H. *Nonlinear Dynamics and Chaos*. Cambridge, MA: Westview, 2007.

PRIME NUMBERS: SOLITARY YET UBIQUITOUS

Cathryn Supko

Typically if your average Joe walks into a bookstore and sees a novel with the words “prime number” in its title, he won’t touch it with a ten foot pole, but Paolo Giordano’s *The Solitude of Prime Numbers* has become an International Bestseller. Giordano, who is not a writer by trade but rather received a Ph.D. in Theoretical Physics, uses references to the field of Mathematics not only in his title but also in analogies throughout the book. He manages to do so in a way that makes the novel very enjoyable and easy to relate to for those of us who spend significant portions of our lives doing math, while remaining accesible to readers who have never taken a calculus course.

The plot traces its two emotionally damaged, sociophobic main characters from elementary school until adulthood. Mattia, who was involved in the disappearace of his twin sister at a very young age, uses his intelligence to seek refuge from the real world by focusing on the study of mathematics. In his teens he meets Alice, who similarly suffered trauma at a young age and as a result is also misunderstood by her peers. The pair has an obvious emotional connection beginning when they first meet, but are too removed from reality to be able to communicate their feelings for one another.

While writing from the perspective of Mattia, one of the most significant techniques used to relate Mattia’s thoughts is Giordano’s incorporation of his knowledge of the study of math and the culture surrounding it. The primary analogy Giordano uses compares Mattia’s loneliness to prime numbers, because similarly to him, they “ended up in that sequence by mistake, that they’d been trapped,... that they too would have preferred to be like all the others, just ordinary numbers, but for some reason they couldn’t do it.” This analogy is extended to explain that he and Alice are like twin primes, “always close to each other, almost neighbors, but between them there is always an even number that prevents them from truly touching.” His application of this concept is explained well enough for anyone to understand, but for mathematicians it relates the ideas of emotional detachment and prime numbers, both of which we are familiar with, in a unique manner.

As Mattia’s education in math progresses throughout the rest of the novel, math references are used both as a description of how he spends his time and as an analogy for his desire to be distanced from social interation. Giordano depicts Mattia as being stereotypically inept with respect to social interraction. Mattia’s inability to deal with reality is highlited when he meets Nadia, a woman who demonstrates romantic interest in him, and rather than becoming emotionally involved in the conversation, “remained absorbed by one of the big earrings that dangled from her ears: a gold circle at least five meters in diameter, which when she moved began swinging in a complicated motion that Mattia tried to decompose into the three Cartesian axes.” This portrayal is intensified by explaining that, when Nadia and he kiss, Mattia “thought of the circular movement of his own tongue, its periodic motion”. The mathematical language that is used in these descriptions constructs a barrier between Mattia and reality, and demonstrates the sentiment felt by many math students that one can easily use the abstract subject to keep a healthy distance from reality.

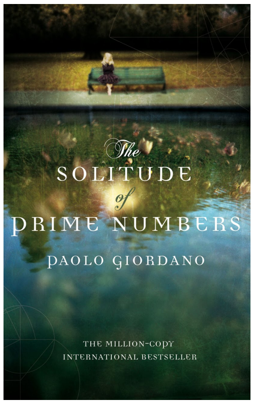


Figure 1: Cover of *The Solitude of Prime Numbers*

One of the main focuses of Mattia’s life as a mathematician is his work on a particularly difficult proof. In describing his work, Giordano explains that Mattia felt as if “he was always stuck on the same step. No matter where they began the proof, he and Alberto always ended up banging their heads against it sooner or later.” While Mattia is cleaning the blackboard after having found the solution, he realizes that “no one would really have understood it, but they were already jealous of the result, as one is of a beautiful secret.” He mentions later in the novel, when attempting to reestablish relationships that he has neglected from his focus on work, that “over time he had become convinced that he no longer knew how to do anything outside of his element, the ordered and transfinite sets of mathematics.” The extreme emotions portrayed by Giordano describing the process of working on a difficult proof are remarkably accurate, leading the mathematically educated reader to sympathize further with Mattia’s tendency to be detached from the real world.

Despite the fact that by the end of the novel you likely still will not have any idea of what algebraic topology is, Giordano’s novel gives readers of all levels of mathematical knowledge a good sense of the emotional journey of both of his characters, which is intensified by the incorporation of mathematical concepts.

□

On the Generalization of a Hardy-Ramanujan Theorem and the Erdos Multiplication Table Problem

Crystel Bujold

In this article we present a generalization of the Hardy-Ramanujan theorem, wherein, for a given number x, we bound the number of prime factors p of an integer $n < x$, with the prime factors coming from a given set. We then proceed to a generalization of the Erdös multiplication table problem. Given the set of primes and number x, we bound the number of distinct integers which can be written as the product of integers $a, b < x$, where we again assume all prime factors are from our given set of primes.

1 Introduction

- " $2 \times 2 = 4, 2 \times 3 = 6, 2 \times 4 = 8...$",
  sing the kids as a choir.
- " Don't forget kids! Tomorrow we have a test;
  finish studying your multiplication table up to 10,
  you have to know it on the tip of your fingers."

Who doesn't remember hearing that as a child? From the earliest age, numbers enter our lives and their magic becomes one of our daily tools and object of study. And yet, we grow so used to them, that we tend to forget how fascinating they are! In fact do we really understand them? Can we even answer this simple question;

" Let x be an integer, how many distinct integers are there in the x by x multiplication table? "

For example, consider the 10 x 10 multiplication table. Clearly, this table contains 100 entries, but in fact, it turns out that only 43 of those are distinct. Would we have been able to predict it?

This problem, known as the " Erdös multiplication table problem ", was proposed by Paul Erdös in 1960 [2], after which he proved an upper bound using a famous theorem of Hardy and Ramanujan [1]. Indeed, using the Hardy-Ramanujan inequality for the number of integers $n \leq x$ with exactly k prime factors

$$\pi_k(x) \leq \frac{C_1 x}{\log x} \frac{(\log\log x + C_2)^{k-1}}{(k-1)!},$$

he showed that the number of distinct integers $A(x)$ in the $x \times x$ table is

$$A(x) \ll \frac{x^2}{(\log x)^{1-\frac{1+\log\log 2}{\log 2}}}.$$

As simple as the problem may seem, finding a good lower bound for the number of distinct integers in a multiplication table is a tricky problem that is still under investigation today. Namely, in the line of his work on divisors, in [5] Kevin Ford works out the bound

$$A(x) \gg \frac{x^2}{(\log x)^{1-\frac{1+\log\log 2}{\log 2}} (\log\log x)^{\frac{3}{2}}}$$

as a consequence of his results on divisors of integers in a given interval.

But we can push the question further; what if we only want to count the integers in the table that belong to a given set? What if we consider a k-dimensional table, i.e. could we count how many integers $n \leq x^k$ such that $n = m_1 m_2 ... m_k$ and $m_i \leq x$ for all $i \leq k$? What about if we only multiply integers from a given set? Could we find (good) bounds for the number of distinct entries in the table?

The two first questions have been investigated by Dimitris Koukoulopoulos, in particular the special case of the integers belonging to the set of shifted primes and the $k+1$-dimensional multiplication table problem, for which he determines bounds. We invite the reader to see [6] for further details.

The third question will be the one we will focus on. In the following article we'll turn our attention towards the integers composed of prime factors from a given set $\mathscr{P}$, and study an analogue of the original problem of Erdös in such a case. We will first use techniques similar to those of Erdös, in particular, we'll use a variation of the Hardy-Ramanujan theorem to prove an upper bound for the restricted problem. Then, we'll show, under some assumptions, a corresponding lower bound using simple estimates.

2 Preliminaries

2.1 Notation and definitions

Let's start by giving some definitions and translate our problem into more mathematical language.

First, let $\mathscr{P}$ be a given set of primes, $S(\mathscr{P})$ be the set of integers with prime factors in $\mathscr{P}$, and $S^*(\mathscr{P})$ be restricted to the squarefree such integers (i.e. all prime factors of the integers have multiplicity 1), that is

$$S(\mathscr{P}) = \{n : p | n \Rightarrow p \in \mathscr{P}\}$$
$$S^*(\mathscr{P}) = \{n : p | n \Rightarrow p \in \mathscr{P} \text{ and } p^2 \nmid n\}.$$

Define

$$L(x) = \sum_{\substack{p \le \sqrt{x} \\ p \in \mathscr{P}}} \frac{1}{p} + c_1$$

where c_1 is an absolute constant to be defined.
Also let $\omega(n)$ denote the number of distinct prime factors of the integer n,

$$\omega(n) = \sum_{p^\alpha \| n} 1$$

where $\|$ means " divides exactly " (i.e. p^α divides n but $p^{\alpha+1}$ doesn't divide n). Define the number of integers $n \in S(\mathscr{P})$ up to x with exactly k prime factors from $\mathscr{P}$ (without multiplicity) to be

$$\pi_{k,\mathscr{P}}(x) = \#\{n \le x : \omega(n) = k, \quad n \in S(\mathscr{P})\}.$$

For a restricted set of squarefree integers define

$$\pi^*_{k,\mathscr{P}}(x) = \#\{n \le x : \omega(n) = k, \quad n \in S^*(\mathscr{P})\}.$$

Finally, we define

$$A(x) = \#\{n \le x^2 : n = ab,\ a \le x,\ b \le x,\ n \in S(\mathscr{P})\}$$

$$A^*(x) = \#\{n \le x^2 : n = ab,\ a \le x,\ b \le x,\ n \in S*(\mathscr{P})\}.$$

Here, $A(x)$ corresponds exactly to the object of the problem in which we are interested, i.e. the set of distinct integers (with prime factors from $\mathscr{P}$) in the multiplication table.

Throughout this article $f(x) \ll g(x)$ means that $f(x) \le Cg(x)$ for some constant C and $f(x) = O(g(x))$ means that $\mid f(x) \mid \le M \mid g(x) \mid$ for some constant M, for all x large enough.

2.2 *A variation of the Hardy-Ramanujan theorem*

Theorem 0. There exists an absolute constant c_2, such that, for $x \ge 1$,

$$\pi_{k,\mathscr{P}}(x) \le \frac{c_2 x}{\log(x)} \frac{L(x)^{k-1}}{(k-1)!}. \qquad (1)$$

Proof. We prove the theorem by induction on k.
By the prime number theorem, if we let $\mathscr{P}$ be all the primes in $\mathbb{Z}$, then there exists an absolute constant c such that

$$\pi(x) \le \frac{cx}{\log x}.$$

That is, the case $k = 1$ holds for any set $\mathscr{P}$ since

$$\pi_{1,\mathscr{P}}(x) \le \pi(x) \le \frac{c_2 x}{\log x}$$

for $c_2 \ge c$.
Assume now that the theorem holds for $k-1$. We have that

$$(k-1)\pi_{k,\mathscr{P}}(x) \le \sum_{\substack{p^2 \le x \\ p \in \mathscr{P}}} \pi_{k-1,\mathscr{P}}\left(\frac{x}{p}\right) + \sum_{\substack{p^3 \le x \\ p \in \mathscr{P}}} \pi_{k-1,\mathscr{P}}\left(\frac{x}{p^2}\right) + \sum_{\substack{p^4 \le x \\ p \in \mathscr{P}}} \pi_{k-1,\mathscr{P}}\left(\frac{x}{p^3}\right) + \cdots \qquad (2)$$

Indeed, we first note that since $k \ge 2$, then if $n = p_1^{\alpha_1} p_2^{\alpha_2} ... p_k^{\alpha_k}$ is the prime factorization (in increasing order) of an integer counted in $\pi_{k,\mathscr{P}}(x)$, then for all $i < k$ we have $p_i^{\alpha_i+1} \le p_i^{\alpha_i} p_k^{\alpha_k} \le n \le x$. Hence, to count all the integers smaller than x and having exactly k prime factors, it is more than enough to count, for each $p \in \mathscr{P}$ such that $p^{\alpha+1} \le x$, the number of integers $m \le \frac{x}{p^\alpha}$ having exactly $k-1$ prime factors. Doing so, we get

$$p^\alpha m = p^\alpha (p_1^{\alpha_1} p_2^{\alpha_2} ... p_{k-1}^{\alpha_{k-1}}) \le x$$

which has exactly k prime factors.

In other words, summing over $\pi_{k-1,\mathscr{P}}(\frac{x}{p^\alpha})$ for all $p^{\alpha+1} \le x$, we in fact count at least $k-1$ times each integer $n \le x$ having exactly k prime factors; once for each prime factors of n that is not the largest. From this we get the inequality (2).

Now, by the induction hypothesis, from (2) we have

$$\pi_{k,\mathscr{P}}(x) \le \frac{c_2}{k-1} \left(\sum_{\substack{p^2 \le x \\ p \in \mathscr{P}}} \frac{x}{p \log(\frac{x}{p})} \frac{L(x)^{k-2}}{(k-2)!} + \sum_{\substack{p^3 \le x \\ p \in \mathscr{P}}} \frac{x}{p^2 \log(\frac{x}{p^2})} \frac{L(x)^{k-2}}{(k-2)!} + \cdots \right)$$

as $L(\frac{x}{\alpha}) \le L(x)$.
This last equation can now be factored as follows;

$$\pi_{k,\mathscr{P}}(x) \le \frac{c_2 x}{(k-1)!} L(x)^{k-2} \left(\sum_{\substack{p^2 \le x \\ p \in \mathscr{P}}} \frac{1}{p \log(\frac{x}{p})} + \sum_{\substack{p^3 \le x \\ p \in \mathscr{P}}} \frac{1}{p^2 \log(\frac{x}{p^2})} + \cdots \right).$$

Hence, it suffices to show that

$$\sum_{\substack{p^2\le x\\ p\in\mathscr{P}}} \frac{1}{p\log(\frac{x}{p})} + \sum_{\substack{p^3\le x\\ p\in\mathscr{P}}} \frac{1}{p^2\log(\frac{x}{p^2})} + \sum_{\substack{p^4\le x\\ p\in\mathscr{P}}} \frac{1}{p^3\log(\frac{x}{p^3})} + \cdots \le \frac{1}{\log x}\left(\sum_{\substack{p^2\le x\\ p\in\mathscr{P}}}\frac{1}{p}+c_1\right). \tag{3}$$

That is, to show the theorem, we now prove two lemmas, which will allow us to bound the previous summation in two steps. We begin with an upper bound for the first term of the summation in the first lemma, and an upper bound for the remaining terms in the second lemma.

