Irish Mathematical Society
Cumann Matamaitice na hÉireann

Bulletin

Number 95 Summer 2025

ISSN 0791-5578

Irish Mathematical Society
Bulletin

The aim of the *Bulletin* is to inform Society members, and the mathematical community at large, about the activities of the Society and about items of general mathematical interest. It appears twice each year. The *Bulletin* is published online free of charge.

The *Bulletin* seeks articles written in an expository style and likely to be of interest to the members of the Society and the wider mathematical community. We encourage informative surveys, biographical and historical articles, short research articles, classroom notes, book reviews and letters. All areas of mathematics will be considered, pure and applied, old and new.

Correspondence concerning books for review in the *Bulletin* should be directed to

`mailto://reviews.ims@gmail.com`

All other correspondence concerning the *Bulletin* should be sent, in the first instance, by e-mail to the Editor at

`mailto://ims.bulletin@gmail.com`

and only if not possible in electronic form to the address

The Editor
Irish Mathematical Society Bulletin
School of Mathematical Sciences
Western Gateway Building
University College Cork
Cork T12 XF62
Ireland.

Submission instructions for authors, back issues of the *Bulletin,* and further information about the Irish Mathematical Society are available on the IMS website

`http://www.irishmathsoc.org/`

The Irish Mathematical Society is a registered charity (RCN: 20020279).

Irish Mathematical Society Bulletin 95, Summer 2025

CONTENTS

EDITORIAL

This is Issue Number 95 of the IMS Bulletin, my second. I hope you will enjoy reading this summer's articles spanning a range of topics. Stephen Buckley and Tony O'Farrell continue their work from Issue 84 on wiring switches to light bulbs. Steven Dougherty has a comprehensive account of the history of coding theory emphasizing how the subject developed from a problem in engineering / signal processing to an area of pure mathematics with mutually enriching connections to other areas of mathematics. Nathan Parker, a PhD student of Gordon Blower in Lancaster, shares interesting results on reproducing kernel Hilbert spaces. Tommy Murphy, a former student of ours at UCC and now at California State University, Fullerton, together with his undergraduate students Khushi Kaushik and David Weed, introduces us to Conway's model, FRACTRAN, of a Turing machine.

Thanks to the Bulletin's Book Review Editor, Eleanor Lingham, and the work of reviewers Christopher Bishop and Brendan Masterson, we have reviews of a complex analysis textbook by this editor and of Susan M. C. Mac Donald's book *Euclid Transmogrified: A National Scandal* on the history of the teaching of geometry in Ireland's second level school system.

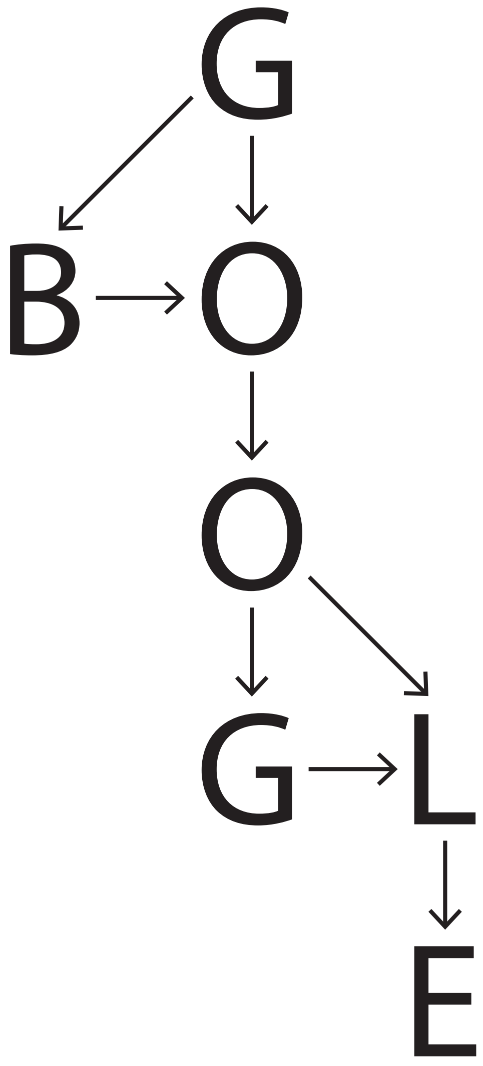
The issue is nicely rounded off by a selection of interesting problems edited by J.P. McCarthy.

Remember that, for a limited time and beginning as soon as possible after the online publication of this Bulletin, a printed and bound copy may be ordered online on a print-on-demand basis at a minimal price[1].

Finally, my thanks to Des MacHale (UCC) for his permission to include the graphic on the next page connecting GBOOLE and GOOGLE.

[1] Go to `www.lulu.com` and search for *Irish Mathematical Society Bulletin*.

A GBOOLE and GOOGLE CONNECTION



Editor, Bulletin IMS, School of Mathematical Sciences, Western Gateway Building, University College Cork, Cork, Ireland.

E-mail address: ims.bulletin@gmail.com

LINKS FOR POSTGRADUATE STUDY

The following are the links provided by Irish Schools for prospective research students in Mathematics:

DCU: mailto://maths@dcu.ie
TUD: mailto://chris.hills@tudublin.ie
ATU: mailto://leo.creedon@atu.ie
MTU: http://mathematics.mtu.ie/datascience
UG: mailto://james.cruickshank@universityofgalway.ie
MU: mailto://mathsstatspg@mu.ie
QUB:
https://www.qub.ac.uk/schools/SchoolofMathematicsandPhysics/Research/culture-environment/PostgraduateResearch/
TCD: http://www.maths.tcd.ie/postgraduate/
UCC: https://www.ucc.ie/en/matsci/study-maths/postgraduate/#d.en.1274864
UCD: mailto://nuria.garcia@ucd.ie
UL: mailto://Romina.Gaburro@ul.ie

The remaining schools with Ph.D. programmes in Mathematics are invited to send their preferred link to the editor.

E-mail address: ims.bulletin@gmail.com

NOTICES FROM THE SOCIETY

Officers and Committee Members 2025

President	Dr Rachel Quinlan	UG
Vice-President	Prof. David Malone	MU
Secretary	Dr Derek Kitson	MIC
Treasurer	Dr Cónall Kelly	UCC

Assoc. Prof. C. Boyd, Dr R. Flatley, Dr R. Gaburro, Dr T. Huettemann, Prof. Emeritus P. Lynch, Dr P. Ó Catháin, Prof. A. O'Shea, Assoc. Prof. H. Šmigoc, Dr N. Snigireva.

Local Representatives

Belfast	QUB	Prof. M. Mathieu
Carlow	SETU	Dr D. Ó Sé
Cork	MTU	Dr J. P. McCarthy
	UCC	Dr S. Wills
Dublin	DIAS	Prof. T. Dorlas
	TUD, City	Dr D. Mackey
	TUD, Tallaght	Dr C. Stack
	DCU	Prof. B. Nolan
	TCD	Prof. K. Soodhalter
	UCD	Dr R. Levene
Dundalk	DKIT	Mr Seamus Bellew
Galway	UG	Dr J. Cruickshank
Limerick	MIC	Dr B. Kreussler
	UL	Dr Romina Gaburro
Maynooth	MU	Prof. S. Buckley
Sligo	ATU	Dr L. Creedon
Tralee	MTU	Prof. B. Guilfoyle
Waterford	SETU	Dr P. Kirwan

Applying for I.M.S. Membership

(1) The Irish Mathematical Society has reciprocity agreements with the American Mathematical Society, the Deutsche Mathematiker Vereinigung, the Irish Mathematics Teachers' Association, the London Mathematical Society, the Moscow Mathematical Society, the New Zealand Mathematical Society and the Real Sociedad Matemática Española.

(2) The current subscription fees are given below:

Institutional member	€250
Ordinary member	€40
Lifetime member	€400
Student member	€20
DMV, IMTA, NZMS, MMS or RSME reciprocity member	€20
AMS reciprocity member	$25
LMS reciprocity member (paying in Euro)	€20
LMS reciprocity member (paying in Sterling)	£20

(3) The subscription fees listed above should be paid in euro by means of electronic transfer, a cheque drawn on a bank in the Irish Republic, or an international money-order.

The subscription fee for ordinary membership can also be paid in a currency other than euro using a cheque drawn on a foreign bank according to the following schedule:

If paid in United States currency then the subscription fee is US$40.
If paid in sterling then the subscription is £30.
If paid in any other currency then the subscription fee is the amount in that currency equivalent to US$40.

The amounts given in the table above have been set for the current year to allow for bank charges and possible changes in exchange rates.

(4) Any member with a bank account in the Irish Republic may pay his or her subscription by a bank standing order using the form supplied by the Society.

(5) Any ordinary member who has reached the age of 65 years and has been a fully paid up member for the previous five years may pay at the student membership rate.

(6) Those members who have reached 75 years of age, and who have been members in good financial standing with the Society for the previous 15 years, are entitled upon notification to the Treasurer to have their subscription rate reduced to €0.

(7) Subscriptions normally fall due on 1 February each year.

(8) Cheques should be made payable to the Irish Mathematical Society.

(9) Any application for membership must be presented to the Committee of the I.M.S. before it can be accepted. This Committee meets three times each year.

(10) Please send the completed application form, available at
`https://www.irishmathsoc.org/business/imsapplicn_2024.pdf`
with one year's subscription, either by post or by email, to:

Dr Cónall Kelly
School of Mathematical Sciences
Western Gateway Building
University College Cork
Cork, T12 XF62, Ireland
`subscriptions.ims@gmail.com`

Irish Math. Soc. Bulletin
Number 95, Summer 2025, 3– 21
ISSN 0791-5578

Coding Theory: The story of how an engineering problem evolved into a branch of pure mathematics

STEVEN T. DOUGHERTY

Abstract. We describe how a very practical engineering problem involving the transmission of electronic information evolved into beautiful, interesting, pure mathematics with branches in algebra, combinatorics, and number theory.

1. Introduction

Throughout the development of mathematics, interesting questions from other disciplines have sparked new mathematics to emerge. For example, when Newton discovered calculus [27], he was doing so largely to answer questions about motion and gravity (in contrast to Leibniz's motivation, which was quite different [23]). However, no one doing real analysis today would think that what they were doing was completely in service to questions of motion or gravity. The mathematics of calculus developed on its own as pure mathematics after it was born to answer applied questions. Similarly, Newton's minimal resistance problem [27] gave rise to the calculus of variations, which sparked a great deal of mathematics. Modern physics has also given mathematicians plenty to study arising from topics like string theory and the theory of relativity. After all, where would differential equations and differential geometry be without a constant flow of problems from physics and engineering. Outside of analysis, Euler developed graph theory to answer the fairly easy recreational question about the bridges of Königsberg [10]. This simple problem gave rise to one of the most useful and interesting branches of discrete mathematics. Moreover, numerous applied problems have been solved using the techniques developed in graph theory. In a similar way, Euler developed the study of Latin squares from the much more difficult recreational problem of arranging 36 officers in a square [11] (the problem took over 100 years to solve after Euler started the approach). In this paper, we are going to describe another situation where a mathematical discipline arose from an engineering problem in the twentieth century to become a highly active and interesting area of pure mathematics. In fact, one could argue that several highly interesting pure branches of coding theory have emerged, such as algebraic geometry codes and codes over rings. In both of these areas, an existing branch of pure mathematics, specifically algebraic geometry and ring theory, was first used in the service of practical coding theory and then was highly enriched as pure mathematics from the techniques that were used in the application. In this paper, while we do talk about algebraic geometry, our main focus will be the development of the study of codes over rings and other alphabets as pure mathematical objects.

1.1. **Coding Theory is Born.** In the late 1940s, coding theory was born as a very practical solution to an engineering problem. At Bell Labs, when the information

2020 *Mathematics Subject Classification.* 01A60,11T71, 94B05 .
Key words and phrases. Coding Theory, Rings, Pure Mathematics.
Received on 28-02-2025; revised on 15/06/2025.
DOI: 10.33232/BIMS.0095.3.21.

age was in its infancy, scientists and engineers worked on practical problems for the monopolistic telephone giant. Basically, the idea arose that if the electronic device could realize that something was, in fact, an error, then the device should also be able to change the error so that with a very high probability the error could be changed to what it should be. In other words, if an error can be detected, it should be possible that the error can be corrected.

The first major step in this direction was made by Claude Shannon in 1948 in the paper "A mathematical theory of communication" [36]. It is impossible to overemphasize the profound effect this paper had on the emerging science of information theory. It is for this work and what follows that Shannon is often called the "Father of Information Theory". In this setting, communication generally means taking information, encoding it, passing it along a channel, decoding it, and receiving it. One can think of information being a message sent by an electronic device, which is encoded into a sequence of 0s and 1s. Then the information can be sent through a wire or over the airways, then it is decoded and received by another device. As an example, one might think of a telephone conversation. In this setting, noise may effect the message while it is in a channel. Certainly, anyone who has had telephone conversations has experienced a noisy channel. What Shannon showed was that effective communication can be conducted in virtually all situations. That is, no matter how noisy the channel is, one can still effectively communicate over it. However, he did not show exactly how this should be done, but rather that it was always possible. Thus began the long search for the mathematics that could make this happen.

2. Nomenclature and Early History

At this point, it might benefit the reader to give the definitions of the names of the disciplines (confusing as they are) that are being discussed. Information theory is the science of communicating, storing, and quantifying information. In general, this overarching term houses three different subjects. The first is coding theory, which studies how to communicate effectively, that is, how to correct errors with high probability that occur when transmitting data. The second is cryptology, which is the science of keeping information secret from bad actors as well as decrypting secret information made secret by someone else. Making messages secret is called cryptography with the obvious etymology of writing secrets and cryptanalysis is the branch which seeks to uncover what someone else has made secret. Here is where we meet our first difficulty in nomenclature, as we admit that often the term cryptography replaces the term cryptology to refer to the entire discipline. The third is called information theory, (which is our next difficulty in nomenclature). While information theory often refers to the entire subject, it also refers to the very practical engineering problem of the quantification of information and its transmission through a channel.

While the three topics are necessarily related and are often applied to the same information, the techniques used in these three disciplines are quite different. The mathematics behind coding theory is largely linear algebra with some help from combinatorics and abstract algebra. The mathematics behind modern cryptography is usually number theory (for example with the RSA crypto-system and the discrete log crypto-system) in non-symmetric key cryptosystems and finite field arithmetic, boolean functions, and other techniques from discrete mathematics in symmetric key cryptosystems. However, as we approach a post-quantum world, the techniques of cryptography are expanding quite rapidly to encompass numerous mathematical fields. The mathematics behind information theory is largely probability with some help from analysis. In actual transmission of information in our time, certainly, all three sciences are at work, as we desire to make the information correct, secure, and efficiently transmitted.

Shannon laid the foundation for all three of these disciplines. For coding theory there was the 1949 paper “Communication in the presence of noise” [37]; for information theory there was the 1948 paper “A mathematical theory of communication” [36]; and for cryptology there was the 1949 paper “Communication theory of secrecy systems” [38]. The three vitally important disciplines for the information age are based on these three seminal papers. We note that the first and third papers were published in the Bell System Technical Journal and the second was published in the proceedings of the IRE which has been renamed as the proceedings of the IEEE (Institute of Electrical and Electronics Engineers). It is quite clear that these are not mathematical journals, but rather very applied engineering journals. At that point, they were not trying to produce interesting mathematics, but rather using mathematics to solve very important and interesting engineering problems.

In this paper, we shall be concerned with the first of these sciences, which is coding theory. We shall show how it evolved from this application to become a branch of pure mathematics studied for its own sake rather than in the service of other applied disciplines.

Following Shannon’s landmark paper [36] in 1948, there came two more important papers. The first by Marcel Golay [16], in 1949, and the second by Richard Hamming [20] in 1950. Within these papers, the Golay codes and the Hamming codes were described. To this day, they remain some of the most discussed codes in coding theory. Moreover, the list of connections between these two families of codes to other interesting mathematical objects seems to never stop growing. It has often been said that if you want to interest a mathematician in coding theory you show them the length 23 Golay code, its connections to the Leech lattice, and its connections to finite groups (see [6] for a description of all of these connections) and any mathematician will quickly become interested in the topic.

3. Techniques of Coding Theory

The techniques that arose from these early papers are essentially the techniques that are still used today. First of all, you define an alphabet A. This alphabet consists of the symbols that one can send. Quite often, in the electronic world, the alphabet is the binary set $A = \{0, 1\}$, but other alphabets are possible. One can even think of the English language as a code over the Latin alphabet. While every discussion of coding theory begins by assuming that A is any set, it very quickly becomes clear that A must have some algebraic structure to make the techniques of coding theory effective. In those days, and in most applications today, it was assumed that A must be a finite field. In practice, A is often the finite field $\mathbb{F}_2$. However, even in early papers, results were often couched in terms of an arbitrary field since the proofs were the same.

While one might assume that the field $\mathbb{F}_2$ is the only field used in applications, this is not correct. Even when the information is stored as a 0 or a 1, one can use the field $\mathbb{F}_{2^r}$. For example, one can use $\mathbb{F}_{2^8}$ and deal with bytes rather than bits of information and still have the information stored as binary. The next task is to define the length of the code, usually denoted by n. Then a code of length n is simply any subset of the space A^n. That is, a code is simply a collection of length n vectors with entries from the alphabet A. Essentially, the code consists of all the possible “words” that you can send over the channel. This means that the only things you want the receiver to read are the elements of the code. In this way, if the receiver reads something that is not in the code, an error must have occurred.

One can think of the parallel situation for the English language when you receive something that is not a word. If you are sent, in a message, a collection of letters that are not an English word, you first recognize that it is not a word, then you try to determine what is the most likely word that was actually sent and had morphed into this collection of letters. This is the same situation as in coding theory. Therefore, the next step is to turn the ambient space, A^n, into a metric space which enables you to determine the distance between a received message and a possible word. This is done by defining the Hamming metric, which is $d_H(\mathbf{v}, \mathbf{w}) = |\{i \mid v_i \neq w_i\}|$ for vectors $\mathbf{v}, \mathbf{w} \in A^n$. It is clear at this point that if you want to define a code that is effective in correcting errors, you want the distance between vectors to be as large as possible. In particular, you want the minimal distance between two distinct vectors to be as large as possible. In that way, if some mistakes are made, it is clear what vector was originally sent.

In terms of the English language analogue, the distance is very small. For example, the words *can*, *cat*, and *car* only differ in one location. Therefore, if someone receives the word *cas*, without any context, it is impossible to know which of these three was the intended message. Mathematically, this is done in the following way. Define the minimum distance of a code C to be $d_C = \min\{d_H(\mathbf{v}, \mathbf{w}) \mid \mathbf{v}, \mathbf{w} \in C, \mathbf{v} \neq \mathbf{w}\}$. Then, using this code, you will be able to detect $d-1$ errors and can correct $\lfloor \frac{d-1}{2} \rfloor$ errors. In terms of the English example above, if you send *cat* and receive *car*, then you would not detect that an error was made since the minimum distance is only 1 in the English language. However, if your language consisted of two words 000 and 111 and you received 110 then you know that a mistake was made in transmission. You would want to correct the vector to 111 since that vector is distance 1 from the received vector, whereas 000 is distance 2 from the received vector. Of course, 2 mistakes might have been made in which case you correct the received vector to the wrong vector.

Already, this setting is sounding like a very mathematical problem. Namely, stated as a mathematical problem, what is the largest set of vectors $C \subseteq A^n$, where A is a set, such that the minimum distance between distinct vectors is d. One can rearrange this question by fixing any two of the parameters and optimizing the third. One can easily imagine this as placing ping pong balls in a room (in which they can float). You want to put as many in the room as possible but keep the distance between any two as far away as possible (two conflicting aims). Therefore, the question becomes how many pingpong balls can you put in the room where they are at least d units away.

3.1. **Bounds and Families of Codes.** Within this very simple combinatorial setting two very important results emerge. The first is the Singleton bound, which states that for a code C of length n over an alphabet of size q with minimum Hamming distance d, we have $\log_q(|C|) \leq n - d + 1$. The proof of this result is very easy and short, however the result has massive consequences. We call any code meeting this bound, that is, $\log_q(|C|) = n - d + 1$, a Maximal Distance Separable (MDS) code. These codes have been shown to be equivalent to many of the most important open questions in combinatorics. For example, a set of k-mutually orthogonal Latin squares is equivalent to certain MDS codes and as such the question of the existence of finite affine and projective planes can be couched in terms of MDS codes. Additionally, the central questions about orthogonal arrays can be phrased in terms of MDS codes. Moreover, there is a well known conjecture about these codes that arose in the study of finite geometry. Specifically, in 1955, Segre posed the MDS conjecture, which is as follows [35]. If $k \leq q$ then $n \leq q + 1$, unless $q = 2h$ and $k = 3$ or $k = q - 1$, in which case $n \leq q + 2$.

The second important result is the sphere packing bound, which states that for a code C of length n over an alphabet of size q with minimum Hamming distance at least $2t + 1$, we have $|C| \left(\sum_{s=0}^{t} C(n, s)(q-1)^s \right) \leq q^n$, where $C(n, s)$ is the binomial coefficient $\frac{n!}{s!(n-s)!}$. The proof of this result is a straightforward counting argument. Namely, $\sum_{s=0}^{t} C(n, s)(q-1)^s$ counts the number of vectors in a ball of radius t around a codeword, so the number of vectors times the number of vectors in the non-intersecting balls must be less than the number of vectors in the ambient space. A code that meets this bound, that is a code C over an alphabet of size q with minimum Hamming weight $2t+1$ and $|C|(\sum_{s=0}^{t} C(n,s)(q-1)^s) = q^n$, is said to be a perfect code. Important open questions remain about perfect codes, but some of the most important perfect codes were found right at the very beginnings of coding theory. Specifically, they were found by Golay in 1949 [16] and Hamming in 1950 [20].

3.2. **Foundations.** We shall describe the underlying mathematical structures laid forth in these early papers, which remain the foundation for modern coding theory. A generating matrix G is given, which is a k by n matrix with elements from a finite field $\mathbb{F}_q$ whose rows are linearly independent. Then, to encode the vector $\mathbf{v} \in \mathbb{F}_q^k$ from the alphabet $\mathbb{F}_q$, one computes $\mathbf{v}G$ to produce a length n codeword. In general, one encodes $\mathbb{F}_q^k$ to obtain a vector subspace of dimension k in $\mathbb{F}_q^n$, which is known as a linear code of length n and dimension k and denoted as an $[n,k]_q$ code. If, in addition, the minimum Hamming distance is known, it is denoted as an $[n,k,d]_q$ code. The fundamental question of coding theory then becomes: "what is the largest dimension k for which a k-dimensional subspace of $\mathbb{F}_q^n$ exists with minimum Hamming distance d." For linear codes, the Hamming distance turns out to be equal to the minimum Hamming weight where the Hamming weight is the number of non-zero entries in a vector and the minimum Hamming weight is the smallest Hamming weight of any non-zero vector in the code. At this point, one can see that this is fundamentally a mathematical question, which naturally interested mathematicians.

To decode information, the following technique was made. The ambient space $\mathbb{F}_q^n$ is endowed with the standard inner-product $[\mathbf{v},\mathbf{w}] = \sum v_i w_i$ and the orthogonal code is defined as $C^\perp = \{\mathbf{w} \mid [\mathbf{v},\mathbf{w}] = 0, \forall \mathbf{v} \in C\}$. A parity check matrix for C is an $(n-k)\times n$ matrix of rank $n-k$ whose row space is $C^\perp$. It is immediate that $\mathbf{v} \in C$ if and only if $H\mathbf{v}^T = \mathbf{0}$. This setting put the mechanics of coding theory solidly in the field of classical linear algebra. For example, one immediately has that $\dim(C) + \dim(C^\perp) = n$ and that $C^\perp$ must be a linear code. Then, one finds each coset of the code in the ambient space and defines it as $\mathbf{e} + C$ where $\mathbf{e}$ is a vector of (hopefully) small Hamming weight, which serves as a possible error. If the vector $\mathbf{u}$ is received, one computes $H\mathbf{u}^T$ and finds $\mathbf{e}$ satisfying $H\mathbf{u}^T = H\mathbf{e}^T$. This means that $\mathbf{u}$ is in the coset $\mathbf{e} + C$ and one assumes that $\mathbf{e}$ is the error vector. Then one assumes the message that was sent was $\mathbf{u} - \mathbf{e}$. Note that $H(\mathbf{u}-\mathbf{e})^T = \mathbf{0}$ so $\mathbf{u}-\mathbf{e}$ must be in the code. One can see immediately that there are many computational difficulties in this scenario. A code that is useful is one that has a high minimum weight (and hence can correct a high number of erroneous entries of a received word) and where there is an efficient algorithm for decoding the received vectors.

Essentially, the code is a k-dimensional subspace of an n-dimensional space over a finite field. The received message is a vector in this n dimensional space and is decoded by finding the closest vector (with respect to the Hamming metric) in the k dimensional code and decoding to that vector. This is further complicated by the fact that there may not be a unique vector that is closest. Not only does this sound like a problem from pure mathematics, it sounds like a classical geometric problem. These types of problems have been studied in Euclidean space for centuries. This problem simply changes the metric and uses a finite field. For example, one can easily see analogues in terms of the sphere packing problem or in terms of uniform distributions.

The main work done in subsequent decades was to come up with codes that had efficient decoding algorithms. That is, a way of describing the code such that there is an efficient algorithm for finding the closest vector. One of the first was the celebrated

Hamming codes [20]. In these codes, the parity check matrix is constructed by using vector representatives of the distinct points of projective space over a finite field as the columns of the matrix. This means that the minimum distance is 3 and that the code meets the sphere packing bound, that is, they are all perfect codes. Then computing $H\mathbf{u}^T$ gives the exact coordinate where the error is made and what the error is. While these codes have many fascinating properties, they were not often used in applications because the minimum distance is small. However, they have been studied extensively in terms of their connections to combinatorics and group theory. For example, the $[7,4,3]$ binary code is intimately related in every imaginable way to the projective plane of order 2, known as the Fano plane.

At about the same time, Golay came up with two other perfect codes, namely a binary $[23,12,7]$ code and a ternary $[11,6,5]$ code. These codes have been intensely studied and they have fascinating connections to groups, lattices, and designs. For example, the binary Golay code is intimately related to the Leech lattice and it produces 5-designs by its vectors of a given weight. Moreover, its automorphism group is the Mathieu group M23. See [6] for a description of these results.

4. Coding Theory Comes to Life

Within the next decade two families of codes were found that were actually highly useful in practice, namely the Reed-Muller codes [32] and the Reed-Solomon codes [33]. These codes were not only shown to have good parameters but efficient decoding techniques were also produced. Both of these codes rely on very clever applications of abstract algebra. The Reed-Muller codes have a wide array of uses in information transfer and have very interesting connections to finite geometry, see [1] for a detailed description of this connection. The Reed-Solomon codes are extensively used in such technologies as compact discs, digital video discs, blue ray discs, and QR codes. Both families of codes have been used in NASA space probes when sending digital information back to earth.

What should be understood about this period in the history of coding theory is that mathematicians and engineers were using classical results from combinatorics, linear algebra, and abstract algebra to produce codes and algorithms associated with these codes. At this early stage it was very much applied mathematics, namely the results of mathematics were used (along with some very clever innovations) to solve practical engineering problems. Codes were not yet being used to answer questions in mathematics (at least not extensively).

As an example of codes being constructed at this time, consider cyclic codes, which were first introduced by Eugene A. Prange in 1957, see [28], [29], [30], and [31]. These papers, despite their importance are exceedingly difficult to find, and are generally not even in the usual mathematical databases. They were technical reports for a United States Air Force project. A cyclic code is a code C such that if $(c_0, c_1, \ldots, c_{n-1}) \in C$ then $(c_{n-1}, c_0, c_1, \ldots, c_{n-2}) \in C$. This family of codes is one of the most well studied families of codes, not only because they are useful but because they have a canonical algebraic description. Specifically, a linear cyclic code corresponds to an ideal in the ring $\mathbb{F}_q[x]/\langle x^n - 1\rangle$, where the vector $(c_0, c_1, \ldots, c_{n-1})$ corresponds to the polynomial $c_0 + c_1x + c_2x^2 + \cdots + c_{n-1}x^{n-1}$. Notice that multiplication by x corresponds to the cyclic shift.

It follows that a complete classification of cyclic codes can be found by factoring the polynomial $x^n - 1$ over the field $\mathbb{F}_q$. If $p(x)$ is a factor, then the ideal $\langle p(x)\rangle$ corresponds to a cyclic code of length n over $\mathbb{F}_q$. One of the reasons that cyclic codes are so widely studied is that polynomial rings are such a well studied object in abstract algebra. In that sense, the machinery necessary to study these codes was already firmly in place in the world of pure mathematics. All that was required was to apply this extensive machinery in the setting of algebraic coding theory. This does not mean that interesting and difficult questions did not arise from this application; they certainly did. But the large machinery of algebra was a great help in building the theory of cyclic codes. For example, finding the ideals when the length was not relatively prime to the characteristic of the field is a difficult algebraic problem.

The ideas used to study cyclic codes have been widely generalized from 1957 to the present day. For example, ideals in $\mathbb{F}_q[x]/\langle x^n+1\rangle$ correspond to codes with the property that

$$(c_0, c_1, \dots, c_{n-1}) \in C$$

implies

$$(-c_{n-1}, c_0, c_1, \dots, c_{n-2}) \in C$$

and are known as negacyclic codes. Ideals in $\mathbb{F}_q[x]/\langle x^n - \lambda\rangle$ correspond to codes with the property that

$$(c_0, c_1, \dots, c_{n-1}) \in C$$

implies

$$(\lambda c_{n-1}, c_0, c_1, \dots, c_{n-2}) \in C$$

and are known as constacyclic codes. Additionally, codes that are ideals in $\mathbb{F}_q[x]/\langle p(x)\rangle$ are known as polycyclic codes. Denoting the cyclic shift by σ, that is

$$\sigma((c_0, c_1, \dots, c_{n-1})) = (c_{n-1}, c_0, c_1, \dots, c_{n-2}),$$

then a code that is held invariant by the action of σ^k is known as a quasi-cyclic code of index k.

Finally, one of the more recent generalizations uses an automorphism θ of the alphabet A. If a linear code has the property that if $(c_0, c_1, ..., c_{n-1})$ is in C then $(\theta(c_{n-1}), \theta(c_0), ..., \theta(c_{n-2}))$ is in C, we say that C is a skew-cyclic code. Numerous references for these codes can be found by looking at one of the standard references for coding theory such as [21], [26], or [34].

4.1. **The MacWilliams Relations.** In the early 1960s, Jessie MacWilliams proved two results that were foundational for the study of coding theory, see [24], [25]. The first theorem states that every linear isometry between linear codes for the Hamming distance can be extended to a linear isometry of the ambient space. The second involves weight enumerators and are known as the MacWilliams relations. We shall describe weight enumerators now. Let C be a code of length n over an alphabet A, then the Hamming weight enumerator of C is defined as $W_C(x,y) = \sum_{\mathbf{c}\in C} x^{n-wt_H(\mathbf{c})} y^{wt_H(\mathbf{c})}$, where $wt_H(\mathbf{c})$ indicates the Hamming weight of the vector $\mathbf{c}$. The weight enumerator is expressed as $W_C(x,y) = \sum A_i x^{n-i} y^i$ where there are A_i vectors of Hamming weight i in C. The MacWilliams relations show that the weight enumerator of the orthogonal code can be determined from the weight enumerator of the code. Specifically, if C is a linear code over the finite field $\mathbb{F}_q$, then $W_{C^\perp}(x,y) = \frac{1}{|C|} W_C(x + (q-1)y, x - y)$. One cannot overestimate the many uses this theorem has in coding theory. For example, if C is a self-dual code, that is $C = C^\perp$, then the weight enumerator is held invariant by the action of the MacWilliams relations and therefore invariant theory can be used to determine the set of all possible weight enumerators for self-dual codes. This result is known as Gleason's Theorem. This would be used extensively in the following years in the application of coding theory to design theory and to lattice theory (see [1],[2],[6],[26]). The MacWilliams relations were one of the earliest and most beautiful theorems in coding theory that were both useful in practical applications and stood alone as beautiful theorems of mathematics. This was a case of new mathematics being developed in coding theory rather than existing mathematics being applied to a problem.

By this I mean that even if there were no applications of codes to the problem of electronic communication, this was still a particularly beautiful and interesting theorem.

The author of these theorems had a particularly interesting story as well. She had studied in England before raising her children and many years later received her Ph.D. from Harvard University. More will be mentioned about her story and accomplishments later in the article.

5. End of the Beginning

In 1970, N. Levinson published "Coding Theory: A Counterexample to G. H. Hardy's Conception of Applied Mathematics" [22]. In this article, Levinson puts forth the idea that Hardy's well known ideas on the distinction between pure and applied mathematics were contradicted by number theory's use in actual applied coding theory. Hardy saw pure mathematics (in his eyes the superior) as useless and should revel in its uselessness. At the apex of this useless but beautiful mathematics was number theory; it was the queen of mathematics and was (at least at that time) considered completely useless in the outside world. What Levinson shows is that results that Hardy saw as useless but wonderful, were used extensively in the design of codes and decoding algorithms. The purest of the pure of mathematics was now used with a very practical purpose. (As an aside, Hardy believed that one of number theory's greatest attributes was that it had no military applications. How disappointed he would be to find out that in the twenty-first century the world's security services were absolutely filled with number theorists working on cryptographic applications.)

At this point, coding theory was solidly an applied mathematics endeavor. Researchers were using known classical mathematics to solve interesting and important questions in electrical engineering and computer science. That is not to say that there were not first-rate mathematicians and first-rate mathematical theorems emerging, but the main focus was solidly on applications.

In 1971, at a workshop on coding theory, Ned Weldon stated: "Too many equations had been generated with too few consequences... Coding theorist professors had begotten more coding theory Ph.D.s in their own image... no one else cared; it was time to see this perversion for what it was. Give up this fantasy and take up a useful occupation... Coding is dead." [42] The author of the present paper was told by people who were present that this conference was known as the "coding theory is dead" conference. The idea behind this comment was that technology was far behind what they could do in theory. Another concern for those present was that mathematicians were getting interested in the central problem of coding theory, which meant that someone was going to give a complete solution to the fundamental problems of the discipline leaving no room for further research. That is, he thought that all of the work being done by coding theorists was not being applied and served no useful purpose. This did not prove to be the case! There were two enormous reasons for this. The first is that the mathematical part of the theory began to explode and find a myriad of interesting paths to take including numerous connections to combinatorics, finite geometry, and number theory. The second was that over the next three decades electronic devices of all kinds were to expand the uses of coding theory greatly. Few in 1970 would have guessed that by the year 2000 most people would have a computer on their desk at work as well as one in their house, nor would they have guessed that cellphones would be carried by virtually every person on the planet (the author of this article still does not have one, but recognizes their universality). This explosion of electronic communication would find many new and interesting applications for coding theory as well as for information theory as a whole. For example, before the dawn of the information age, cryptography was largely the concern of the military, the government, and large financial organizations. In 2024, cryptography is the concern of every person on the planet as it allows for internet commerce. One can hardly overstate the importance of keeping personal and financial information secure in the present day.

In 1973, Delsarte published a paper framing coding theory in very pure terms [7]. In this paper, he studied codes in terms of association schemes. This paper has been referenced numerous times and used to produce interesting results about codes in this setting. The paper was the author's thesis at the Université Catholique de Louvain. In this paper, the author describes an association scheme approach to coding theory. One scheme, the Hamming scheme, is defined using a finite set F with cardinality at least 2, and in the space F^n. Then two points x and y are said to be i-th related if the Hamming distance between them is i. One of the important results in this paper was determining the possible group structures in this Hamming scheme. This result would later be understood more completely in the 1990s leading to an explosion in the study of codes over rings. This paper will be discussed later in detail. From our perspective, the importance of this paper is that the author was examining coding theory as a well described mathematical structure. In essence, coding theory was being considered as pure mathematics with solid foundations and viewing the fundamental objects of coding theory in their own right rather than in service to an application. Just two years after Weldon had incorrectly announced the death of coding theory, Delsarte was putting the mathematical discipline of coding theory on a sound foundation within the field of combinatorics.

6. Coding Theory Emerges as a Full Discipline

One of the biggest events in coding theory, just six years after the pronouncement of its death knell, was the publication of the text "The theory of error-correcting codes" by Jessie MacWilliams and Neil Sloane in 1977. This text became the standard reference for algebraic coding theory for at least the next 30 years. The text was steeped both in the engineering applications and the mathematics that underpinned them. One can hardly overestimate the influence this book had on the subject. It was comprehensive and well written and filled with avenues of future research. As a testament to its importance, checking the standard mathematical databases, the text has been cited thousands of times. The major importance of this work was that it brought the known world of coding theory into one place and set a course for the future of coding theory. It also unified notation and terminology for the discipline and served as the standard reference for works in coding theory for the decades that followed.

In the late 1960s and the 1970s, coding theory began to give results in mathematics, as opposed to being used primarily in applications. For example, in 1969 [2], Assmus and Mattson proved a now celebrated theorem that gave a construction for new 5-designs from extremal self-dual codes. Codes such as the extended Golay code of length 24 could be used to construct 5-designs from the codewords of a given weight. Rather than combinatorics giving constructions for codes, codes were now giving constructions of difficult to produce combinatorial objects. In this way, the results of coding theory were now being used to inform questions in pure mathematics, specifically in the field of combinatorics. There were, in fact, numerous connections between combinatorics and coding theory; see [3], published in 1974, for a taste of canonical connections between the two worlds.

During this time there was an active research group in Cambridge Massachusetts centered around Andrew Gleason (a Harvard professor who had solved Hilbert's fifth problem, had done significant work in breaking enemy codes during the second world war, and has two theorems in coding theory named for him, namely the Gleason-Prange Theorem and Gleason's Theorem, which was mentioned earlier), with members

Ed Assmus, Gene Prange, Vera Pless, John N. Pierce, and Skip Mattson, with frequent visits from Elwyn Berlekamp, Jessie MacWilliams, and Neil Sloane. This group was funded by the United States Air Force and was pivotal in making a wide group of mathematicians interested in coding theory. Moreover, this group began to bring the full force of mathematics to questions in coding theory. Some of the most foundational and beautiful theorems in coding theory arose during this time as mathematicians began building a solid mathematical foundation for coding theory, viewing it as a newly born branch of mathematics.

Unfortunately, this group was disbanded when congress passed new legislation directing that the armed services could only fund research that was directly applicable to practical applications. One of the most interesting things that emerged from this group at this time was a presentation in 1970 given by Ed Assmus on the projective plane of order 10, which was a difficult open problem in finite geometry that was of great interest to many combinatorialists and geometers. This would lead to a major event in coding theory and combinatorics beginning with the paper we describe next.

In 1973, "On the existence of a projective plane of order 10", was published by MacWilliams, Sloane, and Thompson [13]. To give an idea of the level of mathematician who was being attracted to coding theory at this time, we shall give a few of the accomplishments of these authors. Sloane was was the winner of a Lester R. Ford Award in 1978, the Chauvenet Prize in 1979, IEEE Richard W. Hamming Medal in 2005, the Mathematical Association of America David P. Robbins Prize in 2008, and the George Pólya Award in 2013. Despite all of these accomplishments, he is perhaps best known for his creation On-Line Encyclopedia of Integer Sequences. Thompson was awarded the Fields Medal in 1970, the Wolf Prize in 1992, and the Abel Prize in 2008 and proved numerous major results in abstract algebra.

Jessie MacWilliams (mentioned earlier in the article) had a major impact on coding theory and proved one of the foundational results. She received a B.A. from Cambridge in 1938 and an M.A. in 1939 and then moved to the U.S. She raised a family there and later worked at Bell Labs. She completed her Ph.D. in 1962 at Harvard (under the direction of Gleason whose pivotal role was mentioned earlier) where she discovered the MacWilliams relations mentioned earlier. She was also the first Noether Lecturer, and as such gave a talk entitled "A Survey of Coding Theory" in 1980. The accomplishments of these three mathematicians are highlighted just to give an idea of the high quality mathematicians who were being drawn to the discipline at this time. One could also describe the accomplishments of many of the mathematicians that have been cited earlier. The point is that coding theory was being taken seriously by highly able mathematicians from first-rate institutions.

This paper on the projective plane of order 10 was the start of one of the most famous results in which coding theory was able to play a central role. Essentially, one takes a putative projective plane of order 10 and constructs an incidence matrix from its lines and its points. This matrix is used to generate a binary code, which can be extended to a self-dual ($C = C^{\perp}$) $[112, 56, 12]$ code. Using the MacWilliams relations and Gleason's theorem, which is based on this and gives the possible weight enumerators for a self-dual code using invariant theory, the weight enumerator of this putative code can be constructed after determining a few of its parameters with combinatorial (often difficult) arguments.

The existence of the projective plane of order 10 was the first unknown case for finite planes and the problem was often thought to be too difficult for young mathematicians to attempt. In fact, Clement Lam was warned off the problem by his Ph.D. advisor Herbert Ryser as a student at Caltech. Later, after Lam established himself as an accomplished researcher, he took to the problem with full force in the 1980s. He took the following approach. If the weight enumerator of a putative self-dual code formed from the projective plane of order 10 was known, if one could prove the non-existence of such a code, then the plane would not exist. Lam and his team did significant work in reducing what needed to be done to prove its non-existence, such as showing the code had a trivial automorphism group. Following extensive theoretical work they ran a program on a supercomputer for about one year, which showed that no such code existed and hence the non-existence of the projective plane of order 10 was proven. By doing so, they used the machinery developed in coding theory to produce a significant result in pure mathematics. In essence, this result was an example of coding theory giving results in combinatorics rather than combinatorics providing a framework for applicable results in coding theory. This result, together with the proof of the four color theorem, sparked a debate in the mathematical community about whether a computer proof did, in fact, constitute a proof of a theorem.

In a conversation with the author of this article, Lam offered one possible avenue to take in this regard. Namely, we could take a cue from the physical sciences and only accept a computer proof after an independent team verified the computation. Given the amount of work to do this, it seems unlikely that anyone will try to do this for Lam's proof until they have found something that would streamline the computation.

7. Algebraic-Geometry Brings New Ideas

A major advancement that occurred in the 1980s and 1990s was the use of algebraic geometry in coding theory. It has been widely considered that the Varshamov-Gilbert codes were considered best possible codes in terms of optimization. In the early 1980s, V. D. Goppa discovered a broad class of codes arising from algebraic curves over finite fields, see [17], [18]. In 1983, Tsfasman, Vlădut and others showed the existence of Goppa codes better than Varshamov-Gilbert codes for alphabet size $p^2 \geq 49$, where p is a prime in certain cases, see [40] (whose authors received the 1983 Information Theory Society Award).

This was another example of the application of pure mathematics to produce interesting results in coding theory. In this case, it was the gigantic machinery of algebraic geometry. Algebraic geometry certainly had very pure origins in terms of Hardy's definition of pure mathematics. Moreover, the machinery developed in this discipline was absolutely enormous. Mathematicians, who had been applying these ideas to pure questions in number theory, pivoted and began applying these results to questions in coding theory. Of course, Wiles' phenomenal proof of Fermat's Last Theorem sent algebraic geometers in search of a new holy grail. A very large body of results soon followed. While, in overarching philosophy, this was still another branch of mathematics informing questions in coding theory, there were still a vast number of results in algebraic geometry codes that were produced that would certainly be considered pure mathematics in the sense that they were produced for coding theory (not algebraic geometry) but had no real application in the world of electronic communication.

It is interesting to note that these early papers were published in the Soviet Union, in a time when there was still limited exchange of ideas and results between countries in the Soviet block and countries outside of that block, especially in disciplines such as information theory where knowledge of the results could give a militaristic or technological advantage. The opening up of this block and the subsequent fall of the Soviet Union certainly helped spread the use of algebraic geometry to study codes. Perhaps the greatest impact was that numerous mathematicians from this block emigrated to countries in western Europe and North America (or at least visited them for long periods of time) and brought these ideas with them. Certainly, this explosion of the study of coding theory from the viewpoint of algebraic geometry was a very important move in the direction to pure mathematics. For a complete description of this connection and an encyclopedic collection of the results see the book by Tsfasman and Vlădut "Algebraic-geometric codes" [39].

8. Rings Spark a Revolution

The next major move toward pure mathematics was the paper "The $\mathbb{Z}_4$-linearity of Kerdock, Preparata, Goethals, and related codes" [12], which was published in 1994. This paper showed that certain families of binary non-linear codes that nonetheless behaved very much like linear codes are, in fact, images of linear codes over the finite ring $\mathbb{Z}_4$ under the Gray map. That is, they were the images of submodules of $\mathbb{Z}_4^n$ mapped to $\mathbb{F}_2^{2n}$ with the proper map. The Gray map is a non-linear map, which is defined as follows: $0 \to 00, 1 \to 01, 2 \to 11, 3 \to 10$. Note that this map is not the one most mathematicians would think of when mapping $\mathbb{Z}_4$ to $\mathbb{F}_2^2$. That is, usually one would think that 2 would map to 10 and 3 would map to 11. However, this Gray map was the key to showing that these binary codes, which were not linear, were actually simply the image of the quaternary linear codes under this map. This is why these codes behaved like linear codes. That is, their group structure came from their being submodules of $\mathbb{Z}_4^n$ and explained why they seemingly obeyed the MacWilliams relations even though they were not linear codes. It should be noted that an understanding of Delsarte's 1973 paper really should have lead the coding theory community to these results much earlier! While these results were very important in their own right, their impact on the study of codes was even greater. It sparked a massive rush to study codes over finite rings.

There were some previous papers about codes over rings, but it was this paper that really sparked interest in this study. These early papers largely showed some things that were used to study codes over finite fields could also be extended to finite rings. They did not really have an application, either practical or theoretical, that sparked people's interest to continue their study. At first, most of the papers justified the study of codes over rings with an application to binary codes, which would tie the results closely to the applications of coding theory. For example, the first rings to be studied were the commutative rings of order 4. Codes over the finite field $\mathbb{F}_4$ had already been studied and codes over $\mathbb{Z}_4$ were widely studied. Then, numerous papers were written about codes over the ring $\mathbb{F}_2[u]/\langle u^2 \rangle$ and its associated linear Gray map. Finally, codes over the ring $\mathbb{F}_2[v]/\langle v^2 + v \rangle$, which is isomorphic as a ring to $\mathbb{Z}_2 \times \mathbb{Z}_2$, were studied. Codes over these rings were shown to have a canonical connection to lattices in certain spaces. Additionally, motived by the results in Delsarte's 1973 paper, codes were studied over mixed alphabets such as $\mathbb{Z}_4\mathbb{Z}_2$ codes. These were codes that combined the Gray map from the quaternary ring with the identity map from the binary field to construct binary codes. Many interesting and important results were obtained from this viewpoint, see [4] for a complete description of this work.

Next, generalizations of these four rings were studied. For example, some studied codes over the finite fields $\mathbb{F}_{2^r}$, the rings $\mathbb{Z}_{2k}$, $R_k = \mathbb{F}_2[u_1, u_2, \ldots, u_k]/\langle u_i^2, u_iu_j + u_ju_i \rangle$, and $A_k = \mathbb{F}_2[u_1, u_2, \ldots, u_k]/\langle v_i^2 + v_i, v_iv_j + v_jv_i \rangle$. These families of rings are also equipped with corresponding Gray maps to the binary space and are just some of the natural generalizations that were studied very quickly after codes over the finite ring $\mathbb{Z}_4$. More exhaustively, codes were studied over chain rings (rings whose ideals form a chain), local rings (rings with a unique maximal ideal), and then to principal ideal rings. However, the study of these rings was carried out in an essentially ad hoc manner, in that foundational results such as the MacWilliams relations were produced for various families of rings as needed. Foundational results for codes over rings in general were not yet well studied or clearly stated. However, numerous fascinating results for codes over rings were found such as connections to unimodular lattices (see [6] and the massive number of reference therein) and interesting connections to binary codes via Gray maps. While numerous interesting results were found during this time, little thought was given to studying codes over a very broad family of rings. Rather, it was particular applications that fuelled the research.

Throughout the 1990s numerous papers were written on codes over various families of rings and numerous connections were found to number theoretic structures, but still quite often these papers were motivated (at least they were stated as such, if not in reality) by applications in the field of electronic communication. Additionally, old ideas were resurrected because of advances in computing. For example, in 1962 Gallagher wrote a paper [15] on Low Density Parity Check (LDPC) codes. Essentially, these were codes whose parity check matrix had few coordinates containing a non-zero element. Very little was done with these codes in the ensuing years.

In the 1990s and the decades that followed, an explosion of results on these codes appeared. Researchers noticed that these codes could use probabilistic methods, such as belief propagation, for decoding. This gave decoding algorithms of complexity linear in the length of the code. If every coding theorist had a very good computer on their desk in the 1960s, then this would have been noticed decades earlier. By the time of the writing of this article hundreds of papers have been written on this topic. Many techniques from graph theory, algebra, and finite geometry were used to construct these codes and began what is often referred to as modern coding theory to distinguish it from classical coding theory.

9. The Move to Purity

By the 1990s, mathematicians were studying codes in their own right for purely mathematical purposes, but this was still often couched in terms of possible applications, either in engineering or in other branches of mathematics such as combinatorics or number theory. This began to change significantly in this decade. Jay Wood spent the 1989 - 1990 academic year at Lehigh University (during this time he taught the author of this paper algebraic topology) and had numerous productive conversations with E. F. Assmus on coding theory. Recall that Assmus had been part of Gleason's team decades earlier. Assmus certainly viewed coding theory as pure mathematics (at least the part where his interests were) and was largely concerned with studying codes in relation to combinatorics and finite geometry. It was at this time that he wrote a text with Jenny Key on the relationship between codes and designs [1]. Later in the decade, Vera Pless suggested to Wood that it was time to reconsider the MacWilliams Theorems, given the new directions in coding theory. These conversations prompted Wood to write the paper "Duality for modules over finite rings and applications to coding theory" [41], published in 1999. In this paper, he showed that the largest class of rings for which both MacWilliams theorems held was the class of Frobenius rings. It should be noted that, if you were to ask one hundred good coding theorists at the time for a definition of a Frobenius ring, you probably would have received zero correct answers. Asking the same question today to the same group, there would be a marked increase in the number who give the correct answer.

Specifically, he showed the following results.

- If R is a finite Frobenius ring and C is a linear code, then every Hamming isometry $C \to R^n$ can be extended to a monomial transformation.
- If a finite commutative ring R satisfies that all of its Hamming isometries between linear codes allow for monomial extensions, then R is a Frobenius ring.