Lemma 1. For any set of primes $\mathscr{P}$, we have

$$\sum_{\substack{p^2\le x\\ p\in\mathscr{P}}} \frac{1}{p\log(\frac{x}{p})} \le \frac{1}{\log x}\left(\sum_{\substack{p^2\le x\\ p\in\mathscr{P}}}\frac{1}{p}+c_3\right)$$

where c_3 is a constant.

Proof. We first note that the lemma follows if and only if

$$\log x \sum_{\substack{p^2\le x\\ p\in\mathscr{P}}} \frac{1}{p\log(\frac{x}{p})} \le \sum_{\substack{p^2\le x\\ p\in\mathscr{P}}}\frac{1}{p}+c_3$$

$$\Leftrightarrow \sum_{\substack{p^2\le x\\ p\in\mathscr{P}}}\left(\frac{\log x}{p\log(\frac{x}{p})}-\frac{1}{p}\right)\le c_3.$$

This can be deduced by some manipulations as follows:

$$\begin{aligned}\sum_{\substack{p^2\le x\\ p\in\mathscr{P}}}\left(\frac{\log x}{p\log(\frac{x}{p})}-\frac{1}{p}\right) &= \sum_{\substack{p^2\le x\\ p\in\mathscr{P}}}\frac{\log x-\log(\frac{x}{p})}{p\log(\frac{x}{p})}\\ &= \sum_{\substack{p^2\le x\\ p\in\mathscr{P}}}\frac{\log p}{p(\log(x)-\log(p))}\\ &= \sum_{\substack{p^2\le x\\ p\in\mathscr{P}}}\frac{\log p}{p\log x(1-\frac{\log p}{\log x})}.\end{aligned}$$

As $p\le\sqrt{x}$, we get that

$$\sum_{\substack{p^2\le x\\ p\in\mathscr{P}}}\frac{\log x-\log(\frac{x}{p})}{p\log(\frac{x}{p})}\le\frac{2}{\log x}\sum_{\substack{p^2\le x\\ p\in\mathscr{P}}}\frac{\log p}{p}.$$

Now, from the well known relation we get

$$\sum_{p\le x}\frac{\log p}{p}=\log x+O(1)$$

and thus obtain

$$\begin{aligned}\sum_{\substack{p^2\le x\\ p\in\mathscr{P}}}\frac{\log x-\log(\frac{x}{p})}{p\log(\frac{x}{p})} &\le \frac{2}{\log x}\left(\frac{1}{2}\log x+O(1)\right)\\ &\le 1+O\left(\frac{1}{\log x}\right)\end{aligned}$$

which proves the Lemma. □

Now, we show that the sum of the remaining terms in equation (3) is $O\left(\frac{1}{\log x}\right)$.

Lemma 2. For any set of primes $\mathscr{P}$, we have

$$\sum_{\substack{p^3\le x\\ p\in\mathscr{P}}}\frac{1}{p^2\log(\frac{x}{p^2})}+\sum_{\substack{p^4\le x\\ p\in\mathscr{P}}}\frac{1}{p^3\log(\frac{x}{p^3})}+\cdots\le\frac{C}{\log x}$$

where C is a constant.

Proof. We first note that if $p^\alpha\le x$ then

$$\begin{aligned}p &\le x^{\frac{1}{\alpha}}\\ p^{\alpha-1} &\le x^{1-\frac{1}{\alpha}}\\ \frac{x}{p^{\alpha-1}} &\ge x^{\frac{1}{\alpha}}\end{aligned}$$

$$\Rightarrow\frac{1}{\log\left(\frac{x}{p^{\alpha-1}}\right)}\le\frac{\alpha}{\log x}.$$

That is,

$$\sum_{\alpha=2}^{\frac{\log x}{\log 2}}\sum_{\substack{p\le x^{\frac{1}{\alpha+1}}\\ p\in\mathscr{P}}}\frac{1}{p^\alpha\log(\frac{x}{p^\alpha})}\le\frac{1}{\log x}\sum_{\alpha=2}^{\frac{\log x}{\log 2}}(\alpha+1)\sum_{n\ge2}\frac{1}{n^\alpha}$$

and since

$$\begin{aligned}\sum_{n\ge2}\frac{1}{n^\alpha} &\le \frac{1}{2^\alpha}+\int_2^\infty\frac{1}{t^\alpha}dt\\ &\le \frac{1}{2^\alpha}+\frac{1}{(\alpha-1)2^{\alpha-1}}\le\frac{1}{2^\alpha}+\frac{1}{2^{\alpha-1}}\\ &\le \frac{3}{2^\alpha}\end{aligned}$$

we get that

$$\sum_{\alpha=2}^{\frac{\log x}{\log 2}} \sum_{\substack{p\le x^{\frac{1}{\alpha+1}} \\ p\in\mathscr{P}}} \frac{1}{p^\alpha \log(\frac{x}{p^\alpha})} \le \frac{3}{\log x}\sum_{\alpha\ge 2}\frac{\alpha+1}{2^\alpha}$$
$$= \frac{15}{2\log x}.$$

□

This proves Lemma 2 and terminates the proof of the theorem. □

Note that as $\pi^*_{k,\mathscr{P}}(x) \le \pi_{k,\mathscr{P}}(x)$, Theorem 0 holds also in the case of squarefree integers.

It is worth mentioning that this variation of the Hardy-Ramanujan theorem can be proven using the Túran-Kubilius inequality, see [7] for more details.

3 Upper bound for $A(x)$

With this inequality in hand, we can now prove an easy upper bound for $A(x)$, which we will then improve for the case $L(x) > \frac{1}{2\log 2}\log\log x$.

Theorem 1(a). If $L(x) \gg 1$ then

$$A(x) \ll \frac{x^2}{\log^2 x}e^{2L(x)}.$$

Proof. We start by writing

$$A(x) \le \big(\#\{a\in S(\mathscr{P}) : a\le x\}\big)^2.$$

We have that

$$\begin{aligned}\#\{a\in S(\mathscr{P}) : a\le x\} &= \sum_{k=0}^{\infty}\pi_{k,\mathscr{P}}(x) \\ &\le 1 + \frac{c_2 x}{\log(x)}\sum_{k=0}^{\infty}\frac{L(x)^{k-1}}{(k-1)!} \\ &= 1 + c_2\frac{x}{\log x}e^{L(x)} \\ &\le 2c_2\frac{x}{\log x}e^{L(x)}.\end{aligned}$$

By squaring, we get that

$$A(x) \ll \frac{x^2}{\log^2 x}e^{2L(x)}$$

as desired. □

We now improve this bound in the case where $L(x)$ is close to $\log\log x$.

Theorem 1(b). If $L(x) > \frac{1}{2\log 2}\log\log x$, define α by $L(x) = \alpha\log\log x$, then

$$A(x) \ll \frac{x^2}{(\log x)^{1-\frac{1}{\log 2}(1+\log\alpha+\log\log 2)}}.$$

Proof. We start by proving a lemma we will be using for the proof of the theorem;

Lemma 3. Let $t\in\mathbb{R}^+$ and $0<\varepsilon\le 1$.

i If $N < (1-\varepsilon)t$, then

$$\sum_{k\le N}\frac{t^k}{k!} \le \varepsilon^{-1}\frac{t^N}{N!},$$

ii If $N > (1+\varepsilon)t$, then

$$\sum_{k\ge N}\frac{t^k}{k!} \le 2\varepsilon^{-1}\frac{t^N}{N!}.$$

Proof. For (i), we have

$$\begin{aligned}\sum_{k\le N}\frac{t^k}{k!} &= \frac{t^N}{N!}\left(1+\frac{N}{t}+\frac{N(N-1)}{t^2}+\cdots\right) \\ &\le \frac{t^N}{N!}\left(1+(1-\varepsilon)+(1-\varepsilon)^2+\cdots\right) \\ &\le \frac{1}{\varepsilon}\frac{t^N}{N!}.\end{aligned}$$

Similarly, for (ii), we have

$$\begin{aligned}\sum_{k\ge N}\frac{t^k}{k!} &= \frac{t^N}{N!}\left(1+\frac{t}{(N+1)}+\frac{t^2}{(N+1)(N+2)}+\cdots\right) \\ &\le \frac{t^N}{N!}\left(1+\frac{1}{(1+\varepsilon)}+\frac{1}{(1+\varepsilon)^2}+\cdots\right) \\ &\le \frac{1}{1-\frac{1}{1+\varepsilon}}\frac{t^N}{N!} \le \frac{2}{\varepsilon}\frac{t^N}{N!}.\end{aligned}$$

This proves the lemma.

□

Now to prove the Theorem 1(b), let $M = \lambda L(x)$, where M is an integer and λ is some constant. We have that

$$\begin{aligned}A^*(x) \le \#\{n\le x^2 : n\in S^*(\mathscr{P}), \omega(n) > M\} + \\ \#\big\{(a,b)\in S^*(\mathscr{P})^2 : a,b\le x, \omega(a)+\omega(b)\le M\big\}\end{aligned}$$

which is true since we may assume that $(a,b)=1$ in $n=ab$, since n is squarefree. We write

$$A^*(x) \le \sum_{k>M}\pi^*_{k,\mathscr{P}}(x^2) + \sum_{k\le M}\sum_{i+j=k}\pi^*_{i,\mathscr{P}}(x)\pi^*_{j,\mathscr{P}}(x)$$

and from Theorem 0,

$$\begin{aligned}
A^*(x) &\le \sum_{k>M} \frac{c_2 x^2}{\log(x^2)} \frac{L(x^2)^{k-1}}{(k-1)!} \\
&\quad + \sum_{k\le M}\sum_{i+j=k} \frac{c_2^2 x^2}{\log^2 x} \frac{L(x)^{i-1} L(x)^{j-1}}{(i-1)!(j-1)!} \\
&\le \sum_{k\ge M} \frac{c_4 x^2}{\log(x)} \frac{L(x^2)^k}{(k)!} \\
&\quad + \sum_{k\le M}\sum_{i=1}^{k-1} \frac{c_5 x^2}{\log^2 x} \binom{k-2}{i-1} \frac{L(x)^{k-2}}{(k-2)!} \\
&\le \frac{c_4 x^2}{\log(x)} \sum_{k\ge M} \frac{L(x^2)^k}{k!} \\
&\quad + \frac{c_5 x^2}{\log^2 x} \sum_{k\le M} \frac{(2L(x))^k}{k!}
\end{aligned}$$

where we obtained the first sum in this form from changing the range of summation from $M+1$ to M, and where the second sum was derived from the binomial theorem and the addition of the $(M-1)^{\text{th}}$ and M^{th} terms to the sum.

Now using Lemma 3, assume that $(1+\varepsilon)L(x^2) < M < (1-\varepsilon)(2L(x))$,

$$A^*(x) \ll \frac{x^2}{\log x} \frac{L(x^2)^M}{M!} + \frac{x^2}{\log^2 x} \frac{(2L(x))^M}{M!}.$$

By Stirling's formula,

$$\begin{aligned}
A^*(x) \ll \frac{x^2}{\log x} \left(\frac{eL(x^2)}{\lambda L(x)} \right)^{\lambda L(x)} \\
+ \frac{x^2}{\log^2 x} \left(\frac{2eL(x)}{\lambda L(x)} \right)^{\lambda L(x)}
\end{aligned}$$

where $(1+\varepsilon)\frac{L(x^2)}{L(x)} < \lambda < 2-\varepsilon$.

Now, $L(x^2) = L(x) + O(1)$, so we can choose $1+\varepsilon < \lambda < 2-\varepsilon$, to get

$$\begin{aligned}
A^*(x) \ll \frac{x^2}{\log x} \left(\frac{e}{\lambda} \left[1 + O\left(\frac{1}{\lambda L(x)} \right) \right] \right)^{\lambda L(x)} \\
+ \frac{x^2}{\log^2 x} \left(\frac{2e}{\lambda} \right)^{\lambda L(x)}.
\end{aligned}$$

And since $\left(1+O\left(\frac{1}{\lambda L(x)}\right)\right)^{\lambda L(x)} \ll 1$, then

$$\begin{aligned}
A^*(x) &\ll \frac{x^2}{\log x} \left(\frac{e}{\lambda} \right)^{\lambda L(x)} + \frac{x^2}{\log^2 x} \left(\frac{2e}{\lambda} \right)^{\lambda L(x)} \\
&\ll \frac{x^2}{\log x} \Big(e^{\lambda L(x)(1-\log\lambda)} \\
&\qquad + e^{\lambda L(x)(1+\log 2-\log\lambda)-\log\log x} \Big) \\
&\ll \frac{x^2}{\log x} \left((\log x)^{f(\lambda)} + (\log x)^{g(\lambda)} \right)
\end{aligned}$$

where $f(\lambda) = \lambda\alpha(1-\log\lambda)$ and
$g(\lambda) = \lambda\alpha(1+\log 2-\log\lambda) - 1$. Now

$$\begin{aligned}
f'(\lambda) &= -\alpha \log\lambda \\
g'(\lambda) &= -\alpha(\log 2 - \log\lambda).
\end{aligned}$$

Thus, since for all $\lambda \in (1,2)$ we have $f'(\lambda) < 0$ and $g'(\lambda) > 0$, we can deduce that the optimal value of λ will be attained when $f(\lambda) = g(\lambda)$. That is

$$\lambda\alpha(1+\log 2-\log\lambda) - 1 = \lambda\alpha(1-\log\lambda)$$

from which we get $\lambda = \frac{1}{\alpha\log 2}$ in the desired range, since $\alpha < \frac{1}{2\log 2}$ by assumption.
Hence, writing $L(x) = \alpha\log\log x$, and letting $\lambda = \frac{1}{\alpha\log 2}$, we get

$$A^*(x) \ll \frac{x^2}{\log x^{1-\frac{1}{\log 2}(1+\log\alpha+\log\log 2)}}.$$

We then obtain

$$A(x) \le \sum_{d\le x} A^*\left(\frac{x}{d}\right) \ll \frac{x^2}{\log x^{1-\frac{1}{\log 2}(1+\log\alpha+\log\log 2)}}.$$

□

4 A LOWER BOUND FOR $A(x)$

We now find a lower bound for $A(x)$ which leads us to a result which is of a form similar to that of the upper bound. To do so, we will assume that an analogy of the lower bound for $\pi_k^*(x)$ holds for the set $\mathscr{P}$. That is, we assume that

$$\pi^*_{k,\mathscr{P}}(x) \ge \frac{cx}{\log(x)} \frac{L(x)^{k-1}}{(k-1)!} \tag{A1}$$

where c is an absolute constant.

Theorem 2. Assume (A1), then for $x \ge 3$, we have

$$A(x) \gg \frac{x^2}{\log^2 x} \frac{1}{\sqrt{L(x)}} e^{L(x)}.$$

Proof. We start with a simple estimate; let $m \geq 1$ be an integer,

$$A(x) \geq \#\left\{\begin{array}{r} n \leq x^2 : \exists\, a \leq x, b \leq x \\ n = ab \\ a, b \in S^*(\mathscr{P}) \\ \omega(a) + \omega(b) = 2m \end{array}\right\}.$$

Let

$$S_1 = \#\left\{\begin{array}{r} a \leq x : a \in S^*(\mathscr{P}) \\ \omega(a) = m \end{array}\right\}$$

$$S_2 = \max_{n \leq x^2}\#\left\{\begin{array}{r} (a,b) \in S^*(\mathscr{P})^2 : a \leq x,\ b \leq x \\ n = ab \\ \omega(a) = \omega(b) = m \end{array}\right\}.$$

That is, we have

$$A(x) \geq \frac{S_1 \times S_1}{S_2}.$$

For the set of $2m$ prime factors of n, there are $\binom{2m}{m}$ choices for the the m prime factors of a and therefore, $S_2 \leq \binom{2m}{m}$. Hence,

$$A(x) \geq \frac{\left(\pi^*_{m,\mathscr{P}}(x)\right)^2}{\binom{2m}{m}}.$$

Using the assumption (A1) on $\pi^*_{k,\mathscr{P}}(x)$,

$$\begin{aligned} A(x) &\gg \frac{\left(\frac{x}{\log x}\frac{L(x)^{m-1}}{(m-1)!}\right)^2}{\binom{2m}{m}} \\ &= \frac{x^2 m^2}{\log^2 x}\frac{L(x)^{2m-2}}{2m!} \\ &\gg \frac{x^2}{\log^2 x}\left(\frac{m}{L(x)}\right)^2 \frac{1}{\sqrt{m}}\left(\frac{eL(x)}{2m}\right)^{2m}. \end{aligned}$$

And taking m to be $\frac{L(x)}{2} + O(1)$, we get

$$A(x) \gg \frac{x^2}{\log^2 x}\frac{1}{\sqrt{L(x)}}(e)^{L(x)}.$$

Remark that from choosing $m = \frac{\lambda L(x)}{2} + O(1)$, one can show that $\lambda = 1$ is the optimal choice, which gives us the above result and ends the proof of the theorem. □

Corollary 4. Assume (A1) and suppose $L(x) = \alpha \log\log x$, then

$$A(x) \gg \frac{1}{(\alpha \log\log x)^{\frac{1}{2}}}\frac{x^2}{(\log x)^{2-\alpha}}.$$

5 Acknowledgment

Special thanks to Andrew Granville for sharing his knowledge and helping me throughout the development of this article, and giving me the opportunity to discover the fascinating world of number theory.

Thanks also to Daniel Fiorilli, Farzad Aryan, Tristan Freiberg, Kevin Henriot, Mohammad Bardestane and Dimitris Koukoulopoulos who were always available to help when I needed it.

References

[1] G. H. Hardy and S.Ramanujan. *The normal number of prime factors of a number n*. Quart. J. Math. 48 (1920), 76–92.

[2] P. Erdös. *An asymptotic inequality in the theory of numbers*. Vestnik Leningrad Univ. 15 (1960), 41–49 (Russian).

[3] P. Erdös. *On the integers having exactly k prime factors*. Ann. of Math. (2) 49 (1948), 53–66 MR9,333b; Zentralblatt 30,296.

[4] K. Ford. *Integers with a divisor in (y; 2y]*. Anatomy of integers (Jean-Marie Koninck, Andrew Granville, and Florian Luca, eds.) CRM Proc. and Lect. Notes 46, Amer. Math. Soc., Providence, RI, 2008, 65–81.

[5] K. Ford. *The distribution of integers with a divisor in a given interval*. Annals of Math. (2) 168 (2008), 367–433.

[6] D. Koukoulopoulos. *Generalized and restricted multiplication tables of integers*. http://www.crm.umontreal.ca/ koukoulo/phdthesis.pdf

[7] R. R. Hall and G. Tenenbaum. *Divisors*. Cambridge Tracts in Mathematics, vol. 90, Cambridge University Press, Cambridge, 2008.

[8] G. Tenenbaum. *Sur la probabilite qu'un entier possede un diviseur dans un intervalle donne*. Compositio Math. 51 (1984), 243–263.

[9] H. Davenport. *Multiplicative Number Theory, third.* ed., Graduate Texts in Mathematics, vol. 74, Springer-Verlag, New York, 2000, Revised and with a preface by Hugh L. Montgomery.

[10] A. Selberg. *Note on a paper by L. G. Sathe*. J. Indian Math. Soc. 18 (1954), 83–87.

VALIDATING A STATISTICAL MODEL

Julie Novak

Regression analysis has become a very popular field due to its computational feasibility. We first give a brief introduction of where it is being used, and then we illustrate three methods of model validation, which are used to see how accurately the predicted values from the model will predict future responses not used in the model.

1 INTRODUCTION

A fundamental application of statistics is a field called regression analysis. Regression analysis is a technique for modeling the relationship between a set of covariates and an outcome. Although regression analysis has been around for a long time, computational progress has recently been made. Thus with the ability to collect and process a very large amount of data, a statistician can now apply regression analysis to a wide variety of fields: biology, economics, finance, genetics, and numerous others. Finding meaningful relationships between variables is an art, meaning every dataset is different, and requires both mathematical training and subjectivity to build a model.

Recently through the mapping of the human genome, regression has become a very powerful tool in genetics, particularly with research about SNPs (single nucleotide polymorphisms), a single base nucleotide that changes in a human's DNA. These alone account for 80% of differences among human beings. Thus, searching for intricate SNP patterns can lead to finding links between diseases and genes. Once patterns can be found, drugs can be more accurately tested and personalized for individual use. Beyond human genetics, SNP research in agriculture could lead to genetically modified crops, which would not only decrease cost, but also dramatically reduce the need for dangerous pesticides in our food.

A particular example is a predictive model for gestational age using the mother's characteristics. Gestational age is the time from conception to when a baby is born; for example, a child with a gestational age less than 37 weeks is considered premature. The dataset used was the McGill Obstetric and Neonatal Dataset (MOND), which was collected from all singleton births at the Royal Victoria Hospital between 1996 and 2001. The dataset contains detailed records of every mother's characteristics. Among the factors taken into account were hypertension, diabetes, smoking, drug use, and alcohol consumption. From MOND, a multivariate model was built to predict gestational age as precisely as possible with the best combination of variables.

Since every data set, therefore every model, is different, each one needs to be validated to see how well it will predict responses of future data, or data not used in this model. There are a number of validation techniques that we are going to investigate and analyze each of their strengths and weaknesses. The ones we are going to examine closely in this article are data splitting, cross-validation, and bootstrapping.

2 MODEL VALIDATIONS

After building a model, there needs to be a sample to test it on. There are two types of model validation: internal and external. External validation is testing the model on a separate data set not used to create the model, while internal validation uses the same subjects to build the model and then to test it. Yet in internal validation, the entire dataset has already been used to create the model, thus other subjects need to be found to test it on. The problem with external validation is that since not all the possible subjects are being used, the model is being held back from its full potential accuracy.

3 DATA-SPLITTING

The simplest approach for model validation we will start off with, a type of external validation, is called data-splitting. We split the data into two samples: one for model development, and one for model testing. Although this is a straightforward approach, data-splitting has its shortcomings. Since it splits the data in two, it reduces the size of both samples, losing accuracy in both phases. Therefore, there needs to be a very large sample size to proceed with this approach. There should be at least 100 observations to work with. Another question that comes about from this type of validation is where to split the data. Depending upon which samples were used for which phase, the predictive accuracy and the precision of estimation can vary greatly. In the end, only a subset of the sample will be validated. This approach will not validate an entire model.

4 CROSS-VALIDATION

Cross-validation is an improvement on data-splitting. In cross-validation, anywhere between one and a group of observations will be left out. The entire dataset is split into k groups of n samples. One group of n samples is left out the first time, and a model is built on the remaining $k-1$ groups of samples, which is almost the entire dataset. Then, the model is tested on the n samples left out the first time, obtaining an assessment of model performance. Then this process is repeated another $k-1$ times, just as before, leaving out only one of the groups each time, and then the average of all the results is recorded. Although a better technique than the former, some questions still arise. How does one choose how many groups to split the dataset into? Also, the data need to be split into groups many times and reevaluated before obtaining a good estimate of accuracy. And once again, cross-validation does not validate the entire model, but only part of it.

5 Bootstrapping

As always, we assume that a random sample, $\mathbf{x} = \{x_1, x_2, \ldots, x_n\}$, is taken from a population $\mathbf{P} = \{x_1, x_2, \ldots, x_N\}$, where N is much bigger than n. Then we produce many bootstrap replicates by resampling a set of size n, which we denote $\mathbf{b}$ from $\mathbf{x}$, with replacement (so as not to force $\mathbf{b}$ to be a permutation of $\mathbf{x}$). Therefore this can be seen as treating the new sample $\mathbf{b}$ as a random sample from the original $\mathbf{x}$, which is now the 'population', $\mathbf{P}$. This new sample $\mathbf{b} = \{x_{b_1}, x_{b_2}, \ldots, x_{b_n}\}$ is called the bootstrap sample. This procedure is repeated many times, so as to have hundreds of bootstrap samples. This is based on the idea that each new sample $\mathbf{b}$ is chosen with equal probality of $\frac{1}{n}$ from the original sample $\mathbf{x}$.

This idea can be applied to regression. This can be done in two ways: either by treating the regressors, the $\mathbf{x}$s, as random, or as fixed. If the $\mathbf{x}$s are taken to be random, then the n observations of the covariates, and their corresponding y value are resampled to form each bootstrap sample. Then, for every bootstrap sample, the bootstrap regression coefficients are computed, $b_{b_1}, \ldots, b_{b_n}$. Then, the final regression coefficients, confidence intervals and standard errors are estimated by combining the bootstrap values.

Alternatively, if the $\mathbf{x}$s are taken to be fixed, then the residual regression errors, ε are taken to be random. In this case, regression coefficients are obtained from the original sample, and estimates of the errors, $\hat{\varepsilon}_i = Y_i - \hat{Y}_i$ can be computed and then bootstrapped, where the hats refer to the fitted values. Then, new response values are formed by adding the fitted values, $\hat{Y}$ with the bootstrapped error values, and then regressed on the covariates again. This procedure gives B replicates of the regression coefficients, where B is the number of bootstrap resamples taken. The final regression coefficients, confidence intervals and standard errors are then combined using these values.

Unlike in data-splitting or in cross-validation, in bootstrapping the entire original model is used to evaluate the performance of the final model. A good measure of its predictive ability is R^2, the coefficient of determination. None of the data is lost in the predictive phase here. A very good technique for model validation, bootstrapping is very computationally intensive, and large datasets can be easily handled with statistical software.

6 Conclusion

There are many other techniques that can be analyzed, but here one has an overview to some of the more common techniques of model validation. This is a critical phase of building a model, probably the most important, as without model validation, predictions are ultimately meaningless and would have no applicability outside of the original dataset. Model accuracy is essential to making major decisions in the financial market, in genetics, and in other fields. Thus having an in depth understanding of the theory is important for choosing which approaches to take in validating your model.

References

[1] Frank E Harrell, Jr, *Regression Modeling Strategies With Applications to Linear Models, Logistic Regression, and Survival Analysis*, Springer-Verlag, 2001

[2] John Fox, *An R and S-Plus Companion to Applied Regression*, Sage Publications, 2002

[3] John Fox, *Applied Regression Analysis and Generalized Linear Models*, Sage Publications, 2008

[4] Christopher Z. Mooney, Robert D. Duval, *Bootstrapping: A Nonparametric Approach to Statistical Inference*, Issues 94-9, page 17, 1993

[5] M. Stone, *Cross-validatory Choice and Assessment of Statistical Predictions*, Journal of Royal Statistical Society, 1974

[6] B. Efrom, *Bootstrap Methods: Another Look at the Jackknife*, The Annals of Statistics, 1979

[7] Bradley Efrom, *Second Thoughts on the Bootstrap*, Statistical Science, 2003

Jokes

I used to believe that correlation implied causation, but then I took a statistics class and now I don't believe that anymore. So the class worked. □

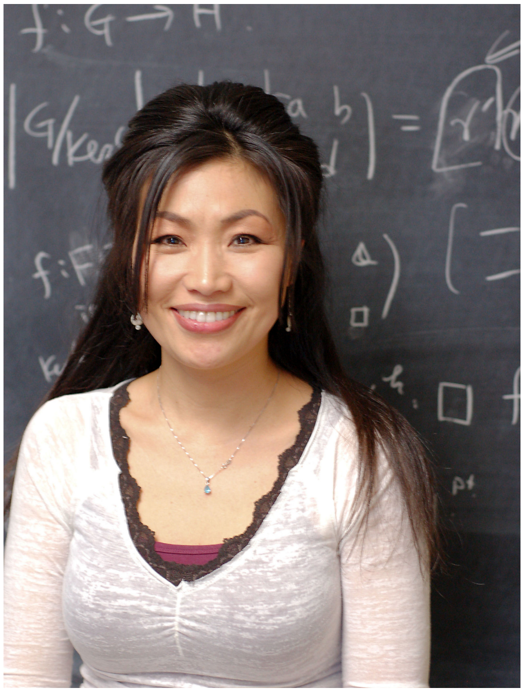
Q: What is the difference between a Ph.D. in mathematics and a large pizza?
A: A large pizza can feed a family of four... □

Interview with Heekyoung Hahn

Cathryn Supko

$\delta\varepsilon$: What is your background, both personal and academic?
I grew up in South Korea and I've known that I wanted to pursue mathematics from a very young age. My curiosity was sparked when I was young and my brother's friend, a math major, saw me working on my math homework involving negative numbers. He asked, "Can you imagine how many negative numbers there are? " and told me that in fact there were the same number of natural numbers as integers. I was convinced he was lying, but he insisted that if I too chose to study math at university, I would be able to learn such things. I always thought that math was the most fun subject as a kid, so it was the only thing I considered when it came time to choose my major. Because I was a good student, my teachers tried to convince me to be a doctor or a lawyer. But to me, selling medicine is the same as selling potato chips, it's not interesting. Despite my father's wish that I become a school teacher after college, I decided that I wanted to teach deeper mathematics than is taught in high school and chose to continue studying math in graduate school. When I told my father, who was a farmer and had been a soldier in the Korean war, that I wanted to get a Ph. D. in the United States, he had no idea how to react. His image of the United States came from his interaction with American soldiers during the war, and he thought that in the US they had buildings made out of gold or something. Although he passed away before I started my Ph. D., I know that he trusted my judgement and ambition. I completed my Ph. D. at University of Illinois at Urbana-Champlain in 2004. I then was a Post-Doc at University of Rochester from 2004 to 2007, after which I took a tenure track position at SUNY-Albany where I'm currently on academic leave. This year I came to McGill as a lecturer, primarily to be with my husband Jayce Getz, who is also a professor here.