By an example of Greferath and Schmidt, [19], it was shown that these results do not extend to quasi-Frobenius rings. Therefore, Frobenius rings are the largest class of rings for which the first MacWilliams Theorem hold.

The next result generalizes the MacWilliams relations which we will state in a very general form, that is for the complete weight enumerator rather than just the Hamming weight enumerator. We require some definitions to state it. Let R be a finite ring with r elements and define $\iota : R \to \{0, 1, 2, 3 \ldots, r-1\}$, where the elements of R are $a_0, a_1, \ldots, a_{r-1}$ and $\iota(a_i) = i$. Define the complete weight enumerator of a code C over R as

$$cwe_C(x_0, x_1, \ldots, x_{r-1}) = \sum_{\mathbf{c} \in C} \prod_{i=1}^{n} x_{\iota(c_i)}.$$

Then, if $T_{a,b} = \chi(ab)$ where χ is a generating character for $\widehat{R}$, for a linear code C over a finite commutative Frobenius ring R, we have

$$cwe_{C^\perp}(x_0, x_1, \ldots, x_{r-1}) = \frac{1}{|C|} cwe_C(T \cdot (x_0, x_1, \ldots, x_{r-1})).$$

As a corollary, we get the MacWilliams relations for the Hamming weight enumerator.

$$W_{C^\perp}(x, y) = \frac{1}{|C|} W_C(x + (r-1)y, x - y).$$

What these results showed was that many of the foundational techniques of codes over finite fields could be applied in the case where the alphabet is a finite Frobenius ring. For example, when the ring is commutative and the code C is linear, we have $|C||C^\perp| = |R|^n$ and $(C^\perp)^\perp = C$. When the ring is non-commutative you must define orthogonals on the left and the right, then similar results are true depending on whether the code is left linear or right linear.

This paper then sparked an intense interest in codes over Frobenius rings and a flood of papers followed investigating what possible results could be obtained in this new path.

9.1. **Questions and Debates.** At the AMS Special Topic Session at Notre Dame University in April, 2000, a talk was given on codes over Frobenius rings (the author does not recall who was giving the talk). Vera Pless, who was a very important coding theorist (also a member of Gleason's team described earlier), casually raised her hand at the end of the talk and asked "Why should we care about codes over Frobenius rings anyway?" Her question was seeking to find motivation for the study of codes over Frobenius rings. Namely, was there a reason for going down this path. It must be noted that by this time Wood's paper was not widely known. While the author does not remember the answer given, it is certain that Vera Pless was far from satisfied with it. Pless had voiced a question that many were considering at the time. Namely, is it interesting to make such broad general definitions – are we still actually doing coding theory or are we doing generalizations for the sake of generalization?

Years later, at the AMS special session honoring the retirement of Than Ward (another mathematician who wrote numerous important papers in coding theory) at DePaul University, Chicago, October 6, 2007, the author of this article gave a talk about codes over rings with Vera Pless in the first row. The talk began recalling the Pless quote from seven years earlier. Pless then responded, loud enough for everyone to hear, "Why does everyone remember everything I say?"

The talk continued giving reasons for why we should be studying codes over Frobenius rings. The first reason is that we have the two foundational MacWilliams Theorems. There are numerous implications of these theorems in the classical case. It becomes natural to investigate what these implications are in the more general case. The second reason is that combinatorial bounds such as the Singleton and Sphere-packing bounds mentioned earlier still apply in this case. Moreover, there are analogues for the algebraic bounds based on the types of rings. Additionally, some of the connections to other branches of mathematics were even better than in the classical case. For example, self-dual codes over rings have a much more natural connection to unimodular lattices than codes over fields do; there is no binary code that can produce the extremal unimodular lattice of length 72, but there is a self-dual code over $\mathbb{Z}_4$ that can produce it. Moreover, infinitely many lattices can be produced by self-dual codes over $\mathbb{Z}_{2k}$ that cannot be produced from codes over fields. Moreover, connections to lattices over various other infinite fields were found from codes over rings. Additionally, studying codes over Frobenius rings opened up a flood gate of applications to other algebraic questions. Finally, the results that were being obtained were, in fact, beautiful mathematics. They were natural, interesting, and highly non-trivial. At the end of the talk, the moderator asked for questions, then he said that he had a question but not for the speaker, but rather for Vera Pless. He asked her if she was now convinced that we should be studying codes over Frobenius rings and she wholeheartedly agreed that we should!

Essentially, if we have the foundational results in such a broad setting, it is quite natural to study these objects to determine what can be said about them. What has happened in these past 25 years is that mathematicians began to study codes as an interesting mathematical object in themselves. Like any objects in pure mathematics, practical applications may be found later for these results, but the drive to study these objects no longer came solely from a particular application.

As Alexander Barg said at an AMS conference at the University of Cincinnati in October 2006: "We do not have to pretend that what we are doing has anything to do with information transfer any more." At this point, codes are algebraic objects just like groups, rings, and fields and should be studied for their own sake whether or not they had an application in engineering or another branch of mathematics. In 2017 the text "Algebraic Coding Theory over Finite Commutative Rings" was published by the author of this paper. This text gives many of the foundational results of codes over rings. The author in no way would compare this book to the other major works described in this article, but mentions it because it is a high level book about coding theory that does not mention any applications at all. The book treats coding theory as a branch of algebra and gives no motivation from any applications. By this time, this approach was perfectly natural.

Within the time between these conferences and the present day, there has been a flood of research done on codes over rings and their applications in algebra and combinatorics. There have been so many written that some journals have had to restrict the number of coding theory papers that they are willing to accept for fear of being overwhelmed by them and losing their original desired focus whether algebraic or combinatorial. Likewise, engineering journals have put restrictions on coding theory papers as well, demanding that the papers they publish should have an immediate application that was the focus of the paper. Their fear was that their engineering journal was quickly becoming a journal of pure mathematics.

10. New Avenues from New Applications

During this time, coding theory was given another avenue of pursuit via an important engineering application. As physicists were rushing headlong into the quantum world, questions arose as to how errors in quantum communication could be detected. In this application, linear codes were not the codes that were interesting. Rather, it was additive codes (codes closed under addition but possibly not under scalar multiplication) that were useful and instead of the standard Euclidean inner-product, different inner-products were used. See [5] for a complete description. When studying additive codes, it was also shown that a variety of inner-products could be used coming from the character group of the underlying additive group. In this way, one can think of a code over a group rather than over a ring. This idea sparked a great deal of research in loosening the algebraic conditions of the alphabet. Namely, a great deal of research was put forth looking at codes that were additive over some group (possible the additive group of a field or a ring). It can be shown that MacWilliams relations hold in this case in a very broad sense as well; see [9] for a complete description of the MacWilliams relations in this case.

Another new idea came to coding theory around this time as well, namely DNA codes. It is well known, and incredibly important scientifically especially in biology, that DNA contains a genetic program for the development of life. It consists of two strands, which are linked by the Watson-Crick pairing. Essentially, DNA is a sequence of information with an alphabet of A,C,G, and T. As such, it is interesting to study this information from the point of view of coding theory, namely as a code over an alphabet of size 4.

Unlike the quantum case, there does not seem to be a canonical connection to one of the rings of order 4, but rather any ring of order 4 can give results in this setting. Interestingly, at this point, it is not uncommon to hear geneticists talking about Hamming distance when they are talking about DNA.

From the point of view of this article, the interesting thing here is that scientists took coding theory as a body of pure mathematics, and then applied it to a scientific situation. In essence, this is what is at the heart of mathematics, scientists can take an already developed, abstract, body of results and apply them to questions in their own discipline.

As a branch of pure mathematics, coding theory can now be viewed in the following way. A code is a subset of A^n where A is a set with an associated metric. In this setting, the questions of coding theory are largely combinatorial (for example the connection between MDS codes and mutually orthogonal Latin squares). We then consider A to have some algebraic structure. In its most general form we assume A is a finite commutative group and linear codes are subgroups of the ambient space. Attached to the ambient space is a function that acts like an inner-product, which defines an orthogonal code. The MacWilliams relations hold for weight enumerators in this setting and we have the double annihilator condition $(C^\perp)^\perp = C$ and the cardinality condition that $|C||C^\perp| = |A|^n$.

Restricting the alphabet, we can make A a finite Frobenius ring (either commutative or non-commutative). Then, with an associated inner-product, the MacWilliams relations, the double-annihilator condition, and the cardinality condition hold. Within this framework, we have an algebraic structure, a metric, and a notion of duality. The essential question then becomes what is the largest code one can construct for a given length with a given minimum distance under the metric. This is certainly a question of pure mathematics and can be stated in a very general abstract manner. Given this setting, various types of codes can be studied, for example codes equal to their duals, codes contained in their orthogonal, codes held invariant by the action of a group, codes meeting a bound, and a host of others. It is then possible that these objects can have a variety of applications both within mathematics and outside of mathematics, which will depend on the choice of alphabet, metric, and inner-product.

11. Conclusion

As it is now, coding theory is the name for two distinct things. The first is a branch of engineering that has applications in electronic communication, information retrieval and storage, quantum computing, cryptographic applications, secret sharing, and a host of other applications. Given the explosion of computer innovations in the past 40 years, each new innovation seems to bring with it a new use for the techniques developed in coding theory. Secondly, coding theory is a branch of pure mathematics. One might think of this as a three petaled flower. The first petal is the connection between codes and topics in combinatorics such as mutually orthogonal latin squares, finite planes, orthogonal arrays, and t-designs. The second petal is number-theoretic, with the fascinating connection between codes and lattices, forms, and the geometry of numbers. The third petal is a branch of abstract algebra that shares concepts with group theory, ring theory, field theory, module theory, and linear algebra in its broadest definition. These three flowers share a common center, which is the classical theory of codes. While the three petals can seem distinct, results in one petal can sometimes be reflected in results in one or both of the other petals. These petals are still very highly connected.

Many of the results in the pure mathematical part of coding theory still have applications in the vast array of applications in the engineering world of codes. However, there are numerous results that would make Hardy laugh with glee at their utter uselessness in the outside world. These are results which, at present, are so removed from any application that no engineer would find any interest in them at all. However, if the history of the discipline has taught us anything, it may only be a matter of time before they find application in some unlikely location.

There is also a strong bridge between these worlds. New applications bring new questions into the pure branch of coding theory. For example, the rush to build quantum technology has provided numerous questions for coding theorists, which has brought them into dialog with theoretical physicists as well.

In a department talk at Lehigh University in 1991, Ed Assmus began his talk on coding theory with a statement that read: "The purpose of applied mathematics is to enrich pure mathematics". The statement caused a great amount of good natured boos and cheers. From his perspective, the applications of coding were important because they enriched pure mathematics. This deliberately provocative statement might not have the complete support of the author of this present work, but he is certainly grateful that these applications were able to spark such interesting and compelling pure mathematics. From the point of view of the author, coding theory is a paradigmatic example of the healthy relationship between pure and applied mathematics in which both benefit highly from the other and spark interesting avenues of research in both.

References

[1] E.F. Assmus, J.D. Key, Designs and their codes, Cambridge Tracts in Mathematics, **103**, Cambridge: Cambridge University Press. x, 352 p., 1992.

[2] E.F. Assmus, H.F. Mattson, New 5-designs, J. Comb. Theory, **6**, 122-151, 1969.

[3] E.F. Assmus, H.F. Mattson, Coding and combinatorics, SIAM Rev., **16**, 349-388, 1974.

[4] J. Borges, C. Fernández-Córdoba, J. Pujol, J. Rifà, M. Villanueva, $\mathbb{Z}_4\mathbb{Z}_2$-linear codes, Cham: Springer (ISBN 978-3-031-05440-2/hbk; 978-3-031-05443-3/pbk; 978-3-031-05441-9/ebook). xii, 245 p., 2022.

[5] A.R. Calderbank, E.M. Rains, P.W. Shor, N.J.A. Sloane, Quantum error correction via codes over $GF(4)$, IEEE Trans. Inf. Theory 44, No. 4, 1369-1387, 1998.

[6] J.H. Conway, N.J.A. Sloane, [E. Bannai, R.E. Borcherds, J. Leech, S.P. Norton, A.M. Odlyzko, R.A. Parker, L. Queen, B.B. Venkov] Sphere packings, lattices and groups. With additional contributions by E. Bannai, R. E. Borcherds, J. Leech, S. P. Norton, A. M. Odlyzko, R. A. Parker, L. Queen

and B. B. Venkov. 3rd ed. Grundlehren der Mathematischen Wissenschaften. 290. New York, NY: Springer. lxxiv, 703 p., 1999.

[7] P. Delsarte, An algebraic approach to the association schemes of coding theory, Philips Research Reports. Supplements **10**, Ann Arbor, MI: Historical Jrl. vi, 1973.

[8] S.T. Dougherty, Algebraic Coding Theory over Finite Commutative Rings, Springer Briefs in Mathematics. Springer, 2017.

[9] S.T. Dougherty, Dualities for Codes over Finite Abelian Groups, Advance in Mathematics of Communication, Volume 18, Issue 6, 1827-1841, 2024, Doi: 10.3934/amc.2023023, 2023.

[10] L. Euler, Commentarii Academiae Scientarum Imperialis Petropolitanae, 8, 128-140, 1736.

[11] L. Euler, Recherches sur une nouvelle espèce des quarrés magiques, Leonardi Euleri Opera Omina Ser. I, Vol 7, 291-392, 1923, Tuebner, Berlin-Leipzig.

[12] A. R. Hammons, P.V. Kumar, A.R. Calderbank, N.J.A. Sloane, P. Solé, The $\mathbb{Z}_4$-linearity of Kerdock, Preparata, Goethals, and related codes, IEEE Trans. Inf. Theory, **40**, no. 2, 301-319, 1994.

[13] F.J. MacWilliams, N.J.A. Sloane, J.G. Thompson, On the existence of a projective plane of order 10, J. Comb. Theory, Ser. A 14, 66-78, 1973.

[14] C.W.H. Lam, L. Thiel, S. Swiercz, The non-existence of finite projective planes of order 10. Can. J. Math. 41, No. 6, 1117-1123, 1989.

[15] R.G. Gallager, Low-density parity-check codes. IRE Trans. Inform. Theory IT, **8**, 21-28, 1962.

[16] M.J.E. Golay, Notes on Digital Coding, Proc. IRE. 37: 657, 1949.

[17] V.D. Goppa, Algebraic-geometric codes, Math. USSR, Izv. 21, 75-91, 1983; translation from Izv. Akad. Nauk SSSR, Ser. Mat. 46, 762-781, 1982.

[18] V.D. Goppa, Codes on algebraic curves, Sov. Math., Dokl. 24, 170-172, 1981; translation from Dokl. Akad. Nauk SSSR 259, 1289-1290, 1981.

[19] M. Greferath, S.E. Schmidt, Finite-ring combinatorics and MacWilliams equivalence theorem, J. Combin. Theory A, **92**, 17-28, 2000.

[20] R.W. Hamming, Error detecting and error correcting codes, Bell Syst. Tech. J., **29**, no. 2, 147-160, 1950.

[21] Huffman, W. Cary; Pless, Vera Fundamentals of error-correcting codes. Cambridge: Cambridge University Press (ISBN 0-521-78280-5/hbk). xvii, 646 p. (2003).

[22] N. Levinson, N., Coding Theory: A Counterexample to G. H. HardyÕs Conception of Applied Mathematics. The American Mathematical Monthly, 77(3), 249-258, 1970, `https://doi.org/10.1080/00029890.1970.11992464`.

[23] G. Leibniz, Nova Methodus pro Maximis et Minimis". Acta Eruditorum 3: 467Ð473, 1684.

[24] F.J. MacWilliams, Combinatorial Problems of Elementary Group Theory, Ph.D. thesis, Harvard University, 1961.

[25] F.J. MacWilliams, A theorem on the distribution of weights in a systematic code, Bell System Tech. J., **42**, 79 - 94, 1963.

[26] F.J. MacWilliams, N.J.A. Sloane, The theory of error-correcting codes. Parts I, II. North-Holland Mathematical Library. Vol. 16. Amsterdam-New York-Oxford: North-Holland Publishing Company. Part I: xv, 369, 1977.

[27] I. Newton, Philosophae Naturalis Principia Mathematica, 1687.

[28] E. Prange, Cyclic error correcting codes, TN-57-103, 1957.

[29] E. Prange, Some cyclic error-correcting codes withs simple decoding algorithms, TN-58-156, 1958.

[30] E. Prange, The use of code equivalence in the analysis of decoding group codes, TN-59-164, 1959.

[31] E. Prange, An alogrism for factoring $x^n - 1$ over a finite field. TN-59-164, 1959.

[32] I.S. Reed, A class of multiple-error-correcting codes and the decoding scheme, Transactions of the IRE Professional Group on Information Theory, **4**, no. 4, 38-49, 1954, doi:10.1109/tit.1954.1057465.

[33] I.S. Reed, G. Solomon, Polynomial Codes over Certain Finite Fields, Journal of the Society for Industrial and Applied Mathematics, **8**, no. 2, 300-304, 1960, doi:10.1137/0108018.

[34] V.S. Pless, V. S., W.C. Huffman, W. C., Handbook of coding theory. Vol. 1. Part 1: Algebraic coding. Vol. 2. Part 2: Connections, Part 3: Applications. Amsterdam: Elsevier., 1998.

[35] B. Segre, Ovals in a finite projective plane, Can. J. Math. 7, 414-416, 1955.

[36] C.E. Shannon, A mathematical theory of communication, Bell Syst. Tech. J. 27, 379-423, 623-656, 1948.

[37] C.E. Shannon, Communication in the Presence of Noise, in Proceedings of the IRE, **37**, no. 1, 10-21, Jan. 1949, doi: 10.1109/JRPROC.1949.232969.

[38] C.E. Shannon, Communication theory of secrecy systems, Bell Syst. Tech. J., **28**, 656-715, 1949.

[39] M.A. Tsfasman, S.G. Vlădut, Algebraic-geometric codes. Transl. from the Russian, Mathematics and Its Applications, Soviet Series, 58. Dordrecht etc.: Kluwer Academic Publishers. xxiv, 1991.

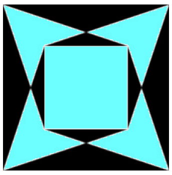
[40] M.A. Tsfasman; S.G. Vlǎdut, Th. Zink, Modular curves, Shimura curves, and Goppa codes, better than Varshamov-Gilbert bound, Math. Nachrichten, **109**, 21-28, 1982.

[41] J. Wood, Duality for modules over finite rings and applications to coding theory, Amer. J. Math., **121**, no. 3, 555 - 575, 1999.

[42] N. Weldon, Comment made at the first IEEE Communications Theory Workshop, St. Petersburg, 1970.

Steven T. Dougherty is a Professor of Mathematics at the University of Scranton, Pennsylvania. He is the author of two books and over 140 academic papers in information theory, number theory, combinatorics, abstract algebra, and the history of mathematics. He was awarded the 2005 Hasse prize by the Mathematical Association of America for a paper in game theory.

(Steven T. Dougherty) University of Scranton, Scranton PA, USA
E-mail address: prof.steven.dougherty@gmail.com



Irish Math. Soc. Bulletin
Number 95, Summer 2025, 23– 34
ISSN 0791-5578

Computing $\sqrt{2}$ with FRACTRAN

KHUSHI KAUSHIK, TOMMY MURPHY AND DAVID WEED

ABSTRACT. The FRACTRAN programs $\sqrt{2}$GAME and NR$\sqrt{2}$GAME are presented, both of which compute the decimal expansion of $\sqrt{2}$. Our $\sqrt{2}$GAME is analogous to Conway's PIGAME program. In fact, our proof carries over to PIGAME to produce a simpler proof of Conway's theorem as well as highlight how the efficiency of the program can be improved. NR$\sqrt{2}$GAME encodes the canonical example of the Newton–Raphson method in FRACTRAN.

1. INTRODUCTION

FRACTRAN is a Turing complete esoteric programming language with several notable features (c.f. [4], [5]). It is simple to understand how the language works. One can code any standard mathematical algorithm in FRACTRAN, and moreover the Gödel number of any program is straightforward to explicitly compute. Conway developed this language in [2], and used it to formalize examples proving that natural generalizations of the famed Collatz conjecture are undecidable [3]. He produced several explicit examples of algorithms in FRACTRAN in [2]. Two examples are PRIMEGAME, which computes, in order, every prime number, and PIGAME, which generates, in order, the digits of the decimal expansion of π. In fact PIGAME ties in with a classical and fundamental question at the intersection of real analysis and theoretical computer science; namely how to compute the decimal expansion of a computable irrational number. Turing defined the computable numbers as the real numbers whose decimal expansions can be computed algorithmically (i.e. with a Turing machine), and they play a central role in the work of both Turing and Gödel. For a fascinating and readable account of this theory, the interested reader is referred to the first two chapters of [6]. Although this book was written in 1989, Penrose expressed prescient thoughts on the role computers and A.I. will play in mathematical research which are extremely relevant today.

As Conway himself states, the proof that PIGAME actually works is nontrivial. It involves using some heavy machinery (e.g. Mähler's famed irrationality measure for π) together with Wallis' infinite product formula for $\frac{\pi}{2}$ to ensure that truncating this infinite product after a certain even number $E \geq 4 \times 2^{10^n}$ terms is sufficiently accurate to compute the n-th digit of π. One initial motivation for this work was to actually explain what Conway does, as many details are omitted. The first main theorem of this paper ($\sqrt{2}$GAME) then computes, in order, the decimal expansion of $\sqrt{2}$ via Catalan's [1] infinite product expansion of $\sqrt{2}$. The mechanics of proof are largely analogous to Conway's, however we find a simpler proof that our truncated approximation is sufficiently accurate to compute. This simpler proof also carries over to PIGAME: one then sees *a posteriori* that a simpler and faster program could be written to compute the decimal expansion of π.

2010 *Mathematics Subject Classification.* 68Q04.
Key words and phrases. FRACTRAN, decimal expansions.
Received on 02-04-2025; revised 10-07-2025.
DOI: 10.33232/BIMS.0095.23.34.

K.K acknowledges support from the LSAMP grant at CSUF. K.K. and D.W were supported with a summer undergraduate research grant in 2023 by the Department of Mathematics at CSU Fullerton. K.K. also thanks the Undergraduate Research Opportunity Center, CSU Fullerton, for travel support. The authors thank Aaron Cottle for helpful comments. We also thank the referee for helping us to improve the paper with several insightful comments.

There are of course several extremely efficient ways to compute the decimal expansion of $\sqrt{2}$, or for that matter π. The most standard, familiar to generations of calculus students, is the Newton–Raphson method. Our second theorem presents NR$\sqrt{2}$GAME, which computes the n-th digit of $\sqrt{2}$ via this standard algorithm.

We wish to emphasize that all our programs are useless in practice: there are much quicker programs to compute the decimal expansion of a given computable number and this is a whole field of research. Even to compute the number E is extremely time consuming as it is double exponential as a function of n. Why then should you care about FRACTRAN? To our knowledge, it is the simplest way to convert an explicit algorithm (i.e. the rules of a Turing machine) into a genuine program in a language. Additionally the language makes the interplay between the state the machine is in (the register) and the commands of the program very clear and easy to follow. As such FRACTRAN is an excellent educational aid which highlights how simple mathematical computation (the code only involves multiplying rational numbers together) is powerful enough to describe every Turing machine. Another very good reason to study FRACTRAN is that Conway *explicitly* produces in [2] a universal Turing machine in this language. In other words, he produces a short list of fractions, and every single computer program can be described by choosing one natural number (the Gödel number of this program, or what Conway calls the catalog number) and running this fixed FRACTRAN program with that input. Finally, Penrose comments ([6], Chapter 2) that computing the decimal expansion of a computable irrational number is precisely the sort of model algorithm one should be able to generate to truly understand a programming language. He lists π and $\sqrt{2}$ as the two canonical examples of such numbers, which motivates generalizing PIGAME to $\sqrt{2}$GAME as a natural problem.

2. Rules of the game

2.1. **Initial Comments.** Turing Machines model the action of a computer. The main parts of a Turing machine are a way to store data, originally (abstractly) thought of as an infinitely long tape, and a set of rules that allow the conditional change of that data. The starting state of the tape is thought of as the input of the code, and the resulting state is the output. Different programs are then made by changing the rules. In FRACTRAN, the entirety of the data is stored in a finite set of fractions (the program) and a single integer (the register). Via the Fundamental Theorem of Arithmetic, each integer $n \in \mathbb{N}$ admits a unique prime decomposition $n = \prod_{i=1}^{k} p_i^{\alpha_i}$. Conway's simple idea is to encode a Turing machine starting with a number N so that each power in its prime decomposition gives the state the Turing machine is in. Each power of the prime appearing in N tells us the initial state of our system: it tells us what is in each register. Now multiply N by a fraction f_i so that $f_i N$ is also a whole number: if we take the prime factor decomposition of the numerator and denominator of f_i, we have that $f_i N \in \mathbb{N}$ if, and only if, the powers appearing in the prime decomposition of N have been redistributed. Included in this statement is the possibility that the primes with 0 in their register will initially become non-empty. This exactly models the mechanisms of a Turing machine and is the basic idea underlying FRACTRAN. More formally, we need an initial state (a stored number) $N \in \mathbb{N}$ which is in our *register* and a fixed list of fractions $\{f_1, f_2, \ldots, f_n\}$. Compute $f_i N$, with $i = 1, 2, \ldots, n$, until we reach the first instance where $f_j N \in \mathbb{N}$, $j \in \{1, 2, \ldots, n\}$. Then change the register to $f_j N$ and iterate. In practice, Conway thinks of FRACTRAN as a flow chart that proceeds from one node to another. To indicate where to go, the nodes are connected by arrows with a well-defined notational hierarchy as follows:

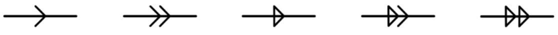


FIGURE 1. Hierarchy of arrows

These arrows are listed in hierarchical order of precedence, read from left to right. These arrows are then labeled with fractions, which tell us how to update the register. There is a well-understood algorithm to convert this flow chart into a list of fractions [2]. We will explain this in due course, and in the appendix a Python code for this algorithm is presented. We will also dwell a little on how to understand the hierarchy of arrows as we explain PIGAME. We present the simplest example to begin.

Example 2.1. Let us write a program to add two given whole numbers, say a and b. Store these numbers in our initial register as $N = 2^a 3^b$. Then build a single loop labeled with $2/3$.

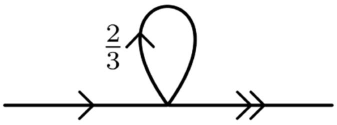


FIGURE 2. A flow chart for addition

Every time we go around the loop, we multiply N by $\frac{2}{3}$. It is easy to see this game ends with output 2^{a+b}. The FRACTRAN code is easy to derive in this example: $N = 2^a 3^b$ is our initial state, and $\{\frac{2}{3}\}$ is our list of fractions.

3. CONWAY'S PIGAME

Theorem 3.1. *(PIGAME* [2]*) When started at $2^n \cdot 89$, the FRACTRAN code*

$$\frac{365}{46}\ \frac{29}{161}\ \frac{79}{575}\ \frac{679}{451}\ \frac{3159}{413}\ \frac{83}{407}\ \frac{473}{371}\ \frac{638}{355}\ \frac{434}{335}\ \frac{89}{235}\ \frac{17}{209}\ \frac{79}{122}\ \frac{31}{183}\ \frac{41}{115}\ \frac{517}{89}\ \frac{111}{83}\ \frac{305}{79}\ \frac{23}{73}\ \frac{73}{71}$$

$$\frac{61}{67}\ \frac{37}{61}\ \frac{19}{59}\ \frac{89}{57}\ \frac{41}{53}\ \frac{833}{47}\ \frac{53}{43}\ \frac{86}{41}\ \frac{13}{38}\ \frac{23}{37}\ \frac{67}{31}\ \frac{71}{29}\ \frac{83}{19}\ \frac{475}{17}\ \frac{59}{13}\ \frac{41}{291}\ \frac{1}{7}\ \frac{1}{11}\ \frac{1}{1024}$$

will terminate at $2^{\pi(n)}$, where $\pi(n)$ is the n-th digit in the decimal expansion of π.

The first order of business is to show how this list of fractions is generated via Conway's algorithm from the following flow chart:

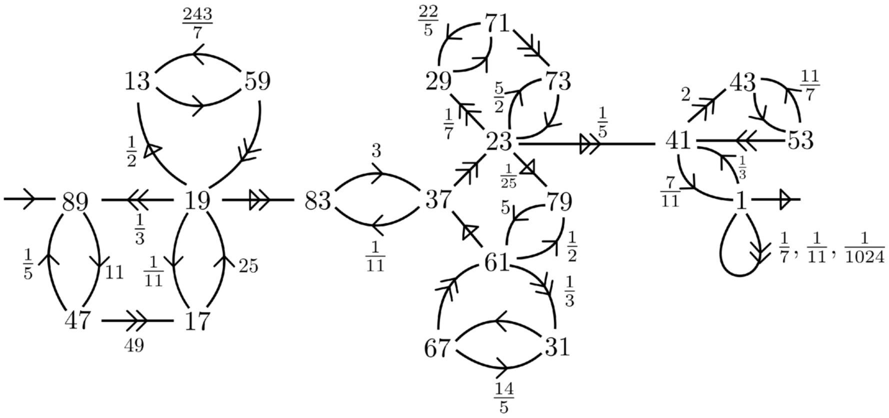


FIGURE 3. The flow chart for PIGAME

Notice that you can identify which part of the flow chart a given fraction corresponds to by looking at the prime decomposition of the numerator and denominator. For instance, the fraction $41/115$ corresponds to moving from node 23 to node 41. We start at node 23, meaning the register N has exactly one copy of 23 in its prime decomposition. For a given prime p, Conway defines r_p as the power of p in the prime decomposition of the register N, so here $r_{23} = 1$. Since $115 = 23 \times 5$, multiplying $(41N)/115$ clears 23 from the register (so $r_{23} = 0$) and puts 41 in its place, since after the multiplication N has updated to have $r_{41} = 1$. As we move from the 23 cell/node to the 41 one, the program tells us to adjust N by reducing r_5 by 1. In full generality, if one goes from a node labelled p to a node labelled q and the program requires us to update N by multiplying by the fraction M_1/M_2, the resulting fraction in our code is $\frac{M_1 q}{M_2 p}$. To make this all work smoothly, it is important to have different primes corresponding to the nodes and the actual program.

The arrow which we are discussing in the flow chart is third in the hierarchy of Figure 1. The arrow going to node 73 ranks first, and the arrow going to node 79 is second. Hence, the corresponding fractions (namely $365/46$ and $79/575$) must come before $41/115$ in the code. Note that when the machine is at the 23 node, all other fractions in the code will not adjust the register as $f_i N \in \mathbb{N}$ if, and only if, 23 is in the denominator of the fraction f_i. So they do not play a role at all when we are at this stage. However, we have to list these three fractions corresponding to the 23 node in the order mandated by the arrows. This means we want to always go to 73 node first until that will violate the rules of FRACTRAN. In particular, every time we go to the 73 node, r_2 will decrease by 1 and r_5 will increase by 1. This stops when $r_2 = 0$, because if $r_2 = 0$, multiplying N by $5/2$ will not be a whole number, and analogously for all later arrows.

Remark 3.2. Conway has an unwritten convention of arranging the fractions in his code in order of decreasing denominators. There have to be some exceptions to this depending on the code. We have just discussed how the fraction $41/115$ corresponds to the arrow moving from node 23 to node 41; but all other arrows emanating from node 23 come before this arrow in the hierarchy and so their corresponding fractions must come before $41/115$ in the code. That is why, for instance, $365/46$ is located as the first fraction despite 46 being a small denominator in the list.

Remark 3.3. There is a small bug in Conway's code, known to experts, where he incorrectly states the code starts at 2^n. A corrected statement is presented here.

4. The proof of PIGAME: setup

Since the proof of Theorem A is based on PIGAME, and his proof that the algorithm actually works is short on details, it is natural first to discuss the proof and fill in some of the steps. For $n \in \mathbb{N}$, the claim is that running PIGAME will compute the n-th decimal digit of π. The flow chart breaks into three phases.

Phase 1 From node 89 to node 83, the program computes E, an even number $\geq 4 \times 2^{10^n}$.

Phase 2 From node 83 to node 41, the program computes

$$10^n N_E = 10^n 2E(E-2)^2 \dots 4^2 2^2, \text{ and}$$
$$D_E = (E-1)^2 (E-3)^2 \dots 3^2 1^2.$$

Phase 3 The program computes the integer part of $\frac{10^n N_E}{D_E}$ and reduces it modulo 10.

The mechanism of these phases are all fully explained in [2]. The number computed in Phase 3 is the n-th term in the decimal expansion of

$$\pi_E = \frac{N_E}{D_E} = \frac{2E(E-2)^2 \dots 4^2 2^2}{(E-1)^2(E-3)^2 \dots 3^2 1^2}.$$

Multiplying the numerator of π_E by 10^n shifts the decimal unit of π_E exactly n places to the right. Taking the floor function turns this into an integer, and reducing mod 10 allows us to find the n-th term in the decimal expansion of π_E. To complete the proof, one has to compute explicitly how close π_E is to π. Another issue to bear in mind comes from the well-known fact that two numbers can be very close together but have differing decimal expansions due to the identification $1 = 0.99\dot{9}$.

So, to show the program actually works, it remains to prove that the n-th decimal digit of π and π_E agree. To this end, Conway states without proof that

$$|\pi - \pi_E| < \frac{\pi}{E} \tag{1}$$

Then $|\pi - \pi_E| < \frac{\pi}{E} < 10^{-n}$, meaning π and π_E agree to n decimal places unless one of them has a decimal expansion containing only zeros from the n-th decimal place onwards (where we make the usual identification $1 = 0.99\dot{9}$). The proof thus reduces to two key steps; (i) establish Equation (1), and (ii) show that $10^n \pi_E$ cannot be an integer.

5. Establishing Equation (1)

The first step is to show that $\pi < \pi_E$ holds for all E even. By way of contradiction, if $\pi_{E_0} < \pi$ then $\pi_{E_0+2} < \pi_{E_0}$, since cancelling common terms we have

$$\pi_{E_0+2} < \pi_{E_0} \iff \frac{E_0(E_0+2)}{(E_0+1)^2} < 1$$

which is true for all E_0. Iterating this argument we obtain (with $E = 2j$ denoting the subsequence of even integers)

$$\pi = \lim_{E\to\infty} \pi_E < \pi_{E_0} < \pi$$

a contradiction. Now for E even, we define

$$\pi_{\tilde{E}} = \pi_E \left(\frac{E}{E+1} \right)$$

A directly analogous argument left to the reader shows that $\pi_{\tilde{E}} < \pi$. Putting these two facts together we obtain

$$\pi_{\tilde{E}} < \pi < \pi_E \tag{2}$$

Equation (2) implies the desired Equation (1). This is a simple computation:

$$|\pi - \pi_E| \overset{\Delta}{=} \pi_E - \pi < \frac{\pi}{E} \iff \pi_{\tilde{E}} < \pi.$$

Note both inequalities in Equation (2) are used. The fact $\pi < \pi_E$ is used for $\overset{\Delta}{=}$. Then

$$\pi_E - \pi < \frac{\pi}{E} \iff \pi_E < \pi \left(\frac{E+1}{E} \right)$$

which rearranges to the statement that $\pi_{\tilde{E}} < \pi$, i.e. the other inequality in Equation (2).

Now we know π and π_E are within 10^{-n} of each other, it remains to show their decimal expansion agrees in the n-th decimal place. To this end, Conway utilizes the following result.

Lemma 5.1. *(Mähler's irrationality measure) If p/q is any rational number with $gcd(p, q) = 1$,*

$$\left| \pi - \frac{p}{q} \right| > \frac{1}{q^{42}}.$$

Write $\pi_E = p/q$, with $\gcd(p,q) = 1$. Applying Mähler's Lemma

$$\frac{1}{q^{42}} < \left|\pi - \frac{p}{q}\right| < \frac{\pi}{E} < \frac{1}{10^{42n}},$$

whence (since $x \to x^{42}$ is an increasing function) $q > 10^n$. Assume that

$$10^n \pi_E = \frac{10^n N_E}{D_E} = \frac{10^n p}{q}$$

is an integer. Since $q > 10^n$, there is a prime number r whose multiplicity in the prime decomposition of q is greater than the multiplicity of r in the prime decomposition of 10^n (the power of r could be zero in the prime decomposition of 10^n). Hence r divides p, which is a contradiction as p and q are coprime. This proves fully that Conway's algorithm works.

There is actually an elementary proof that $\frac{10^n p}{q}$ is not an integer. This will used in the proof of our first main theorem since there is no irrationality measure for $\sqrt{2}$ (it is algebraic). Supposing $\frac{10^n p}{q}$ is an integer means that q divides 10^n. Since q is odd, that implies $q = 5^j$ where $j \leq n$. However, when we cancel all the common factors in N_E and D_E to get p and q, we cannot cancel the largest prime in D_E. This is a consequence of Dirichlet's theorem, which states there must be at least one (odd) prime between E and $E/2$: this number is greater than 5, and no number in N_E divides into it. This is the desired contradiction

Remark 5.2. It is apparent from our discussion that PIGAME can be simplified: there is no need to generate such a large E. The size of E is exploited when using Mähler's irrationality measure, but we have seen this is not needed.

6. $\sqrt{2}$GAME

Our first main result is as follows.

Theorem A. *When started at $2^n \cdot 173$, the Fractran code*

$$\frac{424375}{173}, \frac{101}{1067}, \frac{89}{291}, \frac{13}{194}, \frac{4897}{97}, \frac{2425}{101}, \frac{1243}{89}, \frac{89}{565}, \frac{4949}{113}, \frac{109}{13}, \frac{3159}{763}, \frac{97}{109}, \frac{321}{83}, \frac{83}{1177},$$

$$\frac{103}{107}, \frac{365}{206}, \frac{29}{721}, \frac{79}{64375}, \frac{41}{2575}, \frac{103}{73}, \frac{71}{29}, \frac{638}{355}, \frac{4393}{4189}, \frac{73}{71}, \frac{71}{191}, \frac{1525}{79}, \frac{79}{122}, \frac{12931}{183}, \frac{107}{61},$$

$$\frac{2669}{12931}, \frac{149}{1273}, \frac{18745}{521461}, \frac{31}{67}, \frac{329322079}{18055}, \frac{67}{157}, \frac{157}{131}, \frac{385447}{2533}, \frac{151}{149}, \frac{149}{139}, \frac{2329}{7097}, \frac{67}{151},$$

$$\frac{151}{137}, \frac{67}{163}, \frac{938}{1333}, \frac{61}{31}, \frac{7}{943}, \frac{254}{41}, \frac{41}{11}, \frac{1}{3}, \frac{1}{7}, \frac{1}{13}, \frac{1}{17}, \frac{1}{19}, \frac{1}{23}, \frac{1}{47}, \frac{1}{1024}, \frac{53}{127}, \frac{2921}{371}, \frac{41}{53},$$

will terminate at $2^{\sqrt{2}(n)}$, where $\sqrt{2}(n)$ is the n-th digit in the decimal expansion of $\sqrt{2}$.

This list of fractions is generated from the flow chart in Figure 4, where we label each node with a distinct prime number and break all loops up as per Conway's algorithm. For economy of space, the term $1/C$ in the figure refers to the list of fractions

$$\frac{1}{3}, \frac{1}{7}, \frac{1}{13}, \frac{1}{17}, \frac{1}{19}, \frac{1}{23}, \frac{1}{47}, \frac{1}{1024}.$$

It is obvious from the flow chart that our proof is based on PIGAME. Theorem B, presented in the next section, will show a more standard algorithm for computing $\sqrt{2}$. Nevertheless, $\sqrt{2}$GAME has the merit of fitting into the same framework as PIGAME.

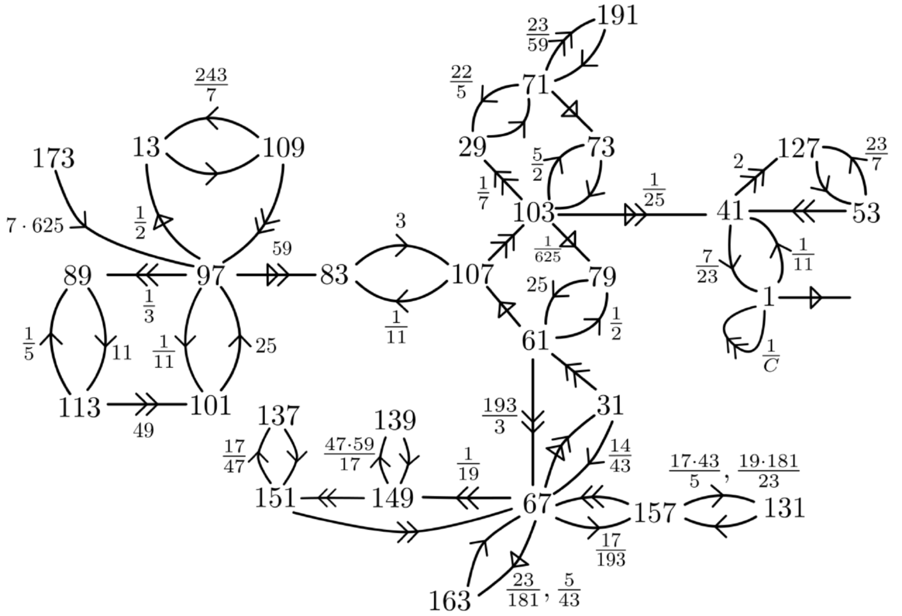


FIGURE 4. The flow chart for $\sqrt{2}$GAME

Proof. The starting point is the infinite product formula for $\sqrt{2}$ due to Catalan in 1874 [1] and which is very similar to Wallis' formula: viz.

$$\sqrt{2} = \left(\frac{2.2}{1.3}\right)\left(\frac{6.6}{5.7}\right)\left(\frac{10.10}{9.11}\right)\cdots$$

This program will truncate Catalan's product formula in an analogous manner to PIGAME. Defining

$$\sqrt{2}_E := \frac{2^2}{1.3}\frac{6^2}{5.7}\cdots\frac{(E-4)^2}{(E-5)(E-3)}\frac{E}{E-1} = \frac{N_E}{D_E},$$

we claim that the approximation $\sqrt{2}_E$ is sufficiently close to $\sqrt{2}$ and show that $10^n\sqrt{2}_E$ is never an integer to prove that the program does indeed compute the n-th digit in the decimal expansion of $\sqrt{2}$.

The first phase, from node 89 to node 83, is almost identical to PIGAME. The only difference is the requirement to kill the extra 2 Conway has in his formula for N_E. This comes from the fact that Wallis' infinite product formula is for $\frac{\pi}{2}$, so he needs to double his numerator to approximate π. In contrast, we have an infinite product formula for $\sqrt{2}$, so a slight modification of Conway's argument is needed. We skip his first pass around the square region, instead first going into the upper triangular region of Phase 1 with initial values $r_5 = 4$ and $r_7 = 49$. From here, the first phase proceeds in the same fashion as Conway, and it is easy to check we reach node 83 with

$$r_2 = 0,\ r_3 = 1,\ r_5 = E,\ r_7 = 10^n,\ r_{11} = 0,\ r_{59} = 1$$

where E is a very large even number. For Conway, it suffices to know that each pass around the square region "at least doubles" r_5 (which is initially set to 4) and keeps it even. This is because there is a well-defined truncation π_E for π for any even number E. However, for Catalan's formula for $\sqrt{2}$ to be appropriately truncated, one has to check that $E \equiv 2 \bmod 4$. Entering the square region for the first time, we have $r_5 = 4$, and we exit with $r_4 = 10$. In fact if we enter the square region with $r_5 = 4j + 2$, we exit with $r_5 = 4(2j + 1) + 2$, as the reader can easily check.

In the second phase, from node 83 to node 41, the essential point is that we copy Conway but modify how much we subtract from r_5 during each loop to generate N_E. However, we have to also generate D_E, which has a different form than the denominator of π_E. We break each pass around the region into part (i), where we travel up from node 107, and part (ii), going down from node 61. Just as in PIGAME, part (i) sets $r_7 = 0$ and multiples r_5 by r_7, storing this number in r_{11}. However we also transfer r_{59} to r_{23} and reset $r_{59} = 0$.

Moving onto part (ii) of our loop, the hierarchy of arrows (corresponding to the order we carry out the operations) becomes more delicate. As in PIGAME, we transfer r_{11} to r_3, while preserving r_{11}. Note r_5 decreases by 2 (as opposed to Conway, who decreases r_5 by 1). With this modified value of r_5, we multiply r_3 by r_5, storing this in r_7. Then we add 1 to r_5 (storing it in r_{17}), and multiply this new number by r_{23}, storing it in r_{59}. The program continues in this phase until r_5 reaches a value of 2. The program then starts phase (i) of the final loop, but cannot go to phase (ii) of the loop and exits to start phase (iii) at node 41. At the end of the second phase $r_{11} = 10^n N_E$ and $r_{23} = D_E$. In the following chart, we summarize how each register updates during the second phase, breaking each loop into (i) and (ii) schematically.

up (i)	down (ii)
$r_{11} = r_5.r_7$	$r_3 = r_{11}$
$r_5 = r_5$	$r_5 = r_5 - 2$
$r_7 = 0$	$r_7 = r_3 \cdot r_5$
$r_{23} = r_{59}$	$r_{17} = r_5 + 1$
$r_{59} = 0$	$r_{59} = r_{23} \cdot r_{17}$

To clarify the proof, let us explicitly perform four loops of the second phase (numbered I–IV) in the following table. Each loop is broken into parts (i) and (ii).

I(i)	I(ii)	II(i)	II(ii)
$r_{11} = 10^n E$ $r_5 = E$ $r_{23} = 1$ $r_7 = r_{59} = 0$	$r_5 = E - 2$ $r_7 = E - 2$ $r_{17} = E - 1$ $r_3 = 10^n E$ $r_{59} = E - 1$	$r_{11} = (E-2)^2$ $r_5 = E - 2$ $r_7 = 0$ $r_{23} = E - 1$	$r_5 = E - 4$ $r_7 = 10^n(E)(E-4)$ $r_{17} = E - 3$ $r_3 = (E-2)^2$ $r_{59} = (E-1)(E-3)$

III(i)	III(ii)
$r_{11} = 10^n(E)(E-4)^2$ $r_5 = E - 4$ $r_7 = 0$ $r_{23} = (E-1)(E-3)$	$r_5 = E - 6$ $r_7 = (E-2)^2(E-6)$ $r_{17} = E - 5$ $r_3 = 10^n(E)(E-4)^2$ $r_{59} = (E-1)(E-3)(E-5)$

IV(i)	IV(ii)
$r_{11} = (E-6)^2(E-2)^2$ $r_5 = (E-6)$ $r_7 = 0$ $r_{23} = (E-1)(E-3)(E-5)$ $r_{59} = 0$	$r_5 = (E-8)$ $r_7 = 10^n(E)(E-4)^2(E-8)$ $r_{17} = (E-7)$ $r_{59} = (E-1)(E-3)(E-5)(E-7)$ $r_3 = (E-6)^2(E-2)^2$

Continuing on one more loop and recording the key register of interest, note that at the end of loop V(i) we have $r_{11} = 10^n E(E-4)^2(E-8)^2$. Since $r_5 \equiv 2 \bmod 4$, the program will complete an even number of full loops until $r_5 = 2$. It will then go into phase (i) of an odd numbered loop, but it cannot go into phase (ii) and so the program passes to the third phase with $r_{11} = 10^n N_E$ as claimed.

Moving into the third phase, we copy with obvious modifications the third phase of PIGAME to compute the n-th decimal of $\sqrt{2}_E$. The balance of the proof will involve two steps.

Step 1 Establish the inequality

$$|\sqrt{2} - \sqrt{2}_E| < \frac{2\sqrt{2}}{E}. \tag{3}$$

Step 2 Show that $10^n \sqrt{2}_E$ is not an integer.

Since $\frac{2\sqrt{2}}{E} < 10^{-n}$, Steps 1 and 2 together prove that the program computes the n-th term in the decimal expansion of $\sqrt{2}$, just as in PIGAME. To prove Equation (3), firstly we show $\sqrt{2}_E > \sqrt{2}$. If to the contrary $\sqrt{2}_{E_0} < \sqrt{2}$ for some $E_0 = 4j + 2$, where $j \in \mathbb{N}$, then

$$\sqrt{2}_{E_0+4} < \sqrt{2}_{E_0} \iff E_0^2 + 4E_0 < E_0^2 + 4E_0 + 3$$

which is obviously true. Since the sub-sequence $\sqrt{2}_{4j+2} \to \sqrt{2}$, we again easily derive a contradiction in the exact same manner as in the proof of PIGAME. Setting

$$\sqrt{2}_{\tilde{E}} = \left(\frac{E}{E+2}\right)\sqrt{2}_E,$$

an analogous proof shows that $\sqrt{2}_{\tilde{E}} < \sqrt{2}$. In summary for all $E = 4j + 2$ we have

$$\sqrt{2}_{\tilde{E}} < \sqrt{2} < \sqrt{2}_E. \tag{4}$$

However, Equation (4) is equivalent to Equation (3), as

$$|\sqrt{2} - \sqrt{2}_E| \overset{\Delta}{=} \sqrt{2}_E - \sqrt{2} < \frac{\sqrt{2}}{x} \iff \sqrt{2}_E < \sqrt{2}\left(\frac{x+1}{x}\right)$$

where $\overset{\Delta}{=}$ uses the second inequality of Equation (4). However Equation (4) establishes $\sqrt{2}_{\tilde{E}} < \sqrt{2}$. Choose now $x = E/2$ to obtain

$$\sqrt{2}_{\tilde{E}} = \left(\frac{x}{x+1}\right)\sqrt{2}_E$$

and we see that Equation (3) immediately follows from the first inequality in Equation (4).

The final step is to prove $\frac{10^n p}{q}$ is never an integer, where $\sqrt{2}_E = \frac{p}{q}$ with p and q coprime. This is directly analogous to our explanation for PIGAME, and the proof of Theorem A is now complete. □

7. NR$\sqrt{2}$GAME

7.1. **Description.** The standard way to approximate $\sqrt{2}$ is to use Heron's algorithm, or equivalently the Newton–Raphson method applied to the function $f(x) = x^2 - 2$ with initial guess $x_1 = p_1/q_1 = 1/1$. This updates via

$$x_{k+1} = \frac{p_{k+1}}{q_{k+1}} = \frac{p_k^2 + 2q_k^2}{2p_k q_k}.$$

We claim that computing x_{2n} will generate a rational number sufficiently close to $\sqrt{2}$ to agree to n decimal places. Encoding this as a FRACTRAN program is our second main result.