$\delta\varepsilon$: How have you enjoyed your time in Montreal so far?
So far I've really enjoyed my time in Montreal- apart from the cold. One of the major advantages of living in this city as a number theorist is the Number Theory Group. Because there are so many universities here, there are a lot of opportunities to use a wide range of resources and offer a huge number of classes and seminars in the subject. Those factors, as well as the active, friendly atmosphere makes working here unlike any other academic setting I've been in before. At the end of the year I will have to decide whether or not I'm returning to Albany, which is a huge dilemma for me right now because being here is great, but it's difficult to give up a position with the possibility of tenure.



Picture 1: Faculty Lecturer Heekyoung Hahn

$\delta\varepsilon$: What are some of your research interests? Can you offer any advice to undergraduate students with an interest in doing research?

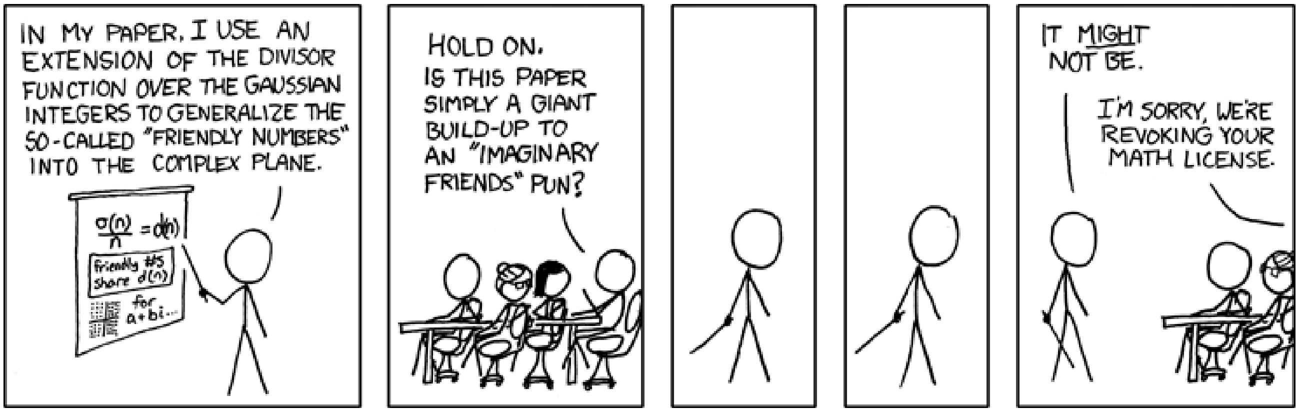
My research interests have not taken a direct path. During my undergrad, I found many topics fascinating, including set theory and modern geometry. I focused on analysis during my master's, and switched to number theory during my Ph. D. I've done research in both analytic and algebraic number theory, and I find it's helpful not to restrict my studies to one subject in particular. I want to be a good mathematician more than a good number theorist.

I chose my Ph. D. advisor not because number theory was my primary interest, but because when I met him I really liked him and knew he was someone I could work with. This may not be the best approach for everyone, but the selection of an advisor is extremely important, they'll be part of your life forever. The choice really depends on the person, but the best advice I can give is to trust yourself to make the decision then take responsibility for whatever happens as a result. Don't worry too much about it, even if it's not a perfect situation you will end up fine.

$\delta\varepsilon$: Do you think being a woman in math has influenced your experiences in the field?
In many ways, being a woman in math has been very ad-

vantageous for me; however, I'm very opposed to the idea that I should be hired *because* I am a woman. To encourage women to pursue graduate studies in mathematics, there are many funding opportunities that are available only to women, in addition to those open to everyone. Having a child presents huge challenges for women in academia because you have to spend so many hours taking care of your baby instead of thinking of math. You can ignore your chores and let your house get messy, but you can't ignore your kid. Only recently did the American Mathematical Society start offering babysitting at their meetings so that more women with children can attend. The financial and time-management challenges associated with having a kid may be one of the reasons that although half of the people who enter graduate school in mathematics are women, many of them drop out. It would be good if there was more support for women in this position.

Jokes


IN MY PAPER, I USE AN EXTENSION OF THE DIVISOR FUNCTION OVER THE GAUSSIAN INTEGERS TO GENERALIZE THE SO-CALLED "FRIENDLY NUMBERS" INTO THE COMPLEX PLANE.
σ(n)/n = d(n)
friendly #s share d(n)
for a+bi...
HOLD ON. IS THIS PAPER SIMPLY A GIANT BUILD-UP TO AN "IMAGINARY FRIENDS" PUN?
IT MIGHT NOT BE.
I'M SORRY, WE'RE REVOKING YOUR MATH LICENSE.

xkcd 410: *Math Paper*

□

Q. What's the contour integral around Western Europe?
A. Zero, because all the Poles are in Eastern Europe □

Q. What's a polar bear?
A. A rectangular bear after a coordinate transform. □

Q. Why do truncated Maclaurin series fit the original function do well?
A. Because they are "Taylor" made. □

Q. What is black and white and fills space?
A. A piano curve.
A2. This joke. □

Q. How many number theorists does it take to change a lightbulb?
A. This is not known, but it is conjectured to be an elegant prime. □

Q. How many analysts does it take to change a lightbulb?
A. Three. One to prove existance, one to prove uniqueness, and one to derive a nonconstructive algorithm to do it. □

Q: How do you tell an extroverted mathematican from an introverted one?
A: An extroverted mathematician stares at *your* shoes when talking to you. □

Random Walks on a Graph

Maria Eberg

This article introduces two different approaches to random walks on a graph: the general Markov chains approach and then electrical resistance tools. Afterwards, we investigate the following problem: Two random walks are placed on a graph G; both walkers start to move simultaneously and they meet if they reach the same vertex at the same step. We are interested in the probability of the walks meeting before one of them hits a special (marked) vertex. We study these probabilities of interest in two specific cases; when G is a complete graph and when it is a hypercube.

1 Introduction

A graph is a universal mathematical description of a set of elements connected pairwise by some relation. A random walk on an undirected connected graph G is a process that starts at some vertex of G, and at each time step moves to one of the neighbors of the current vertex with uniform probability. A random walk on a graph is a special case of a Markov chain, which has the reversibility property. Roughly speaking, this property means that the probabilities of traversing a given path in one direction or in another have a simple relation between them. Some of the examples of random walks include the shuffling of a deck of cards, the Brownian motion of a particle or some models in statistical mechanics. In this article we shall focus on two random walks moving simultaneously on a graph. The aspects studied will try to answer the following questions: How long do we walk until we see a given node? How fast can two walks meet on a graph? What is the probability that the walks meet before one of them reaches the given node?

2 Basic Notions and Facts

2.1 Markov Chains Approach to Random Walks on Graphs

A finite Markov chain is a process which moves along the elements of a finite set Ω such that, when the process is at $x \in \Omega$, the next position is chosen according to a fixed probability distribution $P(x,\cdot)$. Note that if Ω is a countable set, a *probability distribution* on Ω is a non-negative function $\mu : \Omega \to [0,1]$ such that $\sum_{\xi\in\Omega}\mu(\xi) = 1$. For any subset $A \subset \Omega$,

$$\mu(A) = \sum_{\xi\in A}\mu(\xi).$$

Definition. We define a sequence of random variables (X_t) as a Markov chain with state space Ω and transition matrix P, if for all $x,y \in \Omega$, all $t \geq 1$ and all events $H_{t-1} = \cap_{s=0}^{t-1}\{X_s = x_s\}$ with positive probability of each event happening, we have

$$P\Big(X_{t+1} = y|H_{t-1} \cap \{X_t = x\}\Big) = P\left(X_{t+1} = y|X_t = x\right) = P\left(x,y\right).$$

The defined property is the *Markov property* and it implies that the conditional probability of moving from state x to state y is the same, no matter what sequence $x_0, x_1, \ldots, x_{t-1}$ of states precedes the current state x. This is exactly why the $|\Omega| \times |\Omega|$ matrix P suffices to describe the transitions.

The xth row of the matrix P is the distribution $P(x,\cdot)$. We can store our current distribution information in a row vector μ_t which gives the distribution of the chain at step t. The starting position of a walk is not always fixed, but it is given by a probability distribution μ_0 on Ω. Even though for each $t > 0$ the position of the walk at time t is also random, we can find the distribution of the walk from the formula $\mu_t = \mu_0 P^t$, where P is the matrix of transition probabilities taken to the power t. Therefore, the distribution at time t can be found by matrix multiplication.

A graph $G = (V,E)$ consists of a *vertex set* V and an *edge set* E, where elements of E are unordered pairs of vertices. It is easier to think of V as a set of points, where two points υ and u are joined by a line if and only if $\{\upsilon, u\}$ is an element of the edge set. If $\{\upsilon, u\} \in E$, we say that u is a *neighbor* of υ and we write it as $v \sim u$. The degree $deg(v)$ of a vertex v is the number of neighbors of v.

Definition. Given a graph G, we define a *simple random walk on* G as a Markov chain with state space V and transition matrix

$$P_{ij} = \begin{cases} \frac{1}{d(v_i)} & \text{if } \{v_i, v_j\} \in E, \\ 0 & \text{otherwise.} \end{cases}$$

This means that when the chain is at vertex υ_i, it examines all neighbors of υ_i, picks one uniformly at random, and moves to the chosen vertex.

The next two definitions come from the general Markov chain theory and apply to any chains, not only to the simple random walk case.

Definition. A chain (X_t) is *irreducible* if for any two states $x,y \in \Omega$ there exists an integer $t > 0$ such that $P^t(x,y) > 0$, meaning that the probability of reaching state y from state x is nonzero, so it is possible to get from any state to any other state by transitions of positive probability.

Definition. Define $\tau(x) = \{t \geq 0 : P^t(x,x) > 0\}$ as a set of times when it is possible for a chain to return to its starting position x. Then the *period* of the state x is the greatest common divisor of the elements of $\tau(x)$. The chain is *aperiodic* if all states have period 1.

Generally the probability distributions μ_0, μ_1, $\ldots$, are different, but how does μ_t behave in the long term? In fact for irreducible and aperiodic chains, μ_t has limit π as $t \longrightarrow \infty$, where π is defined as the long-term limiting distribution of the chain and called *stationary* if $\pi_t = \pi_0$ for all $t \geq 0$. Specifically for a simple random walk on a connected graph, the stationary distribution is easy to find.

Definition. Given any connected graph G with number of edges equal to m, the distribution

$$\pi(v) = \frac{d(v)}{2m} \quad \forall v \in V$$

is stationary.

Stationary distributions are useful due to their invariance with respect to the transition matrix; and with the knowledge of a stationary distribution it is easier to explore a chain's properties and behavior on a graph.

In order to show that irreducible Markov chains converge to their stationary distributions, we need to define the *total variation distance*. In words, the *total variation distance* is the maximum difference between the probabilities assigned to a single event A by the two distributions, say μ and υ. In mathematical terms,

$$\parallel \mu - \upsilon \parallel_{TV} = \max_{A \subset \Omega} |\mu(A) - \upsilon(A)|$$

We are now ready to state several fundamental theorems that will provide a sufficient background for the reader.

Theorem 1 (Convergence Theorem). Suppose a Markov chain is irreducible and aperiodic, with stationary distribution π. Then there exist constants $\alpha \in (0,1)$ and $C > 0$ such that

$$\max_{x \in \Omega} \parallel P^t(x,\cdot) - \pi \parallel_{TV} \leq C\alpha^t.$$

The convergence theorem implies that irreducible Markov chains converge to their stationary distributions. However, one may ask how many steps it takes for an irreducible chain to converge to its stationary distribution. To answer this question we need the following definitions.

Definition. Given a Markov chain with state space Ω, it is natural to set the *hitting time* τ_A of a subset $A \subseteq \Omega$ to be the first time one of the vertices in A is visited by the chain. So, if (X_t) is a random walk, then

$$\tau_A = \min\{t \geq 0 : X_t \in A\}.$$

We use the notation τ_x in case $A = \{x\}$. We also denote $E_\mu(\tau_x)$ to be the expected hitting time of a vertex $x \in \Omega$ (expected number of steps to reach vertex x) in case μ was the starting distribution. We also use the notation $E_a(\tau_x)$ for the expected hitting time of a vertex x if the starting vertex of the chain is a, almost surely. It is often useful to estimate the worst-case hitting times between states of a chain, so we define

$$t_{hit} = \max_{x,y \in \Omega} E_x(\tau_y).$$

Definition. Let (X_t) be a finite Markov chain with state space Ω. The *cover time* τ_{cov} of (X_t) is the first time at which all the states have been visited, i.e. τ_{cov} is the minimum value such that for every state $y \in \Omega$ there exists $t \leq \tau_{cov}$ with $X_t = y$.

2.2 Electrical Networks Approach

Surprisingly enough, electrical networks are closely connected to Markov chains and provide a different language for reversible Markov chains. In this article we are going to use that approach to study random walks. For an interested reader, [4] gives the best background in the subject.

We will define some of the concepts of electric networks which might become useful in the future.

A *network* is a finite undirected connected graph G with vertex set V and edge set E. We assign to each edge $\{x,y\}$ of G a non-negative number, *conductance*, $C_{xy} > 0$ and let $R_{xy} = \frac{1}{C_{xy}}$ be the *resistance* of the edge $\{x,y\}$.

Definition. Consider the Markov chain on the vertices of G with transition matrix

$$P_{xy} = \frac{C_{xy}}{C_x}$$

where $C_x = \sum_{y:y \sim x} C_{xy}$. This process is called *the weighted random walk* on G with edge weights $\{C_e\}$.