Theorem B. *Starting at $2^n \cdot 89$, the following FRACTRAN code terminates at $2^{\sqrt{2}(n)}$:*

$$\frac{4979909}{89}, \frac{227,123,851}{466}, \frac{233}{239}, \frac{11809}{23533}, \frac{241}{251}, \frac{60,993}{1687}, \frac{267}{723}, \frac{267}{257}, \frac{17355}{2827}, \frac{277}{267}, \frac{271}{277}, \frac{3047}{1355},$$

$$\frac{241}{277}, \frac{2959}{1205}, \frac{233}{241}, \frac{283}{233}, \frac{859579}{8207}, \frac{283}{281}, \frac{24278273}{18961}, \frac{307}{283}, \frac{313}{5833}, \frac{3170}{2191}, \frac{313}{317}, \frac{331}{313}, \frac{2359}{1655},$$

$$\frac{307}{331}, \frac{311}{307}, \frac{8903}{622}, \frac{347}{307}, \frac{359}{14227}, \frac{3350}{15437}, \frac{359}{353}, \frac{367}{359}, \frac{16039}{16515}, \frac{367}{347}, \frac{17101}{694}, \frac{379}{347}, \frac{397}{9475}, \frac{389}{397},$$

$$\frac{3970}{18,283}, \frac{409}{397}, \frac{401}{409}, \frac{19223}{2005}, \frac{379}{409}, \frac{421}{379}, \frac{12151}{2947}, \frac{421}{419}, \frac{283}{40837}, \frac{467}{421}, \frac{433}{13543}, \frac{6465}{4763}, \frac{433}{431},$$
$$\frac{443}{433}, \frac{5423}{2215}, \frac{443}{439}, \frac{467}{443}, \frac{457}{467}, \frac{7}{30619}, \frac{457}{3}, \frac{922}{457}, \frac{5093}{3227}, \frac{461}{463}, \frac{457}{463}, \frac{449}{1024}, \frac{449}{3}, \frac{449}{67}, \frac{1}{449}.$$

This list of fractions was generated from the flow chart in Figure 5 following Conway's algorithm. In the flow chart $1/C$ denotes the following list of fractions;

$$\frac{1}{3}, \frac{1}{67}, \frac{1}{1024}.$$

The program initializes with $r_2 = n$. For the reader's ease, we will break the flow chart into phases (i), (ii), etc., in descending order. Phase (i) terminates at the 283 node. Initially the algorithm sets $r_{11} = r_{29} = r_{67} = 1$. Our initial guess for $\sqrt{2}$ is $x_1 = r_{29}/r_{67} = 1/1$. In general, we set $x_j = p_j/q_j$, where $p_j = r_{29}$ and $q_j = r_{67}$. As we move along phase 1, note we end with $r_{97} = 2n$. This is the number of iterations of the NR algorithm we must perform. Phase (i) also sets $r_{11} = 10^n$ as the reader can check.

In Phase (ii), we transfer both p_j and q_j, where $1 \leq j \leq 2n$ is the current stage of the NR algorithm, to three new registers to facilitate computation later. Phase (ii) ends when we reach the 347 node. Here $r_{29} = p_j^2$. Similarly phase (iii) ends when we reach the 379 node with $r_7 = 2q^2$, and phase (iv) ends at the 379 node with $r_{67} = 2p_jq_j$. We then travel back up to phase (ii) with

$$r_{29} = p_j^2 + 2q_j^2, \quad r_{67} = 2p_jq_j, \quad \text{and} \quad r_5 = 10^n.$$

This key step encodes the iterative loop. Here r_{13} decreases by 1, and we updated from x_k to x_{k+1} as we travel back through the flow chart to phase (ii).

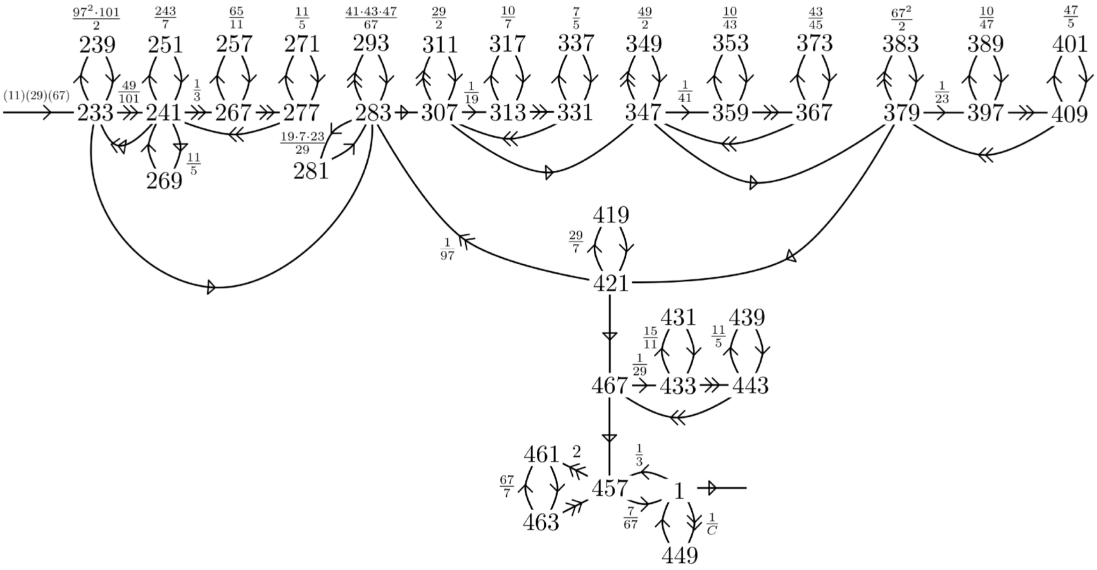


FIGURE 5. The flow chart for NR$\sqrt{2}$GAME

After $2n$ iterations, we move to phase (v) at node 467. Here we firstly multiply $r_{29} = p_{2n}$ by $r_{11} = 10^n$ (storing it in r_3) before, à la PRIMEGAME, computing the integer part of $\frac{10^n p_{2n}}{q_{2n}}$ modulo 10. This is the n-th term in the decimal expansion of x_{2n}. Now the mechanisms of the algorithm have been explained, we have to prove that x_{2n} is sufficiently close to $\sqrt{2}$ that both numbers agree in the n-th decimal place. To this end, we need the following lemma.

Lemma 7.1. *Suppose that f is a smooth function on $[1,2]$ with $|f'| \geq L$ and $|f''| < M$ for some L, $M > 0$. If $f(r) = 0$, then the error which arises from applying the Newton-Raphson algorithm to f, starting at x_1, N times is given by*

$$|x_{N+1} - r| < \frac{M}{2L}|x_N - r|^2.$$

Proof of Theorem B. To compute the n-th decimal digit of $\sqrt{2}$, we need to estimate $\epsilon_N := |x_N - \sqrt{2}|$. For later use $\epsilon_1 = \frac{1}{2}$. By induction, it is clear that $x_k \in [1,2]$ for all $k \in \mathbb{N}$. Applying the standard error estimates for Newton's method with $f(x) = x^2 - 2$, we have $|f''| = 2$ and $2 \leq |f'(x)| \leq 4$ on $[1,2]$. We iterate the error bound from Lemma 7.1 to obtain

$$\epsilon_N < \left(\frac{1}{2}\right)\epsilon_{N-1}^2 < \left(\frac{1}{4}\right)\epsilon_{N-2}^4 \dots < \frac{\epsilon_1^{2N}}{2^N} = \frac{1}{2^{3N}}.$$

This shows that

$$\epsilon_N < \frac{1}{10^{n+1}} \iff \frac{1}{2^{3N}} < \frac{1}{10^{n+1}}$$

which clearly holds if $N = 2n$. With this error bound x_N and $\sqrt{2}$ must agree up to the n-th decimal place, once we know that $\frac{10^n p_{2n}}{q_{2n}}$ is not an integer.

To establish this last claim, assume to the contrary that

$$\frac{10^n(p_{2n-1}^2 + 2q_{2n-1}^2)}{2p_{2n-1}q_{2n-1}} \tag{5}$$

is an integer. With $p_1 = q_1 = 1$, it follows p_n is odd and q_n is even for all $n > 1$. Let λ be a prime divisor of q_{2n-1}. Then $\lambda = 5$ or $\lambda | p_{2n-1}^2 + 2q_{2n-1}^2$, in which case $\lambda | p_{2n-1}$. So every prime divisor of q_{2n-1} aside from 5 divides into p_{2n-1}, meaning we can write

$$\frac{p_{2n-1}}{q_{2n-1}} = \frac{\mu}{5^j}$$

where μ is an even integer with $\gcd(5,\mu) = 1$. Feeding this into Equation (5) yields

$$\frac{10^n(p_{2n-1}^2 + 2q_{2n-1}^2)}{2p_{2n-1}q_{2n-1}} = \frac{10^n(\mu^2 + 2(5^{2j}))}{\frac{2\mu}{5^j}} \in \mathbb{N}$$

which implies that

$$\frac{5^{3j+n}2^n}{\mu} \in \mathbb{N},$$

whence $\mu = 2^r$ for some $r \in \mathbb{N}$. Putting this all together yields

$$\frac{p_{2n-1}}{q_{2n-1}} = \frac{2^r}{5^j}.$$

Cross-multipying yields a contradiction as it implies an even number is equal to an odd one. □

References

[1] Catalan, E. *Sur la constante d'Euler et la fonction de Binet*, C.R. Acad. Sci. Paris Sér. I Math. 77 (1873), 198-201.

[2] Conway, J.H. *FRACTRAN: a simple universal programming language for arithmetic*, Open Problems in Communication and Computation, Springer-Verlag New York Inc. (1987), 4–26.

[3] Conway, J.H. *Unpredictable Iterations*, Proc 1972 Number Tehory Conf., Univ. Colorado, Boulder, pp. 49–52.

[4] Guy, R.K. *Conway's prime-producing machine*, Math. Mag. 56 (1983), no. 1, 26–33. 33.

[5] Lagarias, J.C. *Conway's Work on Iteration: In memory of John Horton Conway (1937–2020)* The Mathematical Intelligencer, (06), 2021, Vol.43 (2), p.3–9.

[6] Penrose, R. *The Emporer's New Mind*, Oxford University Press, 1989.

[7] Sondow, J. and Hi, H. *New Wallis- and Catalan-type infinite products for π, e and $\sqrt{2+\sqrt{2}}$, Amer. Math. Monthly, 117 (2010), no. 10, 912-917.*

APPENDIX: CONVERTING A FLOW CHART INTO A FRACTRAN CODE

The following code converts our flow charts into their corresponding list of FRACTRAN fractions. For a single node in the flow chart, we write a line describing to what node it is connected and through what fraction. Line 17 then shows how you convert that line into a series of fractions. This is described more in Section 8 of [2]. In a single line the order in which the connections are listed handles the hierarchy of the arrows.

```
#Each line should be P, a/b->Q, c/d->R, ...

with open('fracn.txt') as file:
    fractionList = list()
    fractionFactored = list()
    for line in file:
        entries = line.split(',␣')
        P = entries[0]
        for entry in entries[1:]:
            print(entry)
            a,temp = entry.split('/')
            b,Q = temp.split('->')
            Q = Q.strip()
            fractionFactored.append(a+'*'+Q+'/'+b+'*'+P)
            aQ = str(int(a)*int(Q))
            bP = str(int(b)*int(P))
            fractionList.append(aQ+'/'+bP)
    print(fractionFactored)
    print(fractionList)

with open('fractions.txt', 'w') as file:
    file.write(',␣'.join(fractionList))

with open('fractionsFactored.txt', 'w') as file:
    file.write(',␣'.join(fractionFactored))
```

Khushi Kaushik graduated in 2025 from CSU Fullerton with a degree in Computer Science. Broadly interested in machine learning and data science, she is starting her M.Sc. in Comp. Sci. at UC San Diego.
Tommy Murphy is Professor at Cal State Fullerton, having completed his Ph.D. under Jürgen Berndt at UCC and postdoctoral fellowships at the Université Libre de Bruxelles (Belgium) and McMaster University (Canada). His research interests span Riemannian and Kähler geometry, focused specifically on Einstein manifolds and symmetric spaces. He also maintains an active interest in the history of mathematics and collaborating with undergraduate students.
David Weed graduated in 2024 from CSU Fullerton with a degree in mathematics, and is currently undertaking his Ph.D. in mathematics at UC Riverside. He is exploring a range of topics in pure mathematics particularly around the representation and character varieties of surfaces and 3-manifolds.

(Kaushik) DEPARTMENT OF COMPUTER SCIENCE, CALIFORNIA STATE UNIVERSITY FULLERTON.
E-mail address: kkaushik@ucsd.edu

(Murphy) DEPARTMENT OF MATHEMATICS, CALIFORNIA STATE UNIVERSITY FULLERTON.
E-mail address: tmurphy@fullerton.edu
URL: http://www.fullerton.edu/math/faculty/tmurphy/

(Weed) DEPARTMENT OF MATHEMATICS, UC RIVERSIDE.
E-mail address: david@davidweed.net

Irish Math. Soc. Bulletin
Number 95, Summer 2025, 35– 42
ISSN 0791-5578

Commutators of the Unilateral shift and adjoint for reproducing kernel Hilbert spaces on the disk

NATHAN PARKER

Abstract. We generalise the result of Berger and Shaw [2] the trace formula for Hardy Hilbert space to a larger class of rotation invariant Hilbert function spaces on the unit disk. We also demonstrate many meaningful examples of these Hilbert spaces by computing the inner products. We also extend to a wider class than the unilateral shift, that is, weighted shifts under certain restrictions.

1. Introduction

This paper proves an extension of the Berger-Shaw theorem regarding the trace formula for the shift and its adjoint. Berger and Shaw dealt with the Hardy Hilbert space on the disk while we extend to a class of rotation invariant Hilbert function spaces on the disk; remarkably, all these trace formulas involve Dirichlet space. A recent summary of the historical progress made relating to the trace formula can be found in [12].

2. Reproducing Kernel Hilbert Spaces on the Disk

Definition 2.1 (Reproducing kernel Hilbert space)**.** A reproducing kernel Hilbert space RKHS on a domain $D \subseteq \mathbb{C}$ is a complex Hilbert space H of functions on D such that the maps of point evaluations $f \to f(z)$ are continuous linear functionals. For all $z \in D$ there exists a unique $K_z \in H$ such that $\langle f, K_z\rangle = f(z)$. Let $K(z,w) = \langle K_w, K_z\rangle_H$.

Lemma 2.2. *Let H be a RKHS:*

1. *Suppose that $z \to K_z$ is a weakly continuous map $D \to H$. Then the function $(z,w) \to K(z,w)$ is continuous for all z, w.*
2. *Suppose further that*
$$\int_\Gamma K(z,w)dz = 0$$
for all contours Γ in D. Then $f(z) = \langle f, K_z\rangle$ is holomorphic on D.

Proof.
1. By the weak continuity of $z \to K_z$, the map $z \to \langle f, K_z\rangle$ is continuous for all $f \in H$. We let $f = K_w$ and we have $z \to \langle K_w, K_z\rangle = K(z,w)$ continuous. The same argument holds for w and, by symmetry, we have joint continuity of the map.
2. This is due to Morera's theorem.

□

2010 *Mathematics Subject Classification.* 30H05, 47A07, 47B37.

Key words and phrases. Berger-Shaw, Carey-Pincus-Helton-Howe, Dirichlet space.

Received on 23-04-2025; revised 03-07-2025.

DOI: 10.33232/BIMS.0095.35.42.

The author was supported by an EPSRC scholarship. I also give thanks to my supervisor Gordon Blower for his assistance and suggestions.

Definition 2.3 (Rotation Invariance)**.** For the open unit disc $\mathbb{D}$, say that a reproducing kernel Hilbert space is rotation invariant if $R_\theta : f(z) \mapsto f(e^{i\theta}z)$ gives a linear isometric isomorphism on H.

An invertible isometry is a unitary, so $R_{-\theta} = R_\theta^\dagger$.

Definition 2.4 (Dirichlet Space)**.** The Dirichlet space $\mathcal{D}$ on the unit disk $\mathbb{D}$ is the space of holomorphic functions such that, for all $f \in \mathcal{D}$, we have

$$\int_{\mathbb{D}} |f'(z)|^2 dA(z) < \infty.$$

The inner product is given by

$$\langle f, g\rangle_{\mathcal{D}} = f(0)\overline{g(0)} + \frac{1}{\pi}\int_{\mathbb{D}} f'(z)\overline{g'(z)}\, dA(z).$$

The Dirichlet space $\mathcal{D}$ gives a RKHS on $\mathbb{D}$. Let $\mathcal{D}_0$ be the closed linear subspace $\mathcal{D}_0 = \{f \in \mathcal{D} : f(0) = 0\}$ of $\mathcal{D}$. The orthonormal basis of $\mathcal{D}_0$ is given by $\left\{\frac{1}{\sqrt{n}}z^n\right\}_{n=1}^{\infty}$. Let

$$f(z) = \sum_{n=0}^{\infty} a_n z^n, \qquad g(z) = \sum_{n=0}^{\infty} b_n z^n,$$

then

$$\langle f, g\rangle = \sum_{n=1}^{\infty}(n+1)a_n\overline{b_n}.$$

From here onwards we assume $(\alpha_n)_{n=0}^{\infty}$ is a sequence of positive real numbers.

Definition 2.5. For each sequence $\alpha = (\alpha_n)_{n=0}^{\infty}$ such that

$$\limsup_{n\to\infty}(\alpha_n)^{\frac{1}{n}} = 1,$$

let H_α be the Hilbert space whose elements are power series $f, g \in H_\alpha$ given by

$$f(z) = \sum_{n=0}^{\infty} a_n z^n, \qquad g(z) = \sum_{n=0}^{\infty} b_n z^n$$

with inner product given by

$$\langle f, g\rangle_{H_\alpha} = \sum_{n=0}^{\infty} a_n\overline{b_n}\alpha_n.$$

3. Main Theorem

Theorem 3.1. *Let $\alpha = (\alpha_n)_{n=0}^{\infty}$ obey*

$$\lim_{n\to\infty}\frac{\alpha_{n+1}}{\alpha_n} = 1$$

and suppose that α is concave or convex. The following properties hold:

1. *H_α is a rotation invariant Hilbert space.*
2. *H_α has reproducing kernel*

$$K_w(z) = \sum_{n=0}^{\infty}\frac{\overline{w}^n z^n}{\alpha_n}.$$

3. *Let S be the unilateral shift $Sf(z) = zf(z)$. Then S is a bounded linear operator on H_α.*

(4) *The adjoint shift $S^\dagger$ on H_α acting on*

$$f(z) = \sum_{n=0}^{\infty} a_n z^n$$

is given by

$$S^\dagger f(z) = \sum_{n=0}^{\infty} \frac{\alpha_{n+1}}{\alpha_n} a_{n+1} z^n.$$

(5) *The commutator of S and $S^\dagger$ is trace class and for all polynomials f and g*

$$\langle\!\langle f, g \rangle\!\rangle_{H_{a_n}} = \operatorname{tr}\left(g(S)^\dagger f(S) - f(S) g(S)^\dagger \right) = \frac{1}{\pi} \int_{\mathbb{D}} f'(z) \overline{g'(z)} \, dA(z).$$

Proof. (1) We have

$$\|f(e^{i\theta} z)\|_{H_\alpha}^2 = \sum_{n=0}^{\infty} |a_n e^{in\theta}|^2 \alpha_n = ||f||_{H_\alpha}^2.$$

(2) We have

$$f(w) = \sum_{n=0}^{\infty} a_n w^n = \sum_{n=0}^{\infty} \alpha_n a_n \frac{w^n}{\alpha_n} = \langle f, K_w \rangle_{H_\alpha}.$$

Hence

$$K_w(z) = \sum_{n=0}^{\infty} \frac{\overline{w}^n z^n}{\alpha_n}.$$

(3) Firstly, we have $S(\lambda f + g) = z(\lambda f + g) = \lambda z f + z g = \lambda S f + S g$ hence S is linear. Now we have

$$\|f\|_{H_\alpha}^2 = \sum_{n=0}^{\infty} |a_n^2| \alpha_n$$

and

$$\|Sf\|_{H_\alpha}^2 = \sum_{n=0}^{\infty} |a_n^2| \alpha_{n+1} = \sum_{n=0}^{\infty} |a_n^2| \alpha_n \frac{\alpha_{n+1}}{\alpha_n}.$$

Hence, since we know the series obtained by

$$\sup_{n \in \mathbb{N}_0} \left\{ \frac{\alpha_{n+1}}{\alpha_n} \right\} \sum_{n=0}^{\infty} |a_n^2| \alpha_n$$

is convergent, and we have

$$\sup_{n \in \mathbb{N}_0} \left\{ \frac{\alpha_{n+1}}{\alpha_n} \right\} \sum_{n=0}^{\infty} |a_n^2| \alpha_n \geq \sum_{n=0}^{\infty} |a_n^2| \alpha_n \frac{\alpha_{n+1}}{\alpha_n},$$

we must have

$$\|Sf\|_{H_\alpha}^2 \leq \sup_{n \in \mathbb{N}_0} \left\{ \frac{\alpha_{n+1}}{\alpha_n} \right\} ||f||_{H_\alpha}^2.$$

Hence S is a bounded operator.

(4) The adjoint shift must satisfy $\langle Sf, g \rangle_{H_\alpha} = \langle f, S^\dagger g \rangle_{H_\alpha}$. We have

$$\langle Sf, g \rangle_{H_\alpha} = \sum_{n=1}^{\infty} a_{n-1} \overline{b_n} \alpha_n, \quad \langle f, S^\dagger g \rangle_{H_\alpha} = \sum_{n=0}^{\infty} a_n \overline{b_{n+1}} \alpha_{n+1}$$

and these are equal by change of indices. Hence, the operator described must be the adjoint shift.

(5) We first consider $f(z) = g(z) = z^m$ and consider the operation on elements of the orthogonal basis $\{z^n\}_{n=0}^{\infty}$. We have:

$$z^n \xrightarrow{S^m} z^{n+m} \xrightarrow{(S^\dagger)^m} \frac{\alpha_{n+m}}{\alpha_n} z^n \ .$$

Also:

$$z^n \xrightarrow{(S^\dagger)^m} \frac{n-m+\frac{1}{2}+|n-m+\frac{1}{2}|}{2(n-m+\frac{1}{2})} \frac{\alpha_n}{\alpha_{n-m}} z^{n-m} \xrightarrow{S^m} \frac{n-m+\frac{1}{2}+|n-m+\frac{1}{2}|}{2(n-m+\frac{1}{2})} \frac{\alpha_n}{\alpha_{n-m}} z^n \ .$$

Hence we split into two cases to compute the trace. For $m > n$,

$$\left(S^{\dagger^m} S^m - S^m S^{\dagger^m}\right) z^n = \frac{\alpha_{n+m}}{\alpha_n} z^n.$$

For $m \leq n$ we have

$$\left(S^{\dagger^m} S^m - S^m S^{\dagger^m}\right) z^n = \left(\frac{\alpha_{n+m}}{\alpha_n} - \frac{\alpha_n}{\alpha_{n-m}}\right) z^n.$$

Hence we have

$$\operatorname{tr}\left(S^{\dagger^m} S^m - S^m S^{\dagger^m}\right) = \sum_{n=0}^{m-1} \frac{\alpha_{n+m}}{\alpha_n} + \sum_{n=m}^{\infty} \frac{\alpha_{n+m}}{\alpha_n} - \frac{\alpha_n}{\alpha_{n-m}}. \tag{1}$$

We proceed to show this is absolutely convergent. Since α is convex, the sequence $\frac{\alpha_{n+1}}{\alpha_n}$ is non-increasing by 4.1 of [9], hence the series in (1) contains all positive terms and the series is absolutely convergent. In this case the series mostly cancels and we are left with

$$\lim_{N\to\infty} \sum_{n=N-m+1}^{N} \frac{\alpha_{n+m}}{\alpha_n} = m$$

due to our ratio test assumption of

$$\lim_{n\to\infty} \frac{\alpha_n}{\alpha_{n+1}} = 1.$$

The concave case is similar. Hence we have

$$\operatorname{tr}\left(S^{\dagger^m} S^m - S^m S^{\dagger^m}\right) = m.$$

Hence $[S^{\dagger^m}, S^m]$ may be represented by a diagonal matrix with respect to the orthonormal basis $\left\{\frac{z^n}{\sqrt{\alpha_n}}\right\}_{n=0}^{\infty}$ of H_α. This is the same orthonormal basis as $\mathcal{D}_0$ hence these Hilbert spaces are equal and the inner products are identical. This proves this part of the theorem.

□

4. Generalisation to Weighted Shift

Definition 4.1. Given a Hilbert space H with orthonormal basis $\{z_n\}_{n=0}^{\infty}$ and a weight $r = \{r_n\}_{n=0}^{\infty}$ of complex numbers where $\sup_n |r_n| < \infty$, a weighted shift on H is an operator $S_r \in B(H)$ defined by $S_r z_n = r_n z_{n+1}$

Theorem 4.2. *Let $\alpha = (\alpha_n)_{n=0}^{\infty}$ obey*

$$\lim_{n\to\infty} \frac{\alpha_{n+1}}{\alpha_n} = 1$$

and suppose α is concave or convex. Further suppose S_r is a weighted shift for which

$$\lim_{n\to\infty} |r_n| = 1.$$

The commutator of S_r and $S_r^\dagger$ is trace class for all polynomials f and g and we have

$$\langle\langle f, g\rangle\rangle_{H_{an}}^r = \operatorname{tr}\left(g(S_r)^\dagger f(S_r) - f(S_r)g(S_r)^\dagger\right) = \frac{1}{\pi}\int_{\mathbb{D}} f'(z)\overline{g'(z)}\,dA(z).$$

Proof. We begin by explicitly stating the adjoint shift $S_r^\dagger$ on $f \in H_\alpha$. We have

$$S_r^\dagger f = \sum_{n=0}^{\infty} \frac{\alpha_{n+1}}{\alpha_n} a_{n+1}\overline{r_n} z^n.$$

We now mimic the proof of the unilateral case; consider $f(z) = g(z) = z^m$. We have the following:

$$z^n \xrightarrow{S_r^m} \textstyle\prod_{i=n}^{n+m-1} r_i z^{n+m} \xrightarrow{(S_r^\dagger)^m} \prod_{i=n}^{n+m-1} |r_i|^2 \frac{\alpha_{n+m}}{\alpha_n} z^n \ .$$

Also:

$$z^n \xrightarrow{(S_r^\dagger)^m} \prod_{i=n-m}^{n-1} \overline{r_i} \frac{n-m+\frac{1}{2}+|n-m+\frac{1}{2}|}{2(n-m+\frac{1}{2})} \frac{\alpha_n}{\alpha_{n-m}} z^{n-m}$$

$$\xrightarrow{S_r^m} \prod_{i=n-m}^{n-1} |r_i|^2 \frac{n-m+\frac{1}{2}+|n-m+\frac{1}{2}|}{2(n-m+\frac{1}{2})} \frac{\alpha_n}{\alpha_{n-m}} z^n$$

We split into two cases to compute the trace. For $m > n$,

$$\left(S_r^{\dagger^m} S_r^m - S_r^m S_r^{\dagger^m}\right) z^n = \prod_{i=n}^{n+m-1} |r_i|^2 \frac{\alpha_{n+m}}{\alpha_n} z^n.$$

For $m \leq n$ we have

$$\left(S_r^{\dagger^m} S_r^m - S_r^m S_r^{\dagger^m}\right) z^n = \left(\prod_{i=n}^{n+m-1} |r_i|^2 \frac{\alpha_{n+m}}{\alpha_n} - \prod_{i=n=m}^{n-1} |r_i|^2 \frac{\alpha_n}{\alpha_{n-m}}\right) z^n.$$

Hence we have

$$\operatorname{tr}\left(S_r^{\dagger^m} S_r^m - S_r^m S_r^{\dagger^m}\right) = \sum_{n=0}^{m-1} \prod_{i=n}^{n+m-1} |r_i|^2 \frac{\alpha_{n+m}}{\alpha_n} +$$
$$\sum_{n=m}^{\infty} \prod_{i=n}^{n+m-1} |r_i|^2 \frac{\alpha_{n+m}}{\alpha_n} - \prod_{i=n-m}^{n-1} |r_i|^2 \frac{\alpha_n}{\alpha_{n-m}}.$$

By similar arguments we are left with

$$\lim_{N\to\infty} \sum_{n=N-m+1}^{N} \prod_{i=n}^{n+m-1} |r_i|^2 \frac{\alpha_{n+m}}{\alpha_n}.$$

By our assumption on the limits of the weights, this also uniformly converges to m and the same argument holds on the orthonormal bases. □

5. Examples

Definition 5.1 (Polylogarithm function)**.** The polylogarithm function defined for $n \in \mathbb{N}$ and $|z| < 1$ is given by

$$\operatorname{Li}_n(z) = \sum_{k=1}^{\infty} \frac{z^k}{k^n}.$$

This is extended to $\mathbb{C}$ by analytic continuation. We observe that these functions have the property

$$\mathrm{Li}_{n+1}(z) = \int_0^z \frac{\mathrm{Li}(t)}{t} dt$$

and $\mathrm{Li}_1(z) = -\ln(1-z)$.

Example 5.2. For the sequences α_n in the top line of the given table, the corresponding RKHS on the disc has orthonormal basis, reproducing kernel and inner product given on successive lines below α_n. Given $\gamma > -2$ and Γ is Euler's gamma function and our α_n may be zero for up to finitely many elements.

α_n	1	n	$n+1$	$n^2(n-1)$
ONB	$\{z^n\}_{n=0}^{\infty}$	$\left\{\frac{1}{\sqrt{n}} z^n\right\}_{n=1}^{\infty}$	$\left\{\frac{1}{\sqrt{n+1}} z^n\right\}_{n=0}^{\infty}$	$\left\{\frac{1}{n\sqrt{n-1}}\right\}_{n=2}^{\infty}$
$K_w(z)$	$\frac{\overline{w}z}{1-\overline{w}z}$	$-\ln(1-\overline{w}z)$	$-\frac{\ln(1-\overline{w}z)}{\overline{w}z} - 1$	$2\overline{w}z + \ln\left((1-\overline{w}z)^{1-\overline{w}z}\right) - \mathrm{Li}_2(\overline{w}z)$
$\langle .,. \rangle$	$H^2(\mathbb{D})$	$\mathcal{D}_0$	$\mathcal{D}$	$\frac{1}{\pi} \int_{\mathbb{D}} f''(z)\overline{g''(z)} dA(z)$

α_n	$\frac{1}{n}$	$\frac{1}{n+1}$	$\frac{\Gamma(\beta+1)}{(\gamma+2n+2)^{(1+\beta)}}$
ONB	$\{\sqrt{n} z^n\}_{n=1}^{\infty}$	$\{\sqrt{n+1} z^n\}_{n=0}^{\infty}$	$\left\{\frac{(\gamma+2n+2)^{\frac{1+\beta}{2}}}{\sqrt{\Gamma(\beta+1)}} z^n\right\}_{n=0}^{\infty}$
$K_w(z)$	$\frac{\overline{w}z}{(1-\overline{w}z)^2}$	$\frac{\overline{w}z(2-\overline{w}z)}{(1-\overline{w}z)^2}$	$\sum_{n=1}^{\infty} \frac{(\gamma+2n+2)^{(1+\beta)}}{(n-k+1)\Gamma(\beta+1)} \overline{w}^n z^n$
$\langle .,. \rangle$	$\mathcal{A}^2(\mathbb{D})_0$	$\mathcal{A}^2(\mathbb{D})$	$\int_{\mathbb{D}} f(z)\overline{g(z)} \vert z \vert^{\gamma} (\log 1/\vert z \vert)^{\beta} \frac{dA(z)}{\pi}$

α_n	$\frac{(n-k+1)\Gamma(\beta+1)}{(\gamma+2n+2)^{(1+\beta)}} \prod_{i=2}^{k} (n-k+i)^2$
ONB	$\left\{\frac{(\gamma+2n+2)^{\frac{(1+\beta)}{2}}}{\sqrt{(n-k+1)\Gamma(\beta+1)}} \prod_{i=2}^{k} \frac{1}{(n-k+i)} z^n\right\}_{n=k}^{\infty}$
$K_w(z)$	$\sum_{n=k}^{\infty} \frac{(\gamma+2n+2)^{(1+\beta)}}{(n-k+1)\Gamma(\beta+1)} \prod_{i=2}^{k} \frac{1}{(n-k+i)^2} \overline{w}^n z^n$
$\langle .,. \rangle$	$\int_{\mathbb{D}} f^{(k)}(z)\overline{g^{(k)}(z)} \vert z \vert^{\gamma} (\log 1/\vert z \vert)^{\beta} \frac{dA(z)}{\pi}$

Proof. We show computation of the reproducing kernels and inner products. Let $\zeta = \overline{w}z$ so that we have $|\zeta| \leq 1$.

- $\alpha_n = n^2(n-1)$. We have

  $$K_w(z) = \sum_{n=2}^{\infty} \frac{\zeta^n}{n^2(n-1)}.$$

  We differentiate to obtain

  $$\frac{d}{d\zeta} K_w(z) = \sum_{n=2}^{\infty} \frac{\zeta^{n-1}}{n(n-1)} = \sum_{n=2}^{\infty} \frac{\zeta^{n-1}}{n-1} - \sum_{n=2}^{\infty} \frac{\zeta^{n-1}}{n}.$$

By change of indices we obtain:

$$\frac{d}{d\zeta}K_w(z) = \sum_{n=1}^{\infty}\frac{\zeta^n}{n} - \sum_{n=1}^{\infty}\frac{\zeta^n}{n+1}.$$

These are computed similarly by differentiating using the geometric series formula, with a change of index for the second term. We hence obtain

$$\frac{d}{d\zeta}K_w(z) = -\ln(1-\zeta) + \frac{\ln(1-\zeta)}{\zeta} + 1$$

which we integrate by [4] (2.711), (6.254) to obtain

$$K_w(z) = 2\zeta + (1-\zeta)\ln(1-\zeta) - \mathrm{Li}_2(\zeta).$$

- $\alpha_n = \frac{(n-k+1)\Gamma(\beta+1)}{(\gamma+2n+2)^{(1+\beta)}}\prod_{i=2}^{k}(n-k+i)^2$. We have

$$K_w(z) = \frac{1}{\Gamma(\beta+1)}\sum_{n=k}^{\infty}\frac{\zeta^n(\gamma+2n+2)^{\beta+1}}{n-k+1}\prod_{i=2}^{k}\frac{1}{(n-k+i)^2}.$$

This can be computed for any integral values β, k for example we consider, $\beta = 2$ and $k = 3$. We obtain

$$\frac{1}{2}\sum_{n=3}^{\infty}\zeta^n\frac{(\gamma+2n+2)^2}{(n-2)(n-1)^2n^2}.$$

By partial fractions we obtain:

$$\frac{1}{8}\sum_{n=3}^{\infty}\zeta^n\Bigg(\frac{\gamma^2+12\gamma+36}{n-2} + \frac{4\gamma^2+16\gamma}{n-1} - \frac{2\gamma^2+8\gamma+8}{n^2} - \\ \frac{5\gamma^2+28\gamma+36}{n} - \frac{4\gamma^2+32\gamma+64}{(n-1)^2}\Bigg).$$

We use standard series formulae results to obtain:

$$\frac{1}{8}\Bigg(-(\gamma^2+12\gamma+36)(\zeta^2\ln(1-\zeta)) - (4\gamma^2+16\gamma)(\zeta\ln(1-\zeta)+\zeta^2) + \\ (2\gamma^2+8\gamma+8)\Bigg(\zeta+\frac{\zeta^2}{4}-\mathrm{Li}_2(\zeta)\Bigg) + (5\gamma^2+28\gamma+36)\Bigg(\ln(1-\zeta) + \\ \zeta+\frac{\zeta^2}{2}\Bigg) + (4\gamma^2+32\gamma+64)(\zeta^2-\zeta\,\mathrm{Li}_2(\zeta))\Bigg).$$

We see we can calculate these for any values as shown. □

6. Closing Remarks

The result of our main theorem here gives an instance of the Carey Pincus formula, that is, if $T = X + iY$ is such that X, Y are bounded self-adjoint operators where the commutator $[X, Y]$ is trace class and T acts on a Hilbert space H, then for any pair of polynomials

$$p(x,y) = \sum_{j,k=1}^{n} a_{jk}x^jy^k, \qquad q(x,y) = \sum_{j,k=1}^{n} b_{jk}x^jy^k,$$

there exists a positive, integrable, compactly supported function $g_T : \mathbb{R}^2 \to \mathbb{R}$ known as the principal function such that

$$\mathrm{tr}[p(X,Y), q(X,Y)] = \frac{1}{2\pi i}\int_{\mathbb{C}}\left(\frac{\partial p}{\partial x}\frac{\partial q}{\partial y} - \frac{\partial p}{\partial y}\frac{\partial q}{\partial x}\right)g_T(x,y)dxdy.$$

Specifically, when H obeys our assumptions, we obtain that $g_T = 1$. Variations of this trace formula are used in the context of invariant subspaces of Hilbert space. Some discussion is found in [7] and [6]. We note that the sequences discussed here are natural to consider; by 4.1 of [10] we have that such sequences arise from Fourier transforms of L^1 functions.

References

[1] W. Rudin, "Projections on invariant subspaces," *Proceedings of the American Mathematical Society*, vol. 13, no. 3, pp. 429–432, 1962.

[2] C. A. Berger and B. I. Shaw, "Intertwining, analytic structure, and the trace norm estimate," in *Proceedings of a Conference on Operator Theory: Dalhousie University, Halifax, Nova Scotia April 13th and 14th, 1973*, Springer, 2006, pp. 1–6.

[3] J. B. Conway, "The Theory of Subnormal Operators," *Mathematical Surveys and Monographs*, vol. 36, 1991.

[4] I. S. Gradshteyn and I. M. Ryzhik, *Table of Integrals, Series, and Products*, Academic Press, 2014.

[5] H. Hedenmalm, B. Korenblum, and K. Zhu, "Beurling type invariant subspaces of the Bergman spaces," *Journal of the London Mathematical Society*, vol. 53, no. 3, pp. 601–614, 1996.

[6] J. Ni, "A Trace Formula on Invariant Subspaces of Hardy Space Induced by Rotation-Invariant Borel Measure," *Complex Analysis and Operator Theory*, vol. **14**, no. 1, 2020.

[7] K. Zhu, "A trace formula for multiplication operators on invariant subspaces of the Bergman space," *Integral Equations and Operator Theory*, vol. 40, pp. 244–255, 2001.

[8] E. Hille, "Introduction to general theory of reproducing kernels," *The Rocky Mountain Journal of Mathematics*, vol. 2, no. 3, pp. 321–368, 1972.

[9] A. Zygmund, *Trigonometric Series*, vol. 1, Cambridge University Press, 2002.

[10] Y. Katznelson, *An Introduction to Harmonic Analysis*, Cambridge University Press, 2004.

[11] N. K. Nikol'Skii, *Treatise on the Shift Operator: Spectral Function Theory*, vol. 273, Springer Science & Business Media, 2012.

[12] R. Howe, "Traces of commutators of integral operators–the aftermath," in *Mathematical Methods in Systems, Optimization, and Control: Festschrift in Honor of J. William Helton*, Springer, 2012, pp. 221–231.

Nathan Parker is a PhD student under the supervision of Gordon Blower at Lancaster University with interests in control theory, functional analysis and operator theory.

(Nathan Parker) School of Mathematical Sciences, Lancaster University
E-mail address: n.parker1@lancaster.ac.uk

Irish Math. Soc. Bulletin
Number 95, Summer 2025, 43– 63
ISSN 0791-5578

Wiring Switches to More Light Bulbs

STEPHEN M. BUCKLEY AND ANTHONY G. O'FARRELL

Abstract. Given n buttons and n bulbs so that the ith button toggles the ith bulb and perhaps some other bulbs, we compute the sharp lower bound on the number of bulbs that can be lit regardless of the action of the buttons. In the previous article we dealt with the case where each button affects at most 2 or 3 bulbs. In the present article we give sharp lower bounds for up to 4 or 5 wires per switch, and we show that the sharp asymptotic bound for an arbitrary number of wires is $\frac{1}{2}$. (Even if you've found their buttons, you can please no more than half the people all the time!)

1. Introduction

1.1. **The function $\mu(m,n)$.** This article is a continuation of [2], and we refer to that article for motivation and context. The focus of our attention is the function $\mu(n,m)$, which counts the minimum number of bulbs that can always be lit by some switching choice when each of n bulbs has a dedicated button (=switch) that switches it and up to $m-1$ other bulbs on or off. The problem is rephrased in precise terms using vectors and matrices over $\mathbb{F}_2$, the field with two elements, as follows:

Each conceivable wiring from n buttons to r bulbs may be represented by an element of the set $\mathcal{M}(n,r,\mathbb{F}_2)$ of all $n \times r$ matrices over $\mathbb{F}_2$, by letting column i represent the effect of button i. Replacing n and r by their maximum, and filling in with zeros, we might as well use square matrices, so for us a wiring corresponds to a directed graph G on n vertices, represented by an $n \times n$ matrix W over $\mathbb{F}_2$. A column vector in $\mathbb{F}_2^n$ may represent either the state (lit or unlit) of the n bulbs, or a choice (press or don't press) for n buttons. The effect of switch choice x on state c gives state $Wx + c$.

We are focussed on wirings with 1 on the diagonal, and we call these *admissible wirings*, but we shall have occasional use for inadmissible wirings.

The *Hamming norm* $|\cdot| : \mathbb{F}_2^n \to \mathbb{Z}_{\geq 0}$ is defined by letting $|u|$ be the the number of 1 entries in u. We define $M(W,c) := \max\{\, |Wx+c| : x \in Z_2^n \,\}$; it represents the maximal number of bulbs that can be lit by a choice of switches, given initial state c.

Given a wiring W, the *associated degree of vertex i* is the Hamming norm of the i-th column of W (the out-degree of node i in the graph G, the number of bulbs affected by button i). The degree of W is the maximum associated degree.

For any $n \in \mathbb{N}$, and any set A of $n \times n$ matrices over $\mathbb{F}_2$, we define

$$\mu_A = \min\{M(W,0) \mid W \in A\}\,,$$
$$\nu_A = \min\{M(W,c) \mid W \in A,\ c \in \mathbb{F}_2^n\}.$$

For $n, m \geq 1$, let $A(n,m)$ be the set of $n \times n$ matrices over $\mathbb{F}_2$ that have 1s all along the diagonal and satisfy $\deg(W) \leq m$. For $n \geq m \geq 1$, let $A^*(n,m)$ be the set of matrices

2020 *Mathematics Subject Classification.* Primary: 05D99. Secondary: 11B39, 68R05, 94C10.
Key words and phrases. wiring, switching, MAX-XOR-SAT, Hamming distance.
Received on 22-02-2025.
DOI: 10.33232/BIMS.0095.43.63.
The first author was partly supported by Science Foundation Ireland. Both authors were partly supported by the European Science Foundation Networking Programme HCAA.

in $A(n, m)$ for which $\deg(i) = m$, for all $i \in S$. The class of all admissible wirings on n vertices is $A(n) := A(n, n)$.

The functions we study are:

$$\begin{aligned} &\mu(n, m) := \mu_{A(n,m)}\,, \qquad &&\mu^*(n, m) := \mu_{A^*(n,m)}\,, \qquad &&\mu(n) := \mu(n, n)\,, \\ &\nu(n, m) := \nu_{A(n,m)}\,, \qquad &&\nu^*(n, m) := \nu_{A^*(n,m)}\,, \qquad &&\nu(n) := \nu(n, n)\,, \end{aligned}$$

It is convenient to define $\mu(0, m) = 0$ for all $m \in \mathbb{N}$. Given $n \geq m$, we have the following trivial inequalities:

$$\nu(n, m) \leq \nu^*(n, m) \leq \mu^*(n, m) \tag{1.1.1}$$

$$\nu(n, m) \leq \mu(n, m) \leq \mu^*(n, m) \tag{1.1.2}$$

1.2. **Results.** General formulae for ν and ν^*, and formulae for $\mu(\cdot, m)$ and $\mu^*(\cdot, m)$ for $m = 2, 3$ were determined in [2]. We'll summarise these in Section 2 below, but right now we mention only that if $m = 2, 3$, then $\mu(n, m)$ and $\mu^*(n, m)$ are asymptotic to $2n/3$ as $n \to \infty$. By contrast, we will see that for $m = 4, 5$, both functions $\mu(n, m)$ and $\mu^*(n, m)$ are asymptotic to $4n/7$. In fact we have the following result:

Theorem 1.1. *Let $n \in \mathbb{N}$.*

(a) For $j = 4, 5$, $\mu(n, j)$ is given by the equation

$$\mu(n, j) = \begin{cases} \left\lceil \dfrac{4n}{7} \right\rceil, & n \neq 7k - 2 \textit{ for some } k \in \mathbb{N}, \\ \left\lceil \dfrac{4n}{7} \right\rceil + 1 = 4k, & n = 7k - 2 \textit{ for some } k \in \mathbb{N}. \end{cases}$$

(b) If $n \geq 3$, then $\mu^*(n, 4) = 2\left\lceil \dfrac{2n}{7} \right\rceil$, the least even integer not less than $\mu(n, 4)$.

It is not hard to show that $\mu(n, m) \geq n/2$ for all $n, m \in \mathbb{N}$. This is asymptotically sharp according to the following result.

Theorem 1.2. $\lim\limits_{n\to\infty} \mu(n)/n = 1/2$.

In fact, this shows that $\dfrac{\mu(n)}{\nu(n)} \to 1$ (cf. Theorem C below).

1.3. **Outline.** The article is organized as follows. After some introductory material in Section 2, we consider $\mu(n, m)$ and $\mu^*(n, m)$ for numbers of the form $(n, m) = (2^{k+1} - 1, 2^k)$ in Section 3. This special case involves a wiring related to Hadamard matrices, and allows us to deduce Theorem 1.2.

In Section 4, we give an explicit upper bound $U(n, m)$ for $\mu(n, m)$. This upper bound has the appearance of being rather sharp: indeed, we know of no pair (n, m) such that $\mu(n, m) < U(n, m)$. Whether $\mu(n, m) = U(n, m)$ for all n, m is an interesting open question. The upper bound $U(n, m)$ sheds light on the formulae for $\mu(n, m)$ given above and in Section 2 which, although convenient for understanding the asymptotics of $\mu(n, m)$ as $n \to \infty$, do not seem to follow any clear pattern as m changes. The sequence $U(n, n)$ is connected to OEIS sequence A046699, which is of meta-Fibonacci type, and has a number of combinatorial descriptions in terms of trees.

In Section 5, we prove that if $\mu(\cdot, m) = U(\cdot, m)$ for $m = 2^k - 2$, then this equation also holds for $m = 2^k + i$, $i \in \{-1, 0, 1\}$. Theorem 1.1(a) will follow immediately from this result but Theorem 1.1(b) still requires a proof, which can be found in Section 6.

2. A recap of previous results and ideas

For ease of reference, we state and label some results from [2]. We need them either for proofs or for comparison purposes.

2.1. **Theorems from** [2]**.** We begin by listing the three main results in [2]: in the order listed below, these were Theorems 1.1, 1.2, and 3.2 in that article.

Theorem A. *Let $n \in \mathbb{N}$.*

(a) $\mu(n,2) = \left\lceil \frac{2n}{3} \right\rceil$.

(b) If $n \geq 2$, then $\mu^*(n,2) = 2\left\lceil \frac{n}{3} \right\rceil$, the least even integer not less than $\mu(n,2)$.

Theorem B. *Let $n \in \mathbb{N}$.*

(a) $\mu(n,3) = \mu(n,2)$.

(b) If $n \geq 3$, then

$$\mu^*(n,3) = \begin{cases} 4k-1, & n = 6k-3 \textit{ for some } k \in \mathbb{N}, \\ \mu(n,3), & \textit{otherwise.} \end{cases}$$

Note that $\mu^*(n,3) = \mu(n,3) + 1$ in the exceptional case $n = 6k - 3$.

Theorem C. *Let $n, m \in \mathbb{N}$, $m > 1$.*

(a) $\nu(n) = \nu(n,m) = \left\lceil \frac{n}{2} \right\rceil$.

(b) If $n \geq m$, then

$$\nu^*(n,m) = \begin{cases} \nu(n,m) + 1, & \textit{if } n \textit{ is even and } m \textit{ odd,} \\ \nu(n,m), & \textit{otherwise.} \end{cases}$$

In particular, $\nu^*(n,2) = \nu^*(n) = \nu(n)$ for all $n > 1$.

2.2. **Lemmas from** [2]**.** The next four results were, in the order listed below, Lemmas 3.1, 5.1, and 5.2, and Corollary 3.3 in [2].

Lemma D. *Let $n \in \mathbb{N}$. For all $W \in A(n)$ and $c \in \mathbb{F}_2^n$, the mean value of $|Mx + c|$ over all $x \in \mathbb{F}_2^n$ is $n/2$. In particular, $M(W,c) \geq n/2$ and $M(W,c) > n/2$ if the cardinality of $\{i \in [1,n] \cap \mathbb{N} \mid c_i = 1\}$ is not $n/2$.*

Lemma E. *Let $m \geq 2$ and $n \geq 1$. Then either $\mu(n+m,m) = \mu(n+m,m-1)$, or*

$$\mu(n+m,m) \geq \mu(n,m) + \nu(m) = \mu(n,m) + \left\lceil \frac{m}{2} \right\rceil .$$

Lemma F. *Let $n, m, n' \in \mathbb{N}$, with $n \geq m$. Then*

$$\mu^*(n+n', m+1) \leq \mu^*(n,m) + n' .$$

Corollary G. *If λ is any one of the four functions μ, μ^*, ν, or ν^*, then $\lambda(\cdot, m)$ is sublinear for all m:*

$$\lambda(n_1 + n_2, m) \leq \lambda(n_1, m) + \lambda(n_2, m)\,, \tag{2.2.1}$$

as long as this equation makes sense (i.e. we need $n_1, n_2 \geq m$ if $\lambda = \mu^*$ or $\lambda = \nu^*$).

2.3. **Edge functions.** Associated with the graph G is its vertex set S (which we treat as an initial segment $S(n) := \{1, \dots, n\}$ of the set $\mathbb{N}$ of natural numbers) and the *edge function* $F : S \to 2^S$, where $j \in F(i)$ if there is an edge from i to j, and the *backward edge function* $F^{-1} : S \to 2^S$, where $j \in F^{-1}(i)$ if there is an edge from j to i. We extend the definitions of F and F^{-1} to 2^S in the usual way: $F(T)$ and $F^{-1}(T)$ are the unions of $F(i)$ or $F^{-1}(i)$, respectively, over all $i \in T \subset S$. We say that $T \subset S$ is *forward invariant* if $F(T) \subset T$, or *backward invariant* if $F^{-1}(T) \subset T$. Given a wiring W, associated graph G, and $T \subset S$, we denote by W_T and G_T the subwiring and subgraph, respectively, associated with the vertices in T: more precisely, W_T is the matrix obtained by deleting all rows and columns of W other than those with index in T, and G_T is obtained by retaining only the vertices in T and those edges in G between vertices in T.