Given a network (G, C_e), we distinguish two vertices, x and y, which are called the *source* and the *sink* respectively. We call a function $h : V \longrightarrow R$ *harmonic* for P at a vertex v if

$$h(x) = \sum_{u \in V} P(v,u)h(u).$$

A function W which is harmonic on $V \setminus \{x,y\}$ is called *voltage*. Given a voltage W on the network, the *current flow I* associated with W is defined on oriented edges by

$$I_{xy} = \frac{W_x - W_y}{R_{xy}} = C_{xy}\left[W_x - W_y\right].$$

Next we define *effective resistance* between vertices x and y as

$$R(x \longleftrightarrow y) = \frac{W_x - W_y}{\|I\|}$$

where I is the current flow corresponding to the voltage W.

Definition. The *effective conductance* of an electrical network of unit resistors between two distinct vertices x and y is given by $d(x)P_x(\tau_y < \tau_y^+)$, where $d(x)$ is the degree of x and $P_x(\tau_y < \tau_y^+)$ defines the *escape probability*, i.e. the probability that a walker, starting at x, visits y before returning to a.

Lemma 2 (Commute Time Identity). Let (G, C_{xy}) be a network, and let (X_t) be a random walk on this network. For any nodes a and b in V, let $\tau_{a,b}$ be the time to move from a to b and then back to a. Then

$$E_a(\tau_{a,b}) = E_a(\tau_b) + E_b(\tau_a) = \sum_{x \in V} \sum_{y: y \sim x} C_{xy} R(a \longleftrightarrow b).$$

3 What Has Been Done And What Can Be Done

Imagine such a situation:

A mother with two children walks in a maze. At some point she loses both of her children in different parts of it. She is walking randomly and trying to find her kids. At the same time one of them also walks randomly, while the other one just sits and waits to be found. Which one of them is the mother most likely to meet first?

This is an example of a somewhat real life situation which relates to the posed question.

The answer can be different according to the way the walkers move: simultaneously, alternatingly, or in any other way defined by some rule.

Note that if the Markov chains X_t and Y_t are periodic (period m) then the meeting between them might never occur! So we restrict our attention to irreducible and aperiodic chains, where eventually the walks always meet.

3.1 Previous Research on the Topic

One possibility to define the movement of random walks is to have a "demon" choosing which particle, i.e. chain, moves at each step. Its aim is to delay the meeting between the particles. In [3] authors use a potential function to estimate the number of steps before the walks meet. They define vertex t as *hidden* if it has the property that $H(t,v) \leq H(v,t)$ for all $v \in V$, where $H(t,v)$ is the expected hitting time between the two vertices. (For example, a reader may verify that a vertex of a *tree* graph is *hidden* if its average distance to other vertices of the tree is maximum.)

In [3], the authors have proved an interesting result for the case when one of the walks starts from the hidden vertex t. We then have

$$M(u,t) \leq H(u,t)$$

where $M(u,t)$ is the meeting time of two walks such that one of them started at vertex u and another one at vertex t. Even though the "demon" is scheduling the walks with the aim of keeping them apart, the "worst case" expected meeting time of the walks is still at most the expected hitting time of one of them reaching the initial point of the other. In the article the authors were interested in the problem of self-stabilizing systems, therefore the obtained bound would be the maximum amount of steps until a stabilization occurs.

A question arising from the article [3] is whether the inequality $M(u,t) \leq H(u,t)$ is not altered in the "non-demonic" world.

Another interesting way of looking at several random walks on a graph is to define a product graph and observe the random walk on it.

Given graphs G and H, we define the product graph $G \times H$ with vertex set $V(G) \times V(H)$ and say that two vertices (u,v) and (w,z) are connected if either $u = w$ and $vz \in E(H)$ or $v = z$ and $uw \in E(H)$. The technique of using a product graph allows one to replace two random walks on one graph by a single random walk on the product graph. In the product graph the position of a walk at a step t is equivalent to the position of two random walks on the original graph at the same step. Note that if the walk (X_t) is at a vertex (x,x) at step t, this implies that two walks on the original graph G meet at the vertex x at step t.

The authors in [1] studied random walks on the product graph $G \times H$ where G is an arbitrary connected graph and H is either a path, a cycle or a complete graph.

For the complete graph, the probability that a random walk starting from (y,x) reaches (x,x) before (x,y) is at least $\frac{1}{2}$. This means that the two walks are more likely to meet before one of them reaches the starting position of the other. These results are similar to the ones of [3].

In the case of an n-cycle C_n, if we start two walks from the same vertex x of C_n, then the probability of the walks meeting at some other vertex y is higher than the probability of one of them reaching a marked vertex z.

Even though the discussed results of [3] and [1] are intriguing, they still do not assume complete randomness in the choice of the vertices where the walks start.

Now we are going to turn our attention to the case of a complete graph and study the probabilities of interest on this graph.

3.2 Complete Graph Case

A complete graph is a graph in which each pair of graph vertices is connected by an edge. Let G be a complete graph K_n with n vertices and $\frac{n(n-1)}{2}$ edges. Now we add a loop to each vertex. Denote the modified graph by G^*.

Let X_t and Y_t be two lazy random walks on G^*, meaning that each of them can stay at the current vertex (take the loop edge) or leave the current vertex. Suppose X_t starts at vertex i and Y_t starts at vertex j. Also, pick a vertex of G^* uniformly at random and mark it by z. No walk starts from z.

Denote by A the event when X_t and Y_t meet before one of them reaches the marked vertex z or when both of the walks meet at z at the same step. Let $p_{ij} = Pr(A)$, then

$$p_{1j} = 0 \ \text{ if } \ j \neq 1$$

$$p_{i1} = 0 \ \text{ if } \ i \neq 1$$

$$p_{ii} = 1 \ \ \forall i = 1, \dots, n.$$

For all other cases we get the following recurrence relation

$$p_{ij} = \frac{1}{n} + \sum_{k,l} \frac{1}{n^2} p_{kl} \tag{1}$$

where $k \neq z$, $l \neq z$ and $k \neq l$.

Note that K_n is a symmetric graph, meaning that for any two pairs of linked vertices $u_1 - v_1$ and $u_2 - v_2$ of G^* there is a mapping (f) of G^* onto itself where $f : V(G) \to V(G)$ such that $f(u_1) = u_2$ and $f(v_1) = v_2$. This mapping is called an automorphism. Therefore, we can rewrite (1) as

$$p_{ij} = \frac{1}{n} + \frac{1}{n^2} p_{ij}(n-1)(n-2). \tag{2}$$

Observe that the factor $(n-1)(n-2)$ comes from the fact that we need to choose k and l with ordering, such that out of n vertices, they are different from each other, and neither is equal to z. Then, rearranging the terms, we get

$$p_{ij} = \frac{n}{3n-2}. \tag{3}$$

Now suppose that the starting vertices of (X_t) and (Y_t) are picked according to the stationary distribution π, which is uniform. Then

$$Pr_\pi(A) = \sum_{(i,j)} \frac{1}{n^2} p_{ij} = \frac{1}{n^2} \sum_{(i,j)} p_{ij}$$

where (i,j) denotes all possible pairs of vertices $i, j \in \Omega$. Summing over all the pairs, we get

$$\begin{aligned} Pr_\pi(A) &= \frac{1}{n^2}\left[n + \frac{n}{3n-2}(n-1)(n-2)\right] \qquad (4) \\ &= \frac{n}{3n-2} > \frac{1}{3}. \end{aligned}$$

Note that as in (2), $(n-1)(n-2)$ appears due to choice of vertices with ordering, while the factor $\frac{n}{3n-2}$ is explained by (3). The factor n is justified by the observation that both walks can start from the same vertex, i.e. $p_{ii} = 1 \ \forall i = 1, \dots, n$, and then we sum over all $i = 1, \dots, n$. From (4) we can conclude that in the case of a complete graph K_n the observed probability of interest is at least $\frac{1}{3}$.

3.3 Lazy Random Walks on the Hypercube

The n-dimensional hypercube is a graph whose vertices are the binary n-tuples $\{0,1\}^n$. Two vertices are connected by an edge when they differ in exactly one coordinate. The number of edges in the n-dimensional hypercube is $n2^{n-1}$, the number of vertices is 2^n.

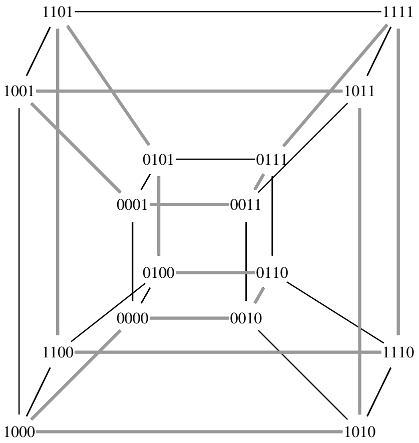


Figure 1: 4-hypercube

Add n loops to each vertex, so the number of edges increases to $n2^{n-1} + n2^n = 3n2^{n-1}$. Adding loops implies that each vertex becomes a neighbor to itself. Thus, the probability of a walk to stay at the current vertex is then equal to the probability of moving to any of its neighbors since in the hypercube graph each vertex has n neighbors. Such modification of the graph is needed in order to better understand how a lazy walk would move on it.

Define the *Hamming weight* $W(x)$ of a vector $x = (x^1, \dots, x^n) \in \{0,1\}^n$ to be the number of its coordinates with value 1:

$$W(x) = \sum_{j=1}^{n} x^j.$$

Now let's introduce a lazy random walk on the defined graph. The algorithm is the following:

1) Pick a coordinate $j \in \{1, 2, \dots, n\}$ uniformly at random.

2) Flip a coin. If the result is heads, the walk stays at its current position and the jth coordinate remains unchanged. If the result is tails, the jth coordinate will change to $1 - v_j$.

We start two lazy random walks on the hypercube with n loops at each edge. Let X_t start at zero, so $X_0 = (0, 0, \dots, 0)$, and suppose Y_t starts at a vertex with all coordinates being equal to 1, so $Y_0 = (1, 1, \dots, 1)$. Also, let the marked vertex Z be the one where X_t starts its walk, i.e. $Z = (0, 0, \dots, 0)$.

Given the vectors $(X_t^1, \cdots, X_t^n)$ and $(Y_t^1, \dots, Y_t^n)$ telling the positions of two walks at step t, define the *symmetric difference* S_t as a difference *modulo* 2 between the vectors $(X_t^1, \cdots, X_t^n)$ and $(Y_t^1, \dots, Y_t^n)$. The vector S_t shows in which coordinates X_t and Y_t are different at step t.

If $S_t = (0,0,\dots,0)$, this implies that all the coordinates of X_t and Y_t are equal and, therefore, they have met at step t. Moreover, with each step both walks get an update, so the symmetric difference gets two updates with each step. The questions then are: When is S_t equal to the zero vector for the first time and when is $Y_t = (0,0,\dots,0)$ for the first time?

We can answer the second question. We are going to apply electrical networks tools as we can find the expectation of the first time when $Y_t = (0,0,\dots,0)$ using the Commute Time Identity, but first we need to see how the commute time is altered in case of a lazy walk, not a simple one.

Claim 3. The expected hitting time of a lazy random walk on a graph G is twice the expected hitting time of a simple random walk on G, i.e. $E^l_n(\tau_0) = 2E_n(\tau_0)$ where $E^l_n(\tau_0)$ stands for the expected hitting time of a lazy walk started at vertex n.

Proof. Let $x, y \in \Omega$ be distinct vertices. If the expected hitting time from x to y is t, then there is a path of the average length t from vertex x to vertex y. How does the length of that path change if the walk is lazy?

Define X^l_i and X_i as the position of the lazy and non-lazy chains at step i respectively. Note that we can add "laziness" to a chain afterwards, meaning that we start the lazy walk at the same vertex as the non-lazy one, but every time the chain makes a step we flip a coin deciding whether the chain moves or stays at the current vertex. How does the expected hitting time change?

$$X^l_0 = X_0$$

$$X^l_1 = \begin{cases} X_0 & \text{with } Pr(tails) = \frac{1}{2}, \\ X_1 & \text{with } Pr(heads) = \frac{1}{2} \end{cases}$$

Suppose $X^l_{\tau_1} = X_1, X^l_{\tau_1+\tau_2} = X_2, X^l_{\tau_1+\tau_2+\tau_3} = X_3$, and so on with $\tau_1, \tau_2, \tau_3, \dots$ i.i.d. geometrically distributed random variables with parameter $p = \frac{1}{2}$. The expectation of a geometric random variable X is $E(X) = \frac{1}{p}$, thus, $E(\tau_i) = 2$ with $i = 1,2,3,\dots$.
On average it takes the lazy chain twice as long to get to another state than the non-lazy walk. Therefore, if $E_x(\tau_y) = t$,we would expect that on average the lazy version of the path X would get from x to y after $2t$ steps. □

Going back to the second question, we can now estimate when $Y_t = (0,0,\dots,0)$ for the first time.

Let $0 = (0,\dots,0)$ be a zero vector in the n-dimensional hypercube $\{0,1\}^n$. Define υ as a vertex with Hamming weight k. Let $h_n(k)$ be the expected hitting time from υ to 0 for a lazy random walk on the hypercube.

Find the expected time for a vertex υ with Hamming weight n to hit the zero vertex.

Define G_n by gluing together the vertices of the hypercube with the same Hamming weight k such that $1 < k < n-1$. We get a graph with vertex set $V = \{0,1,\dots,n\}$ and the number of edges from $k-1$ to k is $k\binom{n}{k}$. To compute $h_n(n)$, we are going to use symmetry and the Commute Time Identity. Note that since the hypercube is symmetric, then

$$\begin{aligned} E_n(\tau_{0,n}) &= E_n(\tau_0) + E_0(\tau_n) = 2E_n(\tau_0) \\ &= c_G R(0 \leftrightarrow n) = \sum_{x\in V} \sum_{y:y\sim x} c(x,y) R(0 \leftrightarrow n). \end{aligned}$$

So

$$2E_n(\tau_0) = 2h_n(n) = 2|edges(G_n)| R(0 \leftrightarrow n).$$

As shown before $E^l_n(\tau_0) = 2E_n(\tau_0)$; therefore, we can find the estimated hitting time for a simple random walk and multiply it by 2 to get the expected hitting time of a lazy version.

The number of edges in G_k is $\sum_{x\in V} \sum_{y:y\sim x} c(x,y) = \sum_{x\in V} 2^{n-1} = n2^{n-1}$.
Now

$$R(0 \leftrightarrow n) = \sum_{k=1}^{n} \left[k \binom{n}{k} \right]^{-1}.$$

In this sum the first and the last terms is $\frac{2}{n}$, while we can bound the sum of the rest of the terms by $\frac{4}{n^2}$. Therefore, $R(0 \leftrightarrow n) \leq \left(\frac{2}{n} + \frac{4}{n^2}\right)$ and

$$h_n(n) \leq n2^{n-1} \left(\frac{2}{n} + \frac{4}{n^2} \right) \leq 2^n \left(1 + \frac{2}{n} \right).$$

So for the lazy chain we get $h^l_n(n) \leq 2(2^n \left(1 + \frac{2}{n}\right)) = 2^{n+1}\left(1 + \frac{2}{n}\right)$.

We can think of applying electrical resistance tools in the case of the symmetric difference. However, there is no universal rule to calculate the edges from a vertex with Hamming weight $k-1$ to a vertex with the weight k, where $k = 1,\dots,n$. Therefore, there is no universal pattern (as in the previous case) which can be used to give an estimate for the hitting time from n to 0.

4 Conclusion

Both a complete graph and a hypercube are special, "nice" types of graphs with such properties as symmetry and regularity which allowed us to use some tools, unapplicable in general. While it is possible to calculate the probability of interest for specific graphs such as complete graphs, hypercubes, d-regular graphs, the proof for a general graph is still an open problem. Some new idea or a completely different approach (as in [3] where the potential function was used) are needed to answer the posed question for all sorts of graphs.

5 Acknowledgments

I thank Professor Louigi Addario-Berry and postdoctoral fellow Simon Griffiths for their guidance and support. I am infinitely grateful to them for introducing me to this topic. I also thank ISM for their funding, which made the research more motivating.

References

[1] B.Bollobas, G.Brightwell, *Random walks and electrical resistances in products of graphs*, Discrete Applied Mathematics, Volume 73 (1997), pp.69–79.

[2] C.Cooper, A.Frieze, T.Radzik, *Multiple random walks in random regular graphs*, SIAM J. Discrete Math. Volume 23 (2009), Issue 4, pp.1738–1761.

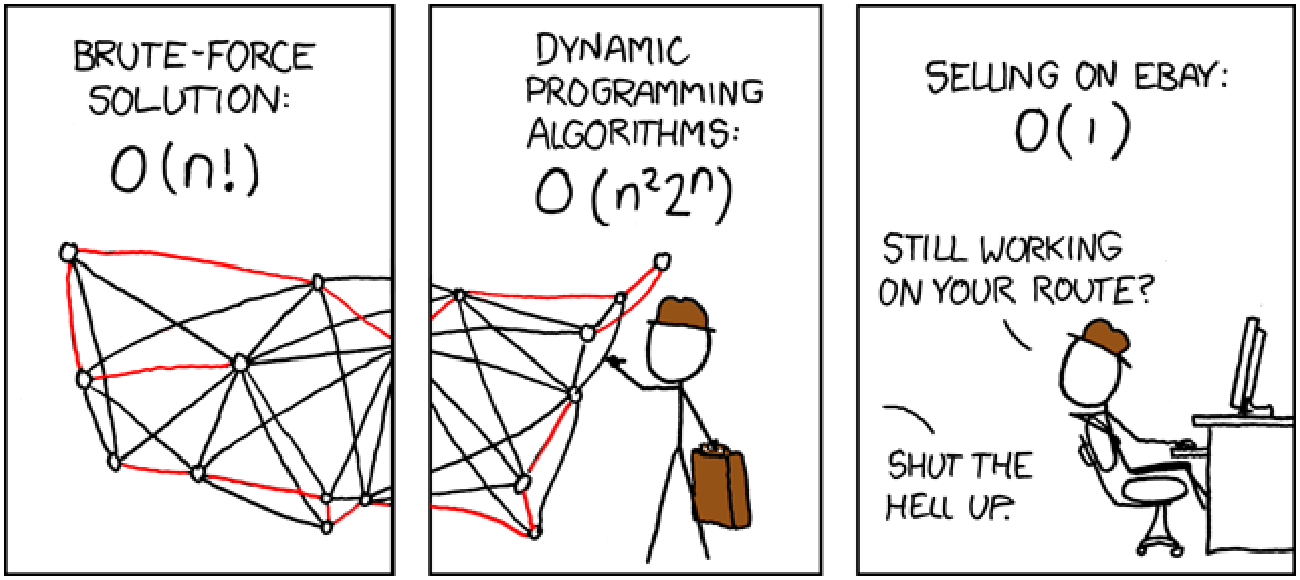
[3] D.Coppersmith, P.Tetali, P.Winkler, *Collisions among random walks on a graph*, SIAM J. Discrete Math. Volume 6 (1993), Issue 3, pp.363–374.

[4] P.G.Doyle, J.L.Snell, *Random walks and electric networks*, 2006.

[5] D.A.Levin, Y.Peres, E.L.Wilmer, *Markov Chains and Mixing Times*, 2009.

[6] L.Lovazs, *Random Walks on Graphs: A Survey*, Combinatorics (1993), Paul Erdős is Eighty, p.146.

Jokes



xkcd 399: *Travelling Salesman Problem*

□

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.” □

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?” □

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

Q.What’s the difference between a whale and a light post?
A. The solution is left as an exercise to the reader. □

Différentes approches à la loi de composition de Gauss

François Séguin

Depuis que les classes d'équivalences de formes quadratiques binaires ont été reconnues comme formant un groupe, une variété de lois de composition pour ce groupe ont été développées. Après avoir introduit la notion de forme quadratique binaire, notre but sera d'inspecter ces différentes approches à cette même loi appellée loi de composition de Gauss, ainsi que de comprendre les subtiles similarités qu'elles se partagent.

1 Introduction aux formes quadratiques binaires

1.1 Motivation

Les formes quadratiques binaires sont des polynômes en deux variables où chaque terme est de degré 2. Elles ont fait l'objet de nombreux problèmes depuis que Gauss en a fait l'étude dans son *Disquisitiones Arithmeticae*. Lui-même n'était pas le premier à considérer cet objet, puisque même Fermat y fait allusion, notamment dans son fameux Théorème des deux carrés (pour un p premier, si p est une somme de deux carrés, alors $p \equiv 1 \bmod 4$). Par contre, la majeure partie des problèmes impliquant ces formes quadratiques binaires avait trait au problème de représentation des nombres. Il s'agit en fait de se demander, pour une forme quadratique binaire donnée, quels nombres peuvent être représentés par cette forme quadratique binaire lorsque l'on remplace les x et y de la forme par des entiers.

Gauss, avant même l'apparition du concept de groupe, avait déjà prouvé que l'ensemble des classes d'équivalence des formes quadratiques binaires de même discriminant en avait les propriétés. Ainsi, il a mis au point une opération dans ce groupe: la loi de Gauss. Bhargava a récemment actualisé la question de composer des formes en apportant une généralisation de cette loi. Ainsi, nous nous pencherons ici sur différentes variante de la loi de composition de formes quadratiques binaires.

1.2 Terminologie et définitions

Une forme k-ique n-aire entière est un polynôme de degré k comportant n variables dont les coefficients sont entiers. Par exemple, une forme quadratique binaire entière est un polynôme $ax^2 + bxy + cy^2$ tel que $a,b,c \in \mathbb{Z}$. Pour des raisons de simplicité de notation, nous allons représenter la forme quadratique binaire $ax^2+bxy+cy^2$ par (a,b,c) et identifierons le terme forme quadratique binaire par FQB.

Définition 1. Une FQB (a,b,c) est *primitive* lorsque $\gcd(a,b,c) = 1$ i.e. lorsque ses coefficients sont premiers entre eux.

Définition 2. Le *discriminant* de la FQB (a,b,c) est $D = b^2 - 4ac$. La notation pour ce discriminant est $Disc((a,b,c))$ ou simplement D lorsque le contexte est clair.

Remarquons ensuite que pour les FQB entières, $D \equiv 0$ ou $1 \pmod 4$. En effet, $4ac \equiv 0 \pmod 4$ en tout cas, ce qui implique que $D \equiv b^2 \equiv 0$ ou $1 \pmod 4$ puisqu'il s'agit d'un carré. Dans le présent document, nous allons nous attarder au cas le plus fréquent, c'est-à-dire où $D < 0$. Aussi, même si la majorité des résultats fonctionnent pour tout discriminant (sauf lorsque spécifié), nous travaillerons souvent avec $D \equiv 1 \bmod 4$.

Définition 3. Une FQB Q est dite *définie positive* si pour toute paire de nombres réels $(x,y) \neq (0,0)$, $Q(x,y) > 0$.

Il est démontré dans [2] par la Proposition 1.2.9 qu'une forme (a,b,c) est définie positive si et seulement si $\operatorname{Disc}((a,b,c)) < 0$ et $a > 0$. Ici, nous travaillerons exclusivement avec des formes définies positives.

2 Équivalence des FQB

Au lieu d'étudier l'ensemble des FQB d'un certain discriminant, il est utile de définir une relation d'équivalence entre plusieurs FQB d'un même discriminant. Il est naturel de voir deux formes comme étant équivalentes si elles représentent les mêmes entiers. Définissons en premier lieu l'action d'une matrice 2×2 sur nos FQB.

2.1 Relation d'équivalence

Définition 4. Nous définissons l'action de la matrice $\left(\begin{smallmatrix}\alpha & \beta \\ \gamma & \delta\end{smallmatrix}\right) \in SL_2(\mathbb{Z})$ sur une FQB $Q(x,y)$ comme

$$\begin{aligned} Q(x,y) * \begin{pmatrix}\alpha & \beta \\ \gamma & \delta\end{pmatrix} \\ = Q(\alpha x + \beta y, \gamma x + \delta y). \end{aligned}$$

Remarquons premièrement qu'il s'agit ici d'un simple changement linéraire de variable défini comme

$$\begin{pmatrix}x' \\ y'\end{pmatrix} = \begin{pmatrix}\alpha & \beta \\ \gamma & \delta\end{pmatrix}\begin{pmatrix}x \\ y\end{pmatrix}.$$

Remarquons aussi l'importance pour une telle matrice d'être élément de $SL_2(\mathbb{Z})$. Premièrement, il est clair que, pour que la forme résultante soit entière, il faut que $\alpha, \beta, \gamma, \delta \in \mathbb{Z}$. Aussi, il est nécessaire, pour conserver le même discriminant, que le déterminant de la matrice soit 1. En effet, il est possible de démontrer que

$$\left(ax^2+bxy+cy^2\right)*\begin{pmatrix}\alpha & \beta\\ \gamma & \delta\end{pmatrix}= \\ \left(a\alpha^2+b\alpha\gamma+c\gamma^2\right)x^2 \\ +\left(2a\alpha\beta+b(\alpha\delta+\beta\gamma)+2c\gamma\delta\right)xy \\ +\left(a\beta^2+b\beta\delta+c\delta^2\right)y^2$$

et donc, nous avons le résultat suivant (voir [3, p.4]).

Fait 5.

$$Disc\left((a,b,c)*\begin{pmatrix}\alpha & \beta\\ \gamma & \delta\end{pmatrix}\right) \\ =\left[\det\begin{pmatrix}\alpha & \beta\\ \gamma & \delta\end{pmatrix}\right]^2\cdot Disc((a,b,c)).$$

Il s'ensuit que les seules matrices conservant le discriminant sont celles de déterminant ± 1. Bien qu'il soit possible d'utiliser des matrices de déterminant -1, nous ne le ferons pas pour des raisons d'orientations qui seront détaillées plus loin.

Cette opération sur les FQB est ensuite utilisée pour définir une relation d'équivalence.

Définition 6. La FQB (a,b,c) est équivalente à (d,e,f) si et seulement si il existe une matrice M dans $SL_2(\mathbb{Z})$ tel que

$$(a,b,c)*M=(d,e,f).$$

On dénote une telle équivalence par $(a,b,c)\sim(d,e,f)$.

Maintenant, prouvons qu'il s'agit bel et bien d'une relation d'équivalence.

Preuve.

1. $(a,b,c)\sim(d,e,f)\Rightarrow(d,e,f)\sim(a,b,c)$.
Si $(a,b,c)\sim(d,e,f)$, alors il existe une matrice $M=\left(\begin{smallmatrix}\alpha & \beta\\ \gamma & \delta\end{smallmatrix}\right)\in SL_2(\mathbb{Z})$ tel que $(a,b,c)*M=(d,e,f)$. Puisque $M\in SL_2(\mathbb{Z})$, $\det(M)=1$ et donc

$$\begin{pmatrix}\alpha & \beta\\ \gamma & \delta\end{pmatrix}^{-1}=\begin{pmatrix}\delta & -\beta\\ -\gamma & \alpha\end{pmatrix}\in SL_2(\mathbb{Z}).$$

Ainsi, $(d,e,f)*M^{-1}=(a,b,c)$ puisqu'il s'agit en fait du changement de variable inverse.

2. $(a,b,c)\sim(a,b,c)$.
Soit $M=\left(\begin{smallmatrix}1 & 0\\ 0 & 1\end{smallmatrix}\right)$, nous avons que $M\in SL_2(\mathbb{Z})$ et que

$$(a,b,c)*M=(a,b,c).$$

3. $(a,b,c)\sim(d,e,f)$ et $(d,e,f)\sim(q,r,s)\Rightarrow(a,b,c)\sim(q,r,s)$.
Nous avons que $ax^2+bxy+cy^2=dx'^2+ex'y'+fy'^2=qx''^2+rx''y''+sy''^2$ pour

$$\begin{pmatrix}x'\\ y'\end{pmatrix}=M\begin{pmatrix}x\\ y\end{pmatrix}\text{ et }\begin{pmatrix}x''\\ y''\end{pmatrix}=N\begin{pmatrix}x'\\ y'\end{pmatrix}$$

avec M et N dans $SL_2(\mathbb{Z})$ étant les matrices données par les relations d'équivalence de l'hypothèse. Ainsi,

$$\begin{pmatrix}x''\\ y''\end{pmatrix}=N\begin{pmatrix}x'\\ y'\end{pmatrix}=N\left[M\begin{pmatrix}x\\ y\end{pmatrix}\right]=(NM)\begin{pmatrix}x\\ y\end{pmatrix}$$

et donc nous avons la matrice $NM\in SL_2(\mathbb{Z})$ tel que

$$(a,b,c)*NM=(q,r,s)$$

ce qui prouve que $(a,b,c)\sim(q,r,s)$.