2.4. **Pivoting.** We now recall the concept of *pivoting*, as introduced in [2, Section 5]. Pivoting about a vertex i, $1 \leq i \leq n$, is a way of changing the given wiring W to a special wiring W^i such that $M(W^i, c) \leq M(W, c)$. Additionally, pivoting preserves the classes $A(n, m)$ and $A^*(n, m)$.

Let us fix a wiring $W = (w_{i,j})$ on n vertices, and let $F : S \to 2^S$ denote the edge function associated to W, where $S = S(n)$. Given $T \subset S$, and $i \in S$, we define $W^{i,T}$ by replacing the jth column of W by its ith column whenever $j \in F(i) \setminus T$. We refer to the wiring $W^{i,T}$ as the *pivot of W about i relative to T*. If T is nonempty, we refer to this process as *partial pivoting*, while if T is empty we call it *(full) pivoting* and write G^i, W^i, and F^i for the resulting graph, matrix, and edge function, respectively.

As in [2], we use the notation $\hat{K}_r$ to denote an augmented complete graph on r vertices, i.e. a complete graph augmented by a loop at each vertex. Full pivoting about vertex i just rewires $F(i)$ so that it becomes a $\hat{K}_{\deg(i)}$, which is thus a forward-invariant subgraph of W^i.

We refer to a forward-invariant $\hat{K}_r$ subgraph of a wiring graph W as an F_r (relative to W).

For $t \in \{0, 1\}$, we denote by $t_{p \times q}$ the $p \times q$ matrix all of whose entries equal t, and let $t_p = t_{p \times p}$. The matrix of a $\hat{K}_r$, is $1_{r \times r}$. This is (of course) different from the $r \times r$ identity matrix I_r, except when $r = 1$.

Pivoting relative to any T is a process with several nice properties: it has the non-increasing property $M(W^{i,T}, c) \leq M(W, c)$, it preserves membership of the classes $A(n, m)$ and $A^*(n, m)$, and if $F^{i,T}$ is the edge function of $W^{i,T}$, then $F^{i,T}(i) = F(i)$ is an augmented complete subgraph of the associated graph $G^{i,T}$, but might not be forward invariant in $G^{i,T}$.

2.5. **Graphical conventions.** We continue the graphical conventions introduced in [2]. Thus, we do not show loops or the internal edges in a $\hat{K}_r$, and a single arrow issuing from $\hat{K}_r$ represents r edges, one from each vertex in the $\hat{K}_r$, all sharing the same target. If several arrows from a $\hat{K}_r$ point to some $\hat{K}_s$, then distinct arrows have distinct targets (so the number of arrows will not exceed s). For instance, Figure 1 shows three views of a $\hat{K}_6$. Notice how the 36 directed edges of the $\hat{K}_6$ are hidden to varying degrees in this figure, and how the arrows represent multiple edges — two each in the version with $\hat{K}_2$s, and three each in the version with $\hat{K}_3$s. To reduce clutter further, we introduce the additional convention that an two-headed arc stands for a pair of arrows, one in each direction. This gives the two more views of $\hat{K}_6$ shown in Figure 2 in which individual two-headed arcs stand for up to six directed edges in the $\hat{K}_6$.

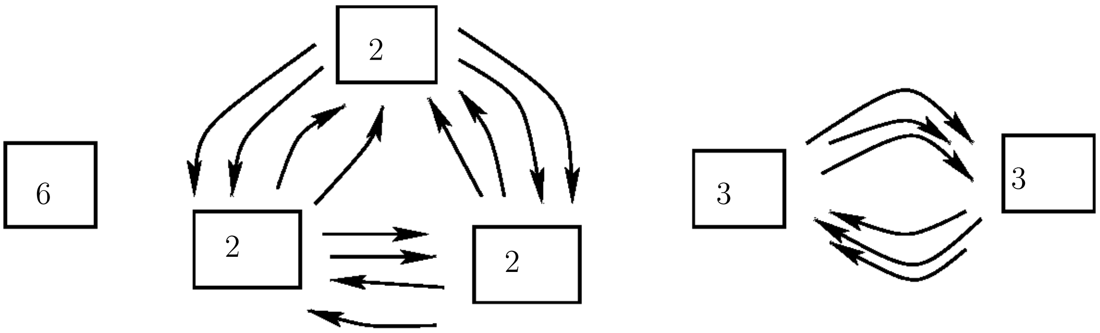
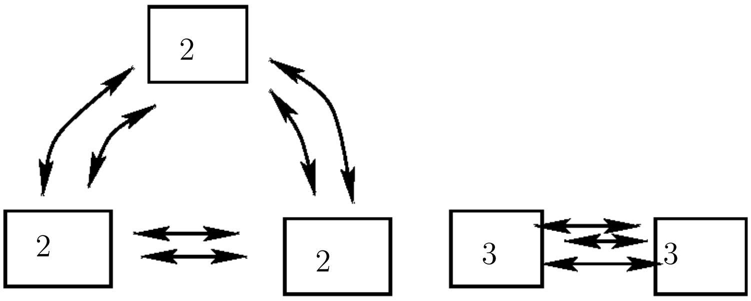


Figure 1. Views of $\hat{K}_6$



[h]

Figure 2. More views of $\hat{K}_6$

3. The case $(n, m) = (2^{k+1} - 1, 2^k)$

3.1. We begin with some observations for general n, m that will be useful here or in later sections. Trivially, $\mu(n, m)$ is nonincreasing as a function of m, but it is also easy to see that it is also nondecreasing as a function of n: given a wiring $W \in A(n, m)$ such that $|Wx| \leq \mu(n, m)$ for all $x \in \mathbb{F}_2^n$, it may be that vertex n has degree 1, in which case it is clear that if W' is obtained by eliminating the last row and column of W, then $|W'x'| \leq \mu(n, m)$ for all $x' \in \mathbb{F}_2^{n-1}$.

If instead vertex n has degree larger than 1 then, by pivoting if necessary, we may assume that vertex n forms a part of a forward invariant $\hat{K}_j$ for some $j > 1$. Because the effect of pressing vertex n is the same as the effect of pressing any other vertex in the $\hat{K}_j$, the set of vectors Wx, as $x = (x_1, \ldots, x_n)^t$ ranges over all vectors in $\mathbb{F}_2^n$ for which $x_n = 0$, coincides with the set of vectors Wx as x ranges over all of $\mathbb{F}_2^n$. It follows that if we define W' as in the previous case, then $|W'x'| \leq \mu(n, m)$ for all $x' \in \mathbb{F}_2^{n-1}$.

In contrast, we do not know whether or not $\mu^*(n, m)$ is an nondecreasing function of n.

3.2. Another easily proven inequality is:

$$\mu(n+1, m) \leq \mu(n, m) + 1 \,. \tag{3.2.1}$$

To see this, we need only consider the matrix $W \in A(n+1, m)$ which has block diagonal form $\operatorname{diag}(W', I_1)$, where $W' \in A(n, m)$ satisfies $M(W', 0) = \mu(n, m)$.

3.3. We now prove a pair of closely related lemmas. We will only use the second one in this section, but we will need the first one later.

Lemma 3.1. *Let $m, m', n \in \mathbb{N}$ and $m \le n$. Then*

$$\mu(nm', mm') \le m'\mu(n,m)$$
$$\mu^*(nm', mm') \le m'\mu^*(n,m)$$

Proof. Essentially the same proof works for μ and μ^*, so we write down only the one for μ. Let $W \in A(n,m)$ be such that $M(W,0) = \mu(n,m)$. We construct a new matrix W' by replacing each entry $w_{i,j}$ in W by an $m' \times m'$ block, each of whose entries is $w_{i,j}$, i.e. W' is the Kronecker product $W \bigotimes 1_{m' \times m'}$. It is readily verified that $W \in A(nm', mm')$.

The graph of W is obtained by replacing each vertex j in the original graph G by m' new vertices which we will label (j, j'), $1 \le j' \le m'$. Pressing vertex (j, j') changes the status of some other vertex (i, i') if and only if pressing j changes the status of vertex i in the original graph. In the new wiring W', each bulb of W has been replaced by a bank of m' bulbs, all of which are switched synchronously by any of their associated switches and it is clear that $M(W', 0) = m'M(W, 0)$. □

Figure 3 illustrates the proof that $\mu^*(18, 9) \le 3\mu^*(6, 3) (= 12)$, i.e. the case $n = 6$, $m = 3$, $m' = 3$. The graph W is the graph from Figure 12 in [2], the wiring example which concludes the proof that $\mu^*(6, 3) = 4$. To construct W', each vertex of W has been replaced by a $\hat{K}_3$ and each edge by three edges, one to each vertex of the $\hat{K}_3$ that replaces the original target. Thus, the original $\hat{K}_2$ and $\hat{K}_3$ become a $\hat{K}_6$ and a $\hat{K}_9$, respectively. In terms of bulbs and switches, each bulb becomes a bank of 3 bulbs, and each switch a bank of 3 switches, all having the same effect.

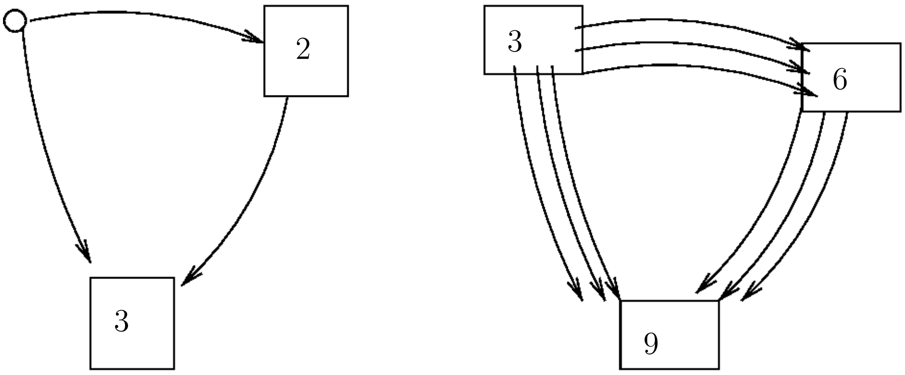


Figure 3. W and W'

It is also possible to view the new wiring W' as a row of m' copies of W, suitably wired together, and when we think of it in this way we refer to the copies as *clones* of W. Figure 4 shows this view of the above example. The view in Figure 4 is comparatively cluttered, but it is still substantially less messy than the full wiring graph, which has 162 directed edges.

Lemma 3.2. *Let $n, m, m' \in \mathbb{N}$ with $m'm \ge n+1$. Then $\mu(m'n+1, m'm) \le m'\mu(n,m)$.*

Proof. Let $W \in A(n,m)$ be such that $M(W,0) = \mu(n,m)$. As in the previous lemma, we construct a new matrix $W' = W \bigotimes 1_{m' \times m'}$. The wiring W' is a wiring for $m'n$ vertices which can be split into n banks of m' vertices that are always in sync (either all on or all off). We add one last vertex v and get a new wiring by connecting v to itself and to one vertex from each of the m' sets of clones. In terms of matrices, this can be achieved by defining a matrix with block form

$$W'' = \begin{pmatrix} W' & V \\ 0_{1 \times m'n} & I_1 \end{pmatrix} \tag{3.3.1}$$

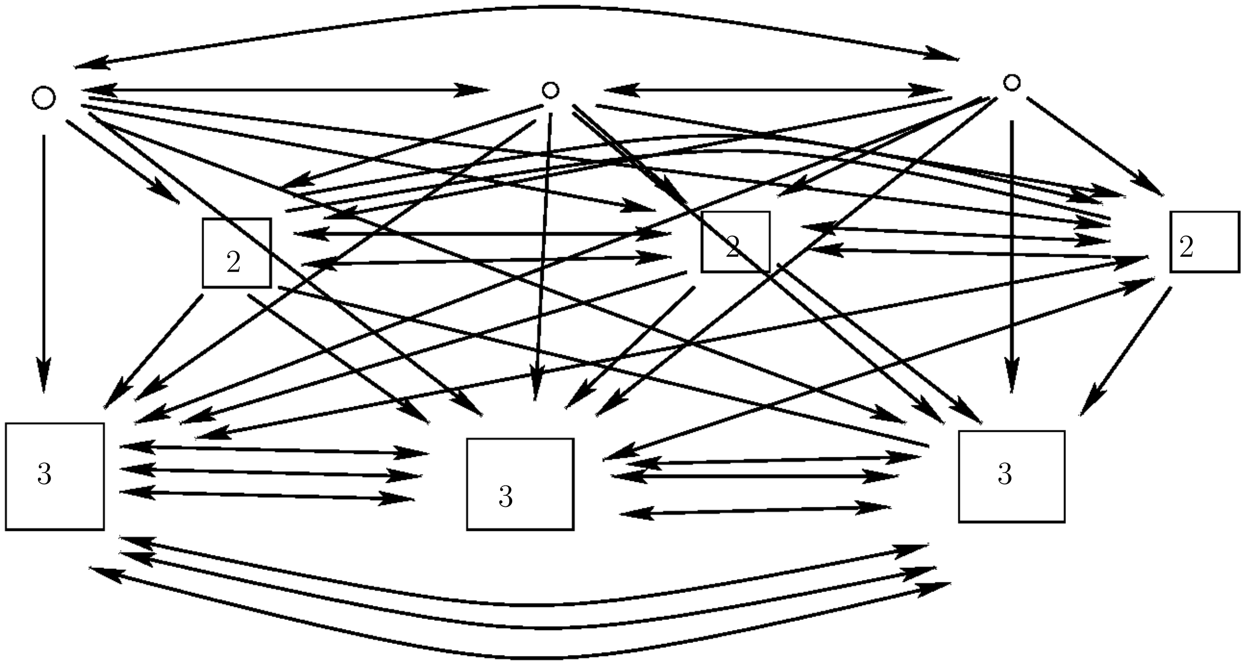


Figure 4. W'

where $V = (v_i)$ is a $m'n \times 1$ column vector with $v_i = 1$ if i is a multiple of m', and $v_i = 0$ otherwise. Using the inequality $m'm \geq n+1$, it is readily verified that $W \in A(m'n+1, m'm)$.

If we do not press v, then it is clear (as in the previous proof) that we can light at most $m'M(W,0) = m'\mu(n,m)$. Suppose therefore that we press v (together with some combination of other vertices). Partitioning each set of m' clones into two subsets S' and S'', where S'' has cardinality 2 and includes the vertex which is toggled by v, it is clear that all vertices in each of the S' sets remain in sync, that precisely one vertex in each S'' is lit, and that v itself is lit. Thus, we can light at most $(m'-2)\mu(n,m)+n+1$ if v is pressed. Since we know from Lemma D that $\mu(n,m) = M(W,0) > n/2$, we have $n+1 \leq 2\mu(n,m)$, and so $(m'-2)\mu(n,m)+n+1 \leq m'\mu(n,m)$, and we are done. □

3.4. We now state our first main result for m close to a power of 2.

Theorem 3.3. *For all $k \in \mathbb{N}$, and $m \geq 2^k$,*

$$\mu(2^{k+1}-1, m) = \mu^*(2^{k+1}-1, 2^k) = 2^k .$$

3.5. Using this theorem, it is easy to deduce Theorem 1.2, i.e. $\lim_{n\to\infty} \mu(n)/n = 1/2$:

Proof of Theorem 1.2. Lemma D implies that $\liminf_{n\to\infty} \mu(n)/n \geq 1/2$, so it suffices to show that $\limsup_{n\to\infty} \mu(n)/n \leq 1/2$. Fixing $k \in \mathbb{N}$, let us assume that $n > p := 2^{k+1}-1$. We write $n = ap+r$, where $a \in \mathbb{N}$ and $0 \leq r \leq p-1$. By inequality (2.2.1), Theorem 3.3, and the fact that $\mu(\cdot,\cdot)$ is nondecreasing in its first argument and nonincreasing in its second, we see that

$$\mu(n) \leq \mu(n, 2^k) \leq a\mu(p, 2^k) + \mu(r, 2^k) \leq (a+1)2^k .$$

Letting $n \to \infty$, it follows easily that $\limsup_{n\to\infty} \mu(n)/n \leq 2^k/(2^{k+1}-1)$. Since k can be chosen to be arbitrarily large, it follows that $\limsup_{n\to\infty} \mu(n)/n \leq 1/2$, as required. □

3.6. Sylvester-Hadamard matrices. Before proving Theorem 3.3, we need to discuss the Sylvester-Hadamard matrices, which are defined as follows:

$$H_2 = \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$$

and inductively H_{2^k} is given in block form by

$$H_{2^k} = \begin{pmatrix} H_{2^{k-1}} & H_{2^{k-1}} \\ H_{2^{k-1}} & -H_{2^{k-1}} \end{pmatrix} .$$

Equivalently, H_{2^k} is the Kronecker product $H_2 \bigotimes H_{2^{k-1}}$.

Let h be the rescaled Haar function given by $h(t) = 1$ if $\lfloor t \rfloor$ is even and $h(t) = -1$ otherwise. Let $h_p(t) = h(2^{-p}t)$ for all $p \in \mathbb{N}$, so that each function h_p is periodic. It is straightforward to verify that for fixed $k \in \mathbb{N}$ and $1 \leq j \leq 2^k$, the jth column $(a_{i,j})_{i=1}^{2^k}$ of H_{2^k} is always given by a pointwise product of one or more of the column vectors $(h_p(i-1))_{i=1}^{2^k}$, $1 \leq p \leq k$, and that any such product gives some column of H_{2^k}. It follows that a pointwise product of any number of the columns of H_{2^k} is another column of H_{2^k}, a fact that will be useful in the following proof.

3.7. Proof of Theorem 3.3.

Proof. By Lemma D and the fact that $\mu(\cdot,\cdot)$ is nonincreasing in its second argument, we have that $\mu^*(2^{k+1}-1, 2^k) \geq \mu(2^{k+1}-1, m) \geq 2^k$. Conversely, by taking $n = 2^{j+1}-1$, $m = 2^j$, and $m' = 2$ in Lemma 3.2, we deduce inductively $\mu(2^{k+1}-1, 2^k) \leq 2^k$, and so $\mu(2^{k+1}-1, m) \leq 2^k$.

It remains to get the same upper bound for $\mu^*(2^{k+1}-1, 2^k)$. For this, we need to work a little harder. Fix k and let $n = 2^{k+1}-1$. We claim that if we delete the first row and column of the Sylvester-Hadamard matrix $H_{2^{k+1}}$, and change each 1 entry to a 0 and each -1 to a 1, then we get an $n \times n$ matrix $W = W_k$ over $\mathbb{F}_2$ such that each column of W has exactly 2^k ones, and such that the pointwise sum of any two columns of W is another column of W or is a column of zeros.

The fact that any pointwise product of columns of $H_{2^{k+1}}$ is another column of that same matrix means that any pointwise product of columns of $H_{2^{k+1}}$ has either zero or 2^k entries equal to -1. Pointwise products for $H_{2^{k+1}}$ correspond to pointwise sums mod 2 for W, so the claim is established.

It follows from the claim that for each $x \in \mathbb{F}_2^n$, the vector Wx is some column of W, so $|Wx| = 2^k$ or 0.

For $k \in \mathbb{N}$, the graph with matrix W_k does not have a loop at each vertex, i.e. it corresponds to an inadmissible wiring. But if V is any matrix all of whose columns are columns of W_k, and which has only 1's on the diagonal, then $V \in A^*(n, 2^k)$ and for each $x \in \mathbb{F}_2^n$ we have $|Vx| = 2^k$ or 0 (because $Vx = WPx$ for some projection P), so we deduce that $M(V, 0) = 2^k$. The simplest way to construct such a matrix V from W is to repeat columns 1,2,4 and so on, respectively, once, twice, four times, etc. In other words, take column i of V equal to column 2^j of V whenever $2^j \leq i < 2^{j+1}$. This concludes the proof. □

3.8. Towers V_k. The matrix $V = V_k$ in the foregoing proof has the property that the nonzero entries occur in blocks that are of the form $1_{r\times r}$, where r runs through powers of 2. Graphically, this wiring V corresponds to a tower of $k+1$ augmented complete graphs, one of degree equal to each power of 2, as illustrated (sideways on) in Figure 5. The corresponding matrix is

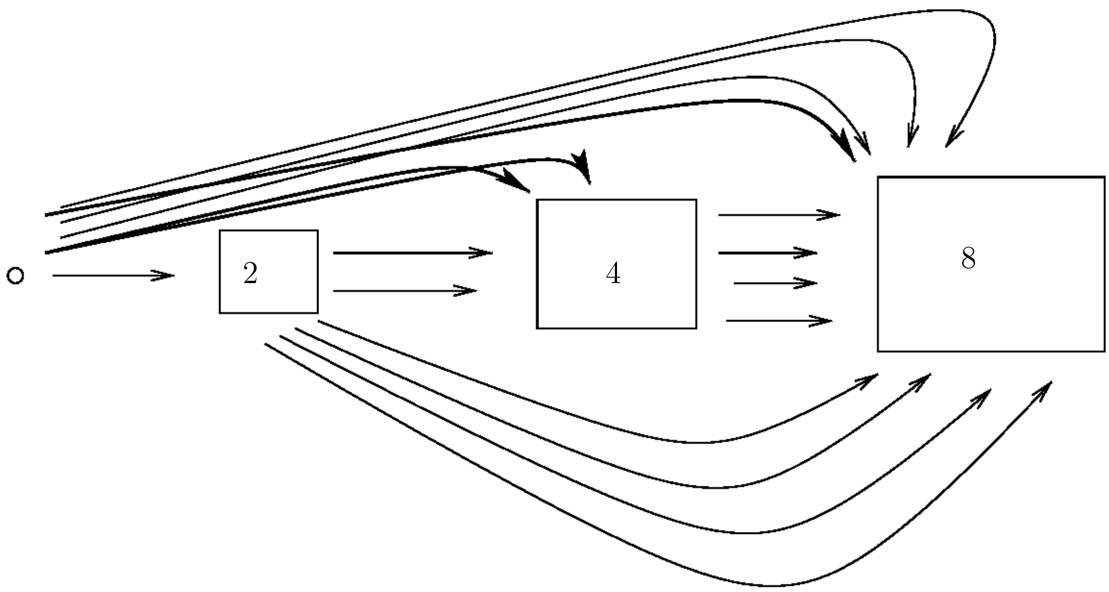


Figure 5. V_3

$$\begin{pmatrix}
1&0&0&0&0&0&0&0&0&0&0&0&0&0&0\\
0&1&1&0&0&0&0&0&0&0&0&0&0&0&0\\
1&1&1&0&0&0&0&0&0&0&0&0&0&0&0\\
0&0&0&1&1&1&1&0&0&0&0&0&0&0&0\\
1&0&0&1&1&1&1&0&0&0&0&0&0&0&0\\
0&1&1&1&1&1&1&0&0&0&0&0&0&0&0\\
1&1&1&1&1&1&1&0&0&0&0&0&0&0&0\\
0&0&0&0&0&0&0&1&1&1&1&1&1&1&1\\
1&0&0&0&0&0&0&1&1&1&1&1&1&1&1\\
0&1&1&0&0&0&0&1&1&1&1&1&1&1&1\\
1&1&1&0&0&0&0&1&1&1&1&1&1&1&1\\
0&0&0&1&1&1&1&1&1&1&1&1&1&1&1\\
1&0&0&1&1&1&1&1&1&1&1&1&1&1&1\\
0&1&1&1&1&1&1&1&1&1&1&1&1&1&1\\
1&1&1&1&1&1&1&1&1&1&1&1&1&1&1
\end{pmatrix}$$

The transition from W_k to V_k in the proof can be described by a sequence of pivots: A first pivot produces a forward-invariant $\hat{K}_{2^k}$, then a partial pivot with respect to the $\hat{K}_{2^k}$ produces a $\hat{H}_{2^{k-1}}$, and so on. The process converts a rather symmetrical inadmissible graph into an asymmetric admissible tower. Alternative constructions that amount to multiplying W_k by a permutation matrix convert the inadmissible graph to a symmetric admissible graph without a proper forward-invariant subgraph. Figure 6 shows an example, obtained by permuting the columns of V_2 to the order $(1, 2, 5, 6, 3, 4, 7)$ (As usual, the loops at the vertices are not shown.) This could be illustrated rather prettily on a regular tetrahedron by placing 1 at the apex, the $2, 4, 6$ as the vertices of the base triangle, and placing the remaining three points on the edges halfway up, with 5 on the edge $1 - 2$, 7 on $1 - 4$, and 3 on $1 - 6$. All the arrows can then be drawn on faces of the tetrahedron.