□

Ainsi, au lieu de considérer des FQB, nous considérons des classes d'équivalence de FQB selon la relation définie ci-haut. La raison pour cette considération est, qu'étant donné que la majorité des études sur les FQB portaient sur la représentation des nombres entiers par une forme précise, il est alors sensé de considérer comme "équivalantes" deux formes qui peuvent être trouvées par une changement de variable, puisqu'il est aisé de voir que ces deux formes peuvent représenter exactement le même ensemble de nombres entiers. En effet, remplacer x et y par leur valeur numérique respective dans la formule matricielle de changement de variable présentée ci-dessus nous donne exactement les valeurs que x' et y' doivent prendre pour représenter le même nombre.

L'ensemble avec lequel nous travaillerons à partir d'ici sera donc l'ensemble quotient suivant

$$G_D:=FQB(D)\diagup SL_2(\mathbb{Z})$$

pour

$$FQB(D):= \\ \left\{Ax^2+Bxy+Cy^2:A,B,C\in\mathbb{Z},B^2-4AC=D\right\}.$$

Ainsi, nous introduisons la notation $[a,b,c]$ pour représenter la classe d'équivalence de la FQB (a,b,c).

2.2 *Classes d'équivalence et représentants*

Maintenant que nous avons défini une manière de regrouper les formes d'un même discriminant en des classes d'équivalence, nous voudrions avoir un ensemble de représentants.

Définition 7. Une FQB (a,b,c) est sous forme *réduite* si et seulement si

$$|b|\leq a\leq c.$$

Il est aussi possible de prouver une propriété très intéressante de cette forme réduite.

Fait 8. *Pour chaque FQB (a,b,c), il existe une unique FQB (a',b',c') sous forme réduite tel que $(a,b,c)\sim(a',b',c')$.*

La preuve est présentée dans [3, Th. 2.5] et consiste partiellement à développer un algorithme pour réduire chaque FQB à une forme réduite (voir [3, Th. 2.3]). Ainsi, par la propriété de transitivité de la relation d'équivalence, toute FQB appartenant à une même classe d'équivalence est associée à la même forme réduite. De plus, il ne peut s'agir de la même forme réduite pour deux classes d'équivalence différentes, ce qui en fait un excellent candidat pour être le représentant de cette classe.

Aussi, nous pouvons en déduire le résultat suivant.

Conséquence 9. *Il n'y a qu'un nombre fini de classes d'équivalence d'un disciminant fixe, i.e.*

$$|G_D| < \infty.$$

Preuve. Soit (a,b,c) une forme quadratique binaire de discriminant D sous forme réduite. Premièrement, nous avons puisque $D<0$ que

$$|D| = 4ac - b^2 \geq 4a^2 - a^2 = 3a^3$$

et donc que

$$a \leq \sqrt{\frac{|D|}{3}}.$$

Ainsi,

$$\begin{aligned} 0 \leq & a \leq \sqrt{\frac{|D|}{3}} \\ -\sqrt{\frac{|D|}{3}} \leq -a \leq & b \leq a \leq \sqrt{\frac{|D|}{3}} \end{aligned}$$

et puisque c est completement déterminé par a, b et D, il s'ensuit qu'il n'y a qu'un nombre fini de possibilités. Finalement, puisque chaque classe d'équivalence est représentée par une forme réduite unique, nous concluons qu'il n'y a qu'une nombre fini de classes d'équivalence. □

3 G_D UN GROUPE

En effet, un des résultats les plus importants sur ces FQB est que l'ensemble de leur classes d'équivalence pour un discriminant fixe, G_D, forme un groupe. De plus, par la Conséquence 9, il s'agit d'un groupe fini.

3.1 Loi de composition de Gauss

La question est donc: quelle peut être la loi de composition de ce groupe? La difficulté ici réside en le fait que deux classes de formes composées doivent en donner une troisième de même discriminant que les deux premières. Celui qui arriva avec la réponse parmi les premiers fût Gauss. Avant même que le concept de groupe soit d'usage, ces mathématiciens trouvèrent une méthode pour composer des FQB, méthode basée sur les manipulations algébriques suivantes. En effet, la technique suivante était apparamment connu depuis très longtemps. Il s'agit d'un méthode pour réduire l'expression

$$\begin{aligned} &\left(x^2+Dy^2\right)\left(z^2+Dw^2\right) \\ &= x^2z^2 + Dw^2x^2 + Dy^2z^2 + D^2y^2w^2 \\ &= (xz+Dyw)^2 - 2Dywxz + D\left(w^2x^2+y^2z^2\right) \\ &= (xz+Dyw)^2 + D(wx+yz)^2 \end{aligned}$$

en une expression de forme $x'^2 + Dy'^2$ où $x' = xz + Dyw$ et $y' = wx + yz$, i.e. où les nouvelles variables sont des combinaisons *non-linéaires* des anciennes variables. Ainsi, nous avons composé ces deux expressions de degré 2 pour en obtenir une de degré 4, mais en ayant de nouvelles variables qui sont définies comme des expressions de degré 2, nous avons retrouvé une expression finale de degré 2. La même idée est utilisée pour la composition de FQB chez Gauss. Il s'agit en fait d'une simple multiplication en définissant de nouvelles variables pour que le degré reste approprié, et pour que le discriminant reste le même. Le changement de variable correspondant à la composition de $\left(a_1x_1^2 + b_1x_1y_1 + c_1y_1^2\right) \circ \left(a_2x_2^2 + b_2x_2y_2 + c_2y_2^2\right) = AX^2 + BXY + CY^2$ ressemblait à

$$\begin{pmatrix} X \\ Y \end{pmatrix} = \begin{pmatrix} p_0 & p_1 & p_2 & p_3 \\ q_0 & q_1 & q_2 & q_3 \end{pmatrix} \begin{pmatrix} x_1x_2 \\ x_1y_2 \\ y_1x_2 \\ y_1y_2 \end{pmatrix}$$

où les p_i et q_i pour $i = 0, \ldots, 3$ sont des entiers determinés par $a_1, a_2, b_1, b_2, c_1, c_2$. Cette méthode de composition a été simplifiée computationellement par l'utilisation des *formes unies de Dirichlet*. La méthode consiste à trouver des formes équivalentes aux formes (a_1, b_1, c_1) et (a_2, b_2, c_2) à composer tel que

$$\begin{aligned} (a_1,b_1,c_1) &\sim (a_1, B, a_2C) \\ (a_2,b_2,c_2) &\sim (a_2, B, a_1C) \end{aligned}$$

Ainsi, nous aurions $[a_1,b_1,c_1] \circ [a_2,b_2,c_2] = [a_1a_2, B, C]$. Ce dernier algorithme est beacoup plus efficace au niveau computationel, mais il y a beaucoup de preuves à faire concernant l'existence de telles formes et la raison pour l'équivalence de la dernière égalité avec la loi présentée précédemment (voir [3, Section 4.2]).

Aussi, selon cette loi de groupe, remarquons que nous avons comme élément neutre de ce groupe la classe de formes représentée par $\left[1, 0, \frac{D}{4}\right]$ dans le cas où $D \equiv 0 \bmod 4$ et $\left[1, 1, \frac{1-D}{4}\right]$ dans le cas où $D \equiv 1 \bmod 4$. Aussi, nous avons que l'inverse d'une forme (a,b,c) se trouve à être la forme $(a,-b,c)$. Nous retrouvons donc tous les éléments d'un groupe.

3.2 Cube de Bhargava

Une autre manière plus récente mais très ingénieuse nous est donné par Bhargava. Il s'agit de considérer le cube C d'entiers tel que représenté dans la figure 1.

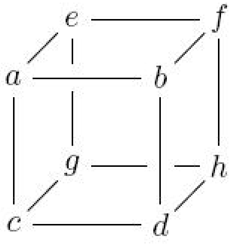


Figure 1: Le cube d'entiers C.

Nous pouvons alors effectuer des coupes dans le cube afin d'obtenir deux matrices 2×2 d'entiers. Les coupes sont faites de la manière suivante: la première coupe se fait en coupant le cube par le plan parallèle à la page passant par le centre du cube. La deuxième coupe est faite par le plan perpendiculaire à la page et vertical, et la dernière coupe est perpendiculaire à la page toujours mais horizontale. Chaque coupe nous donne deux matrices M_i et N_i qui, dans le cas de C, sont les suivantes

$$M_1 = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \qquad N_1 = \begin{pmatrix} e & f \\ g & h \end{pmatrix}$$

$$M_2 = \begin{pmatrix} a & c \\ e & g \end{pmatrix} \qquad N_2 = \begin{pmatrix} b & d \\ f & h \end{pmatrix}$$

$$M_3 = \begin{pmatrix} a & e \\ b & f \end{pmatrix} \qquad N_3 = \begin{pmatrix} c & g \\ d & h \end{pmatrix}.$$

Aussi, nous définissons ici l'action de certaines matrices pour définir des classes d'équivalence. Nous avons que l'action de $SL_2(\mathbb{Z}) \times SL_2(\mathbb{Z}) \times SL_2(\mathbb{Z})$ est défini par

$$\begin{pmatrix} M_i' \\ N_i' \end{pmatrix} = E_i \begin{pmatrix} M_i \\ N_i \end{pmatrix}$$

où M_i' et N_i' sont les matrices du cube C' pour

$$C' = (E_1, E_2, E_3) * C$$

et où $E_i \in SL_2(\mathbb{Z})$ pour $i = 1,2,3$.

Ainsi, nous définissons que lorsqu'un cube peut être trouvé à partir d'un autre grâce à une telle transformation, les deux cubes sont équivalents. Cette définition de relation d'équivalence est très similaire à celle des FQB telle que nous l'avons définie plus haut.

Ensuite, nous pouvons avec chaque couple de matrices obtenu par une coupe, retrouver une FQB selon la formule suivante. Nous avons que

$$Q_i^C(x,y) = -\det(M_i x - N_i y)$$

qui nous donne une FQB. Il est démontré dans [1, p.220] que chacune des trois formes résultantes possède le même discriminant. Ainsi, Bhargava défini une loi de composition selon la règle suivante.

Définition 10.

$$Q_1^C + Q_2^C + Q_3^C = 0.$$

Ainsi, pour composer deux formes quadratiques binaire f et g, nous trouvons un cube C tel que $f = Q_1^C$ et $g = Q_2^C$. Alors, leur composition est donnée par l'inverse de Q_3^C. La beauté de cette technique réside dans son étonnante simplicité, mais elle peut être trompeuse. Bien qu'il semble simple de composer deux formes ainsi, l'étape problématique reste de retrouver le cube qui correspond aux deux formes données. Ainsi, même si conceptuellement cette technique est très simple et efficace, il n'en est rien computationellement.

3.3 Modules et idéaux

Cette dernière méthode pour composer des classes de FQB est probablement la plus populaire à toutes fins pratiques. Il s'agit d'associer à chaque FQB un idéal dans un module spécifique et de multiplier les idéaux pour trouver l'idéal associé à la forme résultante de la composition.

On associe à la classe de forme de discriminant D l'ensemble u

$$[A,B,C] \mapsto u = \mathbb{Z} \cdot A + \mathbb{Z} \cdot \left(\frac{-B + \sqrt{D}}{2} \right).$$

Ainsi, u est un O-module où O est l'anneau des entiers d'un corps quadratique K, i.e. $O = \mathbb{Z}\left[\frac{D+\sqrt{D}}{2}\right]$. Ensuite, nous considérons u comme un idéal de O, ce qui a du sens puisque les deux concepts sont très similaires: il ne s'agit que d'un groupe additif stable par la multiplication par O. Par contre, puisque O n'est pas un anneau principal, nous ne savons pas combien d'éléments génere cet idéal u. C'est pourquoi nous considérons à la place ce sous-ensemble de O comme un module sur l'ensemble des entiers. Nous pouvons aussi considérer ce module comme un idéal dans lequel nous aurions restreint la multiplication scalaire par $\mathbb{Z}$. De plus, en tant que $\mathbb{Z}$-module, ce module est libre de rang 2, ce qui veux dire que le nombre maximal d'éléments linéairement dépendants dans ce module est de deux. Nous avons ensuite le fait suivant.

Fait 11. *Tout module sans torsion sur $\mathbb{Z}$ est isomorphe à $\mathbb{Z}^r$ pour r le rang du module.*

La preuve peut être trouvée dans [4, Ch.12, Th. 6]. Ainsi, il est clair que pour le module spécifié ci-haut sur $\mathbb{Z}$, nous pouvons en tous cas trouver deux générateurs. Alors, u correspond à $I_1 = \langle e_1, e_2 \rangle$, et nous avons trivialement $e_1 = A$ et $e_2 = \frac{-B+\sqrt{D}}{2}$.

L'idée ensuite est de trouver de tels idéaux pour les deux classes à composer et de multiplier ces idéaux. Nous définissons la multiplication d'idéaux de manière très intuitive: il s'agit de considérer les éléments trouvés par la multiplication des éléments des deux idéaux. Autrement dit,

$$I_3 = [I_1]\,[I_2] = \{ab : a \in I_1, b \in I_2\}\,.$$

Remarquons par contre que si $I_1 = \langle e_1, e_2\rangle$ et $I_2 = \langle f_1, f_2\rangle$, alors

$$I_3 = \langle e_1 f_1, e_1 f_2, e_2 f_1, e_2 f_2\rangle\,.$$

Aussi, nous savons par les faits mentionnés ci-haut que nous sommes en mesure de trouver une base de deux éléments à ce dernier idéal I_3. Nous devrons donc trouver une base $\langle g_1, g_2\rangle$ équivalente à celle de quatre éléments détaillée précédemment. Pour prouver cette équivalence, il sufit de montrer que $\langle g_1, g_2\rangle \subseteq \langle e_1 f_1, e_1 f_2, e_2 f_1, e_2 f_2\rangle$ et vice versa, en outre donc montrer que

$$g_1, g_2 \in \langle e_1 f_1, e_1 f_2, e_2 f_1, e_2 f_2\rangle$$

et

$$e_1 f_1, e_1 f_2, e_2 f_1, e_2 f_2 \in \langle g_1, g_2\rangle$$

en ne perdant pas d'esprit que la multiplication scalaire est restreinte à $\mathbb{Z}$.

Une fois ceci fait, nous retrouverons la FQB Q_3 correspondant à I_3 par

$$\begin{aligned} Q_3 &= \text{norme}\,(x \cdot g_1 + y \cdot g_2) \\ &= (g_1\overline{g_1})x^2 + (g_1\overline{g_2} + \overline{g_1}g_2)xy + (g_2\overline{g_2})y^2 \end{aligned}$$

où $\overline{(\alpha + \beta\sqrt{D})} := \alpha - \beta\sqrt{D}$.

Par contre, avant d'effectuer cette étape, il faut s'occuper d'orienter la base. En effet, étant donné qu'il est possible de multiplier la base par $-1 \in \mathbb{Z}$ à volonté, et que selon la formule ci-dessus ces deux bases donnent des formes inverses, il nous faut choisir une de ces deux bases. Pour se faire, remarquons tout d'abord que pour $I = \langle e_1, e_2\rangle$,

$$\det\begin{pmatrix} e_1 & e_2 \\ \overline{e_1} & \overline{e_2} \end{pmatrix} \in \mathbb{Z} \cdot \sqrt{D}.$$

De ce fait, si

$$\det\begin{pmatrix} e_1 & e_2 \\ \overline{e_1} & \overline{e_2} \end{pmatrix} = n \cdot \sqrt{D}$$

tel que $n > 0$, alors e_1, e_2 forment une base positive. Sinon, $e_1, -e_2$ forment une base positive.

Remarquons premièrement qu'une classe de forme $[A,B,C]$ sera associée à l'idéal $I = \left\langle A, \frac{B-\sqrt{D}}{2}\right\rangle$ (base orientée puisque l'on supose que $A > 0$) et qu'ensuite, la forme associée à cet idéal selon notre méthode est $\left(A^2, AB, \frac{B^2-D}{4}\right)$, mais puisque $D = B^2 - 4AC$, nous avons $\left(A^2, AB, AC\right)$. Pour que cette forme soit primitive, nous devons factoriser le facteur commun A pour retrouver la forme (A,B,C).

Aussi, nous aurions très bien pu prendre une base différente et bien orientée en additionnant un des générateurs à l'autre, par exemple, $\left\langle A, A + \frac{B-\sqrt{D}}{2}\right\rangle$. Dans ce cas, il est possible que la forme résultante à la fin du procédé ne soit pas sous forme réduite. On applique alors l'algortihme utilisé dans la preuve du Fait 8 pour réduire cette forme.

Finalement, remarquons qu'étant donné que I_3, l'idéal multiplié, est aussi un O-module au même titre que I_1 et I_2, la forme correspondante aura bel et bien discriminant D.

Pour récapituler, l'algorithme pour composer deux classes de formes est le suivant: Premièrement, prendre les représentants des deux classes à composer et les associer à deux idéaux $I_1 = \langle e_1, e_2\rangle, I_2 = \langle f_1, f_2\rangle$. Ensuite, il faut considérer l'idéal $I_3 = \langle e_1 f_1, e_1 f_2, e_2 f_1, e_2 f_2\rangle$ et trouver une base de deux éléments équivalente à celle de quatre éléments. Nous devons alors orienter cette base et appliquer la formule de la norme pour retrouver une FQB. Enfin, il ne reste qu'à factoriser les trois éléments de cette forme et à appliquer l'algorithme de réduction pour obtenir une forme réduite. Nous avons ainsi le représentant de la classe de FQB issue de la composition des deux premières classes. Voici un exemple.

Problème. Quel est la classe de FQB correspondant à la composition de $[2,1,3]$ avec elle-même?

Solution. Tout d'abord, nous établissons que nous travaillons dans G_{-23}. Il est possible de démontrer en utilisant le principe des formes réduites qu'il n'y a que trois classes de formes dans ce groupe. Premièrement, il y a la classe correspondant à l'élément neutre, $[1,1,6]$. Aussi, nous avons évidemment la classe $[2,1,3]$ ainsi que son inverse $[2,-1,3]$. La classe composée sera alors une de ces trois. Maintenant puisque le groupe a ordre 3, il s'ensuit que $G_{-23} \cong \mathbb{Z}/3\mathbb{Z}$, et donc $[2,1,3]^2 = [2,-1,3]$, mais vérifions tout de même ceci en utilisant la technique décrite.

Soit $[2,1,3] \mapsto 2\mathbb{Z} + \frac{-1+\sqrt{-23}}{2}\mathbb{Z}$. Nous avons

$$I_3 = \left\langle 4, -1+\sqrt{-23}, -1+\sqrt{-23}, \left(\frac{-1+\sqrt{-23}}{2}\right)^2 \right\rangle$$

Premièrement, il est clair que nous pouvons exclure le troisième générateur pour obtenir une base équivalente à trois éléments. Ensuite, nous avons

$$\begin{aligned} \left(\frac{-1+\sqrt{-23}}{2}\right)^2 &= \frac{1}{4}\left(1 - 23 - 2\sqrt{-23}\right) \\ &= \frac{-11-\sqrt{-23}}{2}. \end{aligned}$$

Par contre, nous avons que $-1+\sqrt{-23} \in \left\langle 4, \frac{-11-\sqrt{-23}}{2} \right\rangle$ puisque

$$\left(\frac{11-\sqrt{-23}}{2}\right)\cdot(-2)-4\cdot 3 = -1+\sqrt{-23}$$

et donc $I_3 = \left\langle 4, \frac{-11-\sqrt{-23}}{2} \right\rangle$ (les autres inclusions sont triviales). Avant tout, nous pouvons réduire cette base en additionnant 4 au second élément pour obtenir $I_3 = \left\langle 4, \frac{-3-\sqrt{-23}}{2} \right\rangle$. Ensuite, nous remarquons que la base est déja orientée positivement. Nous avons donc

$$Q_3 = 16x^2 - 12xy + 8y^2 = 4\left(4x^2 - 3xy + 2y^2\right).$$

Mais la FQB $(4,-3,2)$ n'est pas sous forme réduite. Nous appliquons donc l'agorithme de réduction pour avoir que $(4,-3,2) \sim (2,-1,3)$ puisque

$$(4,-3,2) * \begin{pmatrix} 0 & 1 \\ -1 & 1 \end{pmatrix} = (2,-1,3)$$

et donc

$$[2,1,3]\circ[2,1,3] = [2,-1,3].$$

□

References

[1] Bhargava, Manjul. *Higher composition laws I: A new view on Gauss composition, and quadratic generalizations*. Annals of Mathematics, 159 (2004): 217 – 250.

[2] Buchmann, Johannes; Vollmer, Ulrich. *Binary Quadratic Forms : An Algorithmic Approach*. Berlin: Springer-Verlag, 2007.

[3] Buell, D.A. *Binary Quadratic Forms : Classical Theory and Modern Computations*. New York: Springer-Verlag, 1989.

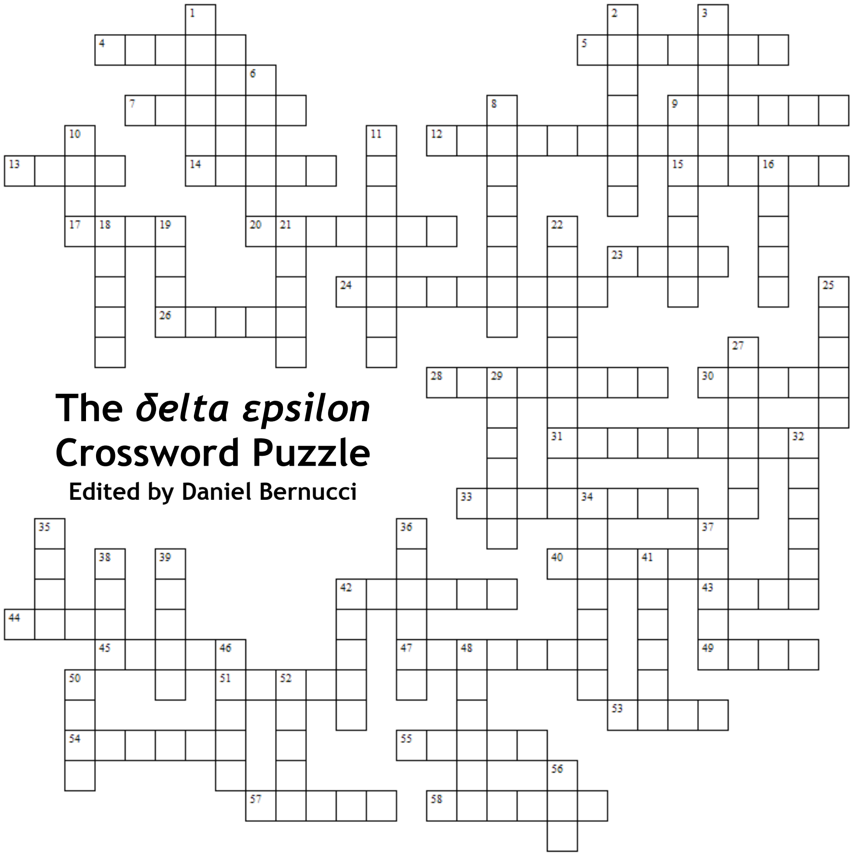
[4] Dummit, D.S., and Foote, R.M. *Abstract Algebra* 3$^{\text{e}}$ ed. New Jersey: Wiley & Sons, 2004.

Jokes

Lors d'un grand jeu télévisé, les trois concurrents se trouvent être un ingénieur, un physicien et un mathématicien. Ils ont une épreuve à réaliser. Cette épreuve consiste à construire une clôture tout autour d'un troupeau de moutons en utilisant aussi peu de matériel que possible.
L'ingénieur fait regrouper le troupeau dans un cercle, puis décide de construire une barrière tout autour.
Le physicien construit une clôture d'un diamètre infini et tente de relier les bouts de la clôture entre eux jusqu'au moment où tout le troupeau peut encore tenir dans le cercle.
Voyant ça, le mathématicien construit une clôture autour de lui-même et dit en pointant où il se trouve: "Définissons cette partie comme étant l'extérieur...". □

Un biologiste, un physicien et un mathématicien sont assis à la terrasse d'un café et regardent les passants. De l'autre côté de la rue, ils voient un homme et une femme entrer dans un immeuble. 10 minutes plus tard, ils ressortent avec une troisième personne.
- Ils se sont multipliés, dit le biologiste.
- Oh non, une erreur de mesure s'écrie le physicien.
- S'il rentre exactement une personne dans l'immeuble, il sera de nouveau vide, conclut le mathématicien. □

A woman walks into a bar accompanied by a dog and a cow. The bartender says, "Hey, no animals are allowed in here"
The woman replies, "These are very special animals."
"How so?"
"They're knot theorists."
The bartender raises his eyebrows and says, "I've met a number of knot theorists who I thought were animals, but never an animal that was a knot theorist."
"Well, I'll prove it to you. Ask them them anything you like."
So the bartender asks the dog, "Name a knot invariant."
"Arf, arf" barks the dog.
The bartender scowls and turns to the cow asking, "Name a topological invariant."
The cow says, "Mu, mu."
At this point the bartender turns to the woman, says, "Just what are you trying to pull" and throws them out of the bar.
Outside, the dog turns to the woman and asks, "Do you think I should have said the Jones polynomial?" □



The *δelta εpsilon* Crossword Puzzle

Edited by Daniel Bernucci

ACROSS
4 A colorful mathematician?
5 [*a*, *b*] is, e.g.
7 __ canonical form
9 In contrast to vector
12 Shortest path
13 Trig function
14 Butterfly effect
15 A type of group
17 Its complement is closed
20 Matrix used to find extrema
23 In programming, a method that returns nothing
24 Method of proof
26 Syrup for computing integrals?
28 Formal statements
30 Test for convergence
31 Where each point has its own neighborhood
33 As opposed to continuous
40 Everything here vanishes
42 Logical quantifier
43 Part of QED
44 Angry average?
45 A normal mathematician
47 Friend of delta
49 In PDE's, __ equation
51 There is no better ring
53 Part of iff
54 A variable out of nowhere?
55 Spooky remains of a fixed point
57 In all sets
58 Axiom of __

DOWN
1 Distance
2 __ series
3 See 34-down
6 Complete and normed, as spaces
8 When all 3-down sequences converge
10 Type of function
11 Standard deviation squared
15 A rule for derivatives
16 As *x* approaches…
18 All 28-across' need one
19 Socially acceptable length
21 Mathematician from Edmonton?
22 Structurally identical
25 A prolific mathematician
27 Keanu Reeves meets linear algebra
29 His algorithm computes 56-downs
32 If only he had bigger margins!
34 With 3-down, their equations ensure analycity
35 A type of graph
36 Where edges meet
37 Letter denoting the cardinality of infinite sets
38 Z/nZ to a married man?
39 A type of estimator
41 His method finds zeroes
42 Where cows graze and algebraists divide
46 Sums it up
48 Michael Jackson's hit, "Continuously differentiable criminal"?
50 A vector operator
52 A vector, value, space or function
56 (8, 20) = 4, e.g.

CREDITS

in alphabetical order

The δelta-εpsilon Editing Team

- Daniel Bernucci
- Cyndie Cottrell
- François Séguin
- Cathryn Supko

Cover Art and Design

- François Séguin

Reviewing Board

- Luca Candelori
- Victoria de Quehen
- Jan Feys
- Daphna Harel
- Sean Kennedy
- Tony Li
- Marc Masdeu
- Maksym Radziwill
- Alexandre Tomberg

We would like to give credit to the following websites for the math jokes in this year's issue:
`http://www.xkcd.com`
`http://www.reddit.com`
`http://mathoverflow.net`
`http://www.math.ualberta.ca/~runde/jokes.html`
`http://www.ams.org/notices/200501/fea-dundes.pdf`
`http://www.xs4all.nl/~jcdverha/scijokes/1.html`

ACKNOWLEDGEMENTS

Firstly we would like to thank Dr. Axel Hundemer and Dr. Heekyoung Hahn for taking the time to talk with us and for their valuable advice. We would also like to thank everyone on our reviewing board for their contributions in ensuring the quality of this publication. In addition, thank you to the authors of articles which appeared in this edition, as well as Spencer Frei for his contribution to the comedic sections. Thanks to SUMS, the Department of Mathematics and Statistics, the Arts Undergraduate Society and the Science Undergraduate Society for the generous financial support. Finally, we extend a special thanks to last year's editing team, as your work and advice has been key to the realization of this year's issue.

CROSSWORD PUZZLE SOLUTION