3.9. Remark. Note that there are Hadamard matrices H_{4n} of dimension $4n$ for many $n \in \mathbb{N}$, not just powers of 2; in fact, they are conjectured to exist for all dimensions $4n$ [10]. Since by definition the rows of an Hadamard matrix are pairwise orthogonal,

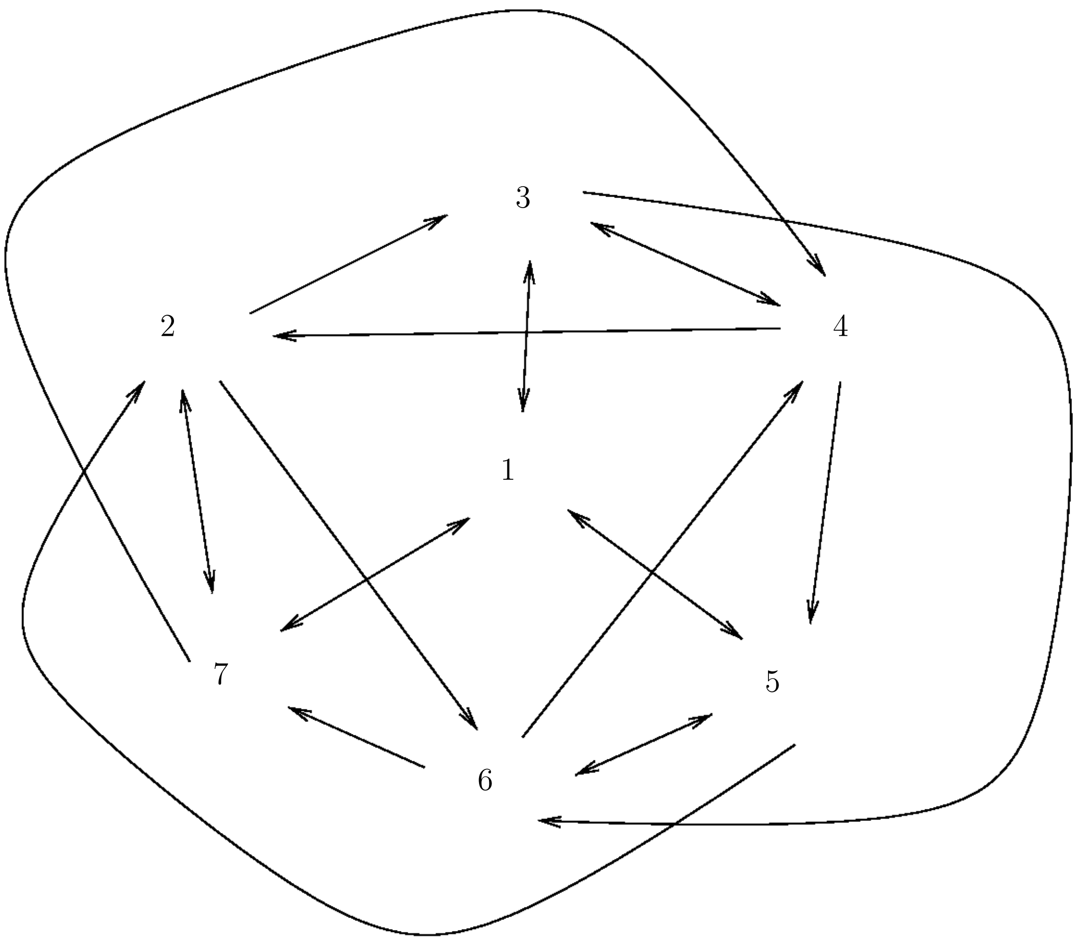


Figure 6. An alternative V for $k = 2$

one might wish to use H_{4n}^t as we used the symmetric Sylvester-Hadamard matrices. However, this is not possible for several reasons: we do not in general have a complete row and column of 1s suitable for deleting (although there is always an equivalent Hadamard matrix with this property), there may not be -1s along the diagonal of an associated minor, and some pointwise products of more than two columns of H_{4n} may have more than $2n$ entries equal to -1 (even if n is a power of 2). For instance, in the Paley-Hadamard matrix

$$P = \begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ -1 & 1 & -1 & -1 & 1 & -1 & 1 & 1 \\ -1 & 1 & 1 & -1 & -1 & 1 & -1 & 1 \\ -1 & 1 & 1 & 1 & -1 & -1 & 1 & -1 \\ -1 & -1 & 1 & 1 & 1 & -1 & -1 & 1 \\ -1 & 1 & -1 & 1 & 1 & 1 & -1 & -1 \\ -1 & -1 & 1 & -1 & 1 & 1 & 1 & -1 \\ -1 & -1 & -1 & 1 & -1 & 1 & 1 & 1 \end{pmatrix},$$

the pointwise product of columns 2, 3, and 5 contains all -1s, except from the first entry. For all these reasons, the method for Sylvester-Hadamard matrices does not in other cases produce a $W \in A(4n-1, 2n)$, let alone W such that $M(W, 0) = 2n$.

3.10. Codes. Hadamard matrices generate Hadamard codes, which have a certain optimality property. Recall that the code associated with H^{2^k} has 2^{k+1} codewords that make up a group $G < (\mathbb{F}_2^{2^k}, +)$. The above wiring $W \in A^*(2^k - 1, 2^{k-1})$ can by constructed from the code as follows. First, let $H < G$ be the order 2 subgroup generated by $(1, \ldots, 1)^t \in G$, and select the element in each coset of H, other than H itself, that has a 0 in the first coordinate. Discarding the first coordinate of each selected codeword yields a set of projected codewords that give the columns of W.

It would be interesting to know if there are any further connections between optimal codes and optimal wirings. There is a reason to expect that (near-)optimal linear codes may be associated with (near-)optimal wirings: a near-optimal linear code is one in which the minimum over all codewords w of the Hamming distance $|w|$ is about as large as possible, so if we take many of these codewords as the columns of the wiring matrix (perhaps after discarding one or more coordinates, as we did for Hadamard codes), we get a matrix for which $|Wx|$ is fairly large, except for the relatively few times when $Wx = 0$. A relatively large minimum nonzero value for $|Wx|$ should therefore be associated with a relatively small maximum value for $|Wx|$, since Lemma D says that the average of $|Wx|$ over all $x \in \mathbb{F}_2^n$ is $n/2$.

4. An upper bound for $\mu(n,m)$

In this section, we establish an upper bound $U(n,m)$ for $\mu(n,m)$ in all cases. This upper bound seems rather sharp, insofar as we know of no values n, m for which $\mu(n,m)$ and $U(n,m)$ differ. We also investigate $U(n,m)$ and a related nondecreasing sequence $(a(n))_{n=1}^\infty$ which we use to define U.

4.1. The sequence $a(n)$. We first define $(a(n))$ by the following inductive process:

$$\begin{aligned} a(1) &= 1\,, \\ a(2^k - 1 + i) &= 2^{k-1} + a(i)\,, && 1 \le i \le 2^k - 1,\ k \in \mathbb{N}\,, \\ a(2^{k+1} - 1) &= 2^k\,, && k \in \mathbb{N}\,. \end{aligned}$$

Thus $(a(n))$ begins:

1, 2, 2, 3, 4, 4, 4, 5, 6, 6, 7, 8, 8, 8, 8, 9, 10, 10, 11, 12, 12, 12, 13, 14, 14, 14, 15, 16, 16, 16, 16, 16, 17, ...

It is not hard to verify that the above sequence has the following alternative description: it is the nondecreasing sequence consisting of all positive integers, where the frequency of each integer n is the 2-adic norm of $2n$.

Note that $a(n) \le 2^k$ whenever $n \le 2^{k+1} - 1$.

If we add an extra 1 term to the beginning of the sequence $(a(n))$, we get a sequence $(b(n))$ listed in the OEIS (Online Encyclopedia of Integer Sequences) as A046699 [1]. The sequence (b_n) is defined by the initial conditions $b(1) = b(2) = 1$, and the following recurrence relation:

$$b(n) = b(n - b(n-1)) + b(n - 1 - b(n-2))\,, \qquad n > 2\,.$$

It can be deduced from this that $(a(n))$ satisfies the same recurrence relation as $(b(n))$: we just need to modify the initial conditions. We leave the verification of this to the reader, with the hint that it is straightforward to deduce it from the two inequalities $a(n) > n/2$ and $a(n+1) \le a(n) + 1$.

Such so-called *meta-Fibonacci sequences* go back to D. Hofstadter [7, p. 137], and are generally considered to be rather mysterious. Indeed, one of them was the subject of a \$10 000 prize offered by the late J. Conway [4]. However $(a(n))$ and $(b(n))$ are clearly rather tame members of this family, and one or other has appeared elsewhere in the context of binary trees; see [9], [5], [3], and [6].

4.2. The function U. Having defined $(a(n))$, we are now ready to define our upper bound function U. Given positive integers n and m, we choose the nonnegative integer k for which $2^k \le m < 2^{k+1}$, and we let q and r be the integers with $n = (2^{k+1}-1)q + r$, with $q \ge 0$ and $1 \le r < 2^{k+1}$. Thus, q and r are the usual integral quotient and remainder when n is divided by $2^{k+1}-1$, except when the remainder is zero, and in that case $r = 2^{k+1}-1$ and $q = (n-r)/(2^{k+1}-1)$. We then define $U(n,m) = q2^k + a(r)$.

Note that given n and m, the integers k, r, q so defined are unique, and that $U(n,m) \ge a(n)$. Following our usual notation, we write $U(n) = U(n,n)$, so that $U(n)$ is just an alternative notation for $a(n)$.

Proposition 4.1. *We have $\mu(n,m) \le U(n,m)$ for all $n, m \in \mathbb{N}$.*

Proof. The result is trivially true when $m = 1$. We prove the result for $2^k \le m < 2^{k+1}$ by induction on k. Assuming $\mu(\cdot, m) \le U(\cdot, m)$ for $2^{k-1} \le m < 2^k$, we need to prove that this estimate also holds for $2^k \le m < 2^{k+1}$. From now on, we assume that $2^k \le m < 2^{k+1} - 1$.

Sublinearity of $\mu(\cdot, m)$ and the inductive hypothesis gives $\mu(n, 2^k - 1) \le 2^k$ for all $n < 2^{k+1} - 1$. Since any wiring with a vertex of degree at least 2^k allows us to light at least 2^k vertices, we must have

$$\mu(n,m) = \mu(n, 2^k - 1) \le U(n, 2^k - 1) = U(n,m)$$

for $n < 2^{k+1} - 1$. If $n = 2^{k+1} - 1$, then Theorem 3.3 yields

$$\mu(n,m) = \mu(n, 2^k) = 2^k = U(n,m)\,.$$

Finally, the required inequality follows readily for all $n \ge 2^{k+1}$ by using the case $n < 2^{k+1}$ and sublinearity of $\mu(\cdot, m)$. Thus, we have proven the inductive step, and we are done. □

4.3. Sublinearity. Equation (2.2.1) says that $\mu(\cdot, m)$ is sublinear for all m. We now prove the same for $U(\cdot, m)$

Theorem 4.2. *For all $n_1, n_2, m \in \mathbb{N}$, we have $U(n_1 + n_2, m) \le U(n_1, m) + U(n_2, m)$.*

Proof. Since $U(\cdot, m)$ is unchanged as m varies over a dyadic block, it suffices to assume that $m = 2^k$ for some $k \ge 0$. We will show that $U(n, 2^k) = \mu'(n, 2^k)$, where $\mu'(n, 2^k) = \mu_{A'(n,2^k)}$ and $A'(n, 2^k)$ is an appropriate set of wiring matrices $W \in M(n, n; \mathbb{F}_2)$ that has the following closure property: if $W_i \in A'(n_i, 2^k)$ for $i = 1, 2$, then the block diagonal matrix

$$W = \begin{pmatrix} W_1 & 0 \\ 0 & W_2 \end{pmatrix}$$

lies in $A'(n_1 + n_2, 2^k)$. In terms of wirings, this just says that a disjoint union of two wirings in this class for given $m = 2^k$ also lies in this class for the same value of m. Sublinearity then follows easily from the definition of μ' and this closure property.

To define $A'(n, 2^k)$, we first define W_j for each $j \ge 0$ to be some wiring in $A^*(2^{j+1} - 1, 2^j)$ such that $M(W, 0) = \mu^*(2^{j+1} - 1, 2^j) = 2^j$; this exists by Theorem 3.3. We now define $A'(n, 2^k)$ to be the collection of matrices $W \in M(n, n; \mathbb{F}_2)$ that are of block diagonal form with $n_j \ge 0$ diagonal blocks of type W_j for some $0 \le j \le k$. Thus, $n = \sum_{j=0}^{k} n_j (2^{j+1} - 1)$.

We first show that $\mu'(n, 2^k) \le U(n, 2^k)$. Taking $k = 0$, it is clear that $U(n, 1) = \mu'(n, 1) = n$; note that the identity matrix is the only element of $A'(n, 1)$. We therefore assume that $k > 0$.

If $n < 2^{k+1} - 1$, then $U(n, 2^k) = U(n, 2^{k-1})$, so by choosing $W \in A'(n, 2^{k-1})$ satisfying $M(W, 0) = U(n, 2^{k-1})$, we get

$$\mu'(n, 2^k) \le \mu'(n, 2^{k-1}) \le U(n, 2^{k-1}) = U(n, 2^k)\,.$$

If $n = 2^{k+1} - 1$, then $\mu'(n, 2^k) \le M(W_k, 0) = 2^k = U(n, 2^k)$.

Finally if $n > 2^{k+1} - 1$, then we simply write $n = q(2^{k+1} - 1) + r$ in the usual way and select a wiring W that decomposes into q copies of W_k plus one copy of a wiring $W' \in A'(r, 2^k)$ satisfying $M(W', 0) = U(r, 2^k)$ to deduce that $\mu'(n, 2^k) \le q2^k + U(r, 2^k) = U(n, 2^k)$, as required.

We now prove the opposite inequality by induction. As mentioned above, the case $k = 0$ is clear. Suppose that $\mu'(\cdot, 2^j) = U(\cdot, 2^j)$ for all $0 \le j < k$, and suppose that $\mu'(n', 2^k) = U(n', 2^k)$ for all $n' < n$, $n' \in \mathbb{N}$. Let $W \in A'(n, 2^k)$ be such that $M(W, 0) < U(n, 2^k)$. Since $U(n, 2^k) \le U(n, 2^{k-1}) = \mu'(n, 2^{k-1})$, W must have a vertex of degree 2^k which is part of a W_k. Let W' be the subwiring obtained from W by removing this W_k, and so $W' \in A'(n - 2^k, 2^k)$. Now $M(W_k, 0) = 2^k$ and by minimality of n, we have $M(W', 0) \ge U(n - 2^k, 2^k)$, so $M(W, 0) \ge U(n - 2^k, 2^k) + 2^k \ge U(n, 2^k)$, as required. □

Since $U(n, m) = a(n)$ whenever there exists $k \in \mathbb{N}$ such that $n/2 < 2^k \le m$, it follows that $(a(n))$ is also sublinear, a fact we now record.

Corollary 4.3. *For all $n_1, n_2 \in \mathbb{N}$, we have $a(n_1 + n_2) \le a(n_1) + a(n_2)$.*

5. Results for m near a power of 2

5.1. In this section, we give some results for $2^k - 2 \le m \le 2^k + 1$. Our first result follows rather easily from Theorem 3.3.

Proposition 5.1. *For all $2 \le k \in \mathbb{N}$, we have $\mu(\cdot, 2^k - 1) = \mu(\cdot, 2^k - 2)$.*

Proof. Let $m := 2^k - 1$. By Proposition 4.1, we have $\mu(n, m - 1) \le 2^{k-1} + 1 \le m$ for all $n \le 2^k$. It follows that $\mu(n, m) = \mu(n, m - 1)$ for $n \le 2^k$, since any wiring W with a degree m vertex satisfies $M(W, 0) \ge m$.

Suppose inductively that $\mu(n', m) = \mu(n', m-1)$ for all $1 \le n' < n$, where $n > 2^k$, and we wish to extend this equation to $n' = n$. By Lemma E, either $\mu(n, m) = \mu(n, m - 1)$ and we have established the inductive step, or

$$\mu(n, m) \ge \mu(n - m, m) + 2^{k-1} = \mu(n - m, m - 1) + 2^{k-1}$$

and so

$$\begin{aligned}
&\mu(n - m, m - 1) + 2^{k-1} \le \mu(n, m) \\
&\text{(trivial estimate)} \qquad \le \mu(n, m - 1) \\
&\text{(sublinearity)} \qquad \le \mu(n - m, m - 1) + \mu(m, m - 1) \\
&\text{(trivial estimate)} \qquad \le \mu(n - m, m - 1) + \mu(m, 2^{k-1}) \\
&\text{(by Theorem 3.3)} \qquad = \mu(n - m, m - 1) + 2^{k-1}\,.
\end{aligned}$$

The inductive step, and so the lemma, follows from equality of the first and last lines. □

Theorem 5.2. *Let $m = 2^k$ for some $k \in \mathbb{N}$, and suppose that $\mu(\cdot, m-1) = U(\cdot, m-1)$. Then $\mu(\cdot, p) = U(\cdot, p)$ also holds for $p = m$ and $p = m + 1$. In particular, $\mu(\cdot, m) = \mu(\cdot, m + 1)$.*

Proof. Proposition 4.1 tells us that $\mu(\cdot, \cdot) \le U(\cdot, \cdot)$, so we must prove inequalities in the opposite direction. For $k = 1$, the desired conclusion follows from Theorems A and B, so we assume that $k > 1$.

We first consider the case $p = m$. Suppose for the sake of contradiction that $m = 2^k > 2$ is such that $\mu(\cdot, m) \ne U(\cdot, m)$, even though $\mu(\cdot, m - 1) = U(\cdot, m - 1)$. Also for the sake of contradiction, assume that $n \in \mathbb{N}$ is the smallest number such that $\mu(n, m) < U(n, m)$, and that $W \in A(n, m)$ is such that $M(W, 0) < U(n, m)$. Since

$\mu(n, m-1) = U(n, m-1) \geq U(n, m)$, it follows that W must contain a vertex of degree m. This certainly implies that $M(W, 0) \geq m = U(2m-1, m)$, so $n \geq 2m$.

We write $n = q(2m-1) + r$, where $q, r \in \mathbb{N}$ and $r < 2m$. By induction we have $M(W, 0) < qm + \mu(r, m)$. We may also assume that we cannot increase the number of F_m subgraphs in W by any amount of pivoting; recall that an F_m is a forward invariant augmented complete subgraph on m vertices.

We now carry out what for later reference we call a *Partition by Degree argument*: we partition the set of n vertices into subsets A and B, where A consists of all vertices that lie in an F_m, and B consists of all other vertices. Let us write n_A, n_B for the cardinalities of A and B, respectively.

Since we cannot increase the number of F_m subgraphs by pivoting, we have $W_B \in A(n_B, m-1)$. Since we can light all vertices in A by pressing one vertex in every F_m, we must have

$$n_A < U(n, m) = qm + \mu(r, m) \leq (q+1)m\,.$$

But n_A is a multiple of m, so $n_A \leq qm$. Alternatively, we can first light at least $\mu(n_B, m-1)$ of the B-vertices followed by at least $\nu(n_B, m) \geq n_A/2$ of the A-vertices, and so

$$\mu(n_B, m-1) + n_A/2 < qm + \mu(r, m)\,. \tag{5.1.1}$$

Suppose $n_A = qm$, and so $n_B = n - qm = q(m-1) + r$. By assumption, $\mu(n_B, m-1) = qm/2 + \mu(r, m-1)$, and so

$$\mu(n_B, m-1) + n_A/2 = qm + \mu(r, m-1) \geq qm + \mu(r, m)\,,$$

contradicting (5.1.1). If n_A is smaller than qm, it must be smaller by $q'm$ for some $q' \in \mathbb{N}$, thus increasing $\mu(n_B, m-1)$ by at least $q'm/2$:

$$\mu(n - qm - q'm, m-1) \geq \mu(n - qm - q'(m-1), m-1) = \mu(n - qm, m-1) + \frac{q'm}{2}\,.$$

Thus, $\mu(n_B, m-1) + n_A/2$ is at least as large as in the case $n_A = qm$, and we still get a contradiction.

We next prove that $\mu(n, m+1) = \mu(n, m)$. Again for the sake of contradiction, we suppose that $m = 2^k > 2$ is such that $\mu(\cdot, m+1) \neq U(\cdot, m+1)$, even though $\mu(\cdot, p) = U(\cdot, p)$ when $p = m-1$. This last equation holds also for $p = m$ by the first part of the proof. Note that $U(n, m+1) = U(n, m) = \mu(n, m)$.

Suppose also for the sake of contradiction that n is minimal for the inequality

$$\mu(n, m+1) < U(n, m+1) = \mu(n, m)\,.$$

Now, $U(n, m+1) \leq m+1$ for $n \leq 2m$, so as in the first part of the proof, we must have $n > 2m$. We again write $n = q(2m-1) + r$, where $q, r \in \mathbb{N}$ and $r < 2m$. Let $W \in A(n, m+1)$ be such that $M(W, 0) = \mu(n, m+1)$, and we assume that the number of F_{m+1}s cannot be increased by pivoting, and that the only possible pivoting operations that may increase the number of $\hat{K}_m$ subgraphs are those that decrease the number of F_{m+1} subgraphs; recall that a $\hat{K}_m$ is an augmented complete subgraph on m vertices (which is not necessarily forward invariant).

We carry out another Partition by Degree argument, with A consisting of all vertices that lie in a $\hat{K}_m$ or an F_{m+1}, and $W_B \in A(n_B, m-1)$. Now, W must be a vertex of degree $m+1$, since $M(W, 0) < \mu(n, m)$, and so W contains at least one F_{m+1}. Suppose that there are at least two F_{m+1}s. We can light at least $\mu(n - 2m - 2, m+1)$ of the other vertices, followed by at least $2\nu(m+1) = m+2$ of the vertices in the pair of

F_{m+1}s. Now

$$\begin{aligned}
&\text{(minimality of } n\text{)} \quad & \mu(n-2m-2, m+1) + m + 2 &= U(n-2m-2, m+1) + m + 2 \\
&& &= U(n-3, m) + 2 \\
&& &= \mu(n-3, m) + \mu(3, m) \\
&\text{(sublinearity)} && \geq \mu(n, m)\,,
\end{aligned}$$

contradicting the fact that $\mu(n, m+1) < \mu(n, m)$.

Thus, there is precisely one F_{m+1}, and n_A is equivalent to 1 mod m. We distinguish between those $\hat{K}_m$s that are forward invariant, which we denote as usual by F_m, and those that are not, which we denote by N_m. The one external link of each N_m is to the F_{m+1}, since otherwise we could pivot to get a second F_{m+1}. Furthermore, any two N_ms must link to the same vertex in the F_{m+1}, since if this were not the case, we could pivot about a vertex in one N_m to get a wiring with one N_m linked to a second N_m, which in turn links to a F_{m+1}, and such a configuration would allow us to get a second F_{m+1} by pivoting about the vertex in the first N_m.

It follows that we can light all except possibly one of the vertices in A, and so $n_A - 1 < qm + \mu(r, m-1) \leq (q+1)m$, which self-improves to $n_A \leq qm+1$. Alternatively, as in the first part of the proof, we get

$$\mu(n_B, m-1) + (n_A+1)/2 < qm + \mu(r, m-1)\,. \tag{5.1.2}$$

Suppose $n_A = qm + 1$, and so $n_B = q(m-1) + r - 1$. By the inductive hypothesis, $\mu(n_B, m-1) = qm/2 + \mu(r-1, m-1)$, and so by Lemma F,

$$\mu(n_B, m-1) + (n_A+1)/2 = qm + \mu(r-1, m-1) + 1 \geq qm + \mu(r, m) = qm + \mu(r, m-1),$$

contradicting (5.1.2). The case where n_A is smaller than qm is ruled out as in the first part of the proof. □

5.2. Partition by degree arguments. Since we will be seeing other variations of the above *Partition by Degree arguments*, let us describe the common features of these arguments, so that we can be sketchy in all subsequent uses of it. Given a wiring W on n vertices, we partition the set of vertices into two subsets, typically called A and B, and we denote the cardinality of A and B by n_A and n_B, respectively. The wiring will be initially pivoted so that A is forward invariant and W_A will consist only of $\hat{K}_j$s for various $j \geq 2^k$. There will be very few links between different $\hat{K}_j$s in A, allowing us to light almost all except at most n_0 of the vertices in A by pressing one vertex in each $\hat{K}_j$; for instance, n_0 was either 0 or 1 in the two Partition by Degree arguments in the above proof. This gives the bound $n_A \leq K - n_0$, where K equals either $\mu(n, m)$ or an assumed value of $\mu(n, m)$ from which we wish to derive a contradiction. By the structure of A, we often know that n_A has a certain value mod 2^k, allowing us to improve the estimate $n_A \leq K - n_0$ to $n_A \leq n_1$ for some $n_1 \leq K - n_0$.

By somehow maximizing the number of $\hat{K}_j$s in A, we arrange for the restricted wiring W_B to lie in $A(n_B, m')$ for some $m' \leq 2^k - 1$, so we may light at least $\mu(n_B, m')$ of these vertices followed by at least $\nu(n_A)$ vertices in A. This gives the inequality

$$\mu(n_B, m') + \nu(n_A) \leq K \tag{5.2.1}$$

The aim of the Partition by Degree argument is now either to derive a contradiction, or to show that $n_A = n_1$. To do this, we first consider the possibility that $n_A = n_1$, and we typically deduce that $\mu(n - n_1, m') + \nu(n_1)$ either equals or exceeds K. If instead we allow n_A to decrease below n_1, then n_A typically must be decreased by a multiple of 2^k, and $\mu(n_B, m')$ increases by at least as much as $\mu(n_A)$ decreases. Thus, if $\mu(n - n_1, m') + \nu(K_1) > K$, we get a contradiction to (5.2.1) also for any value of n_A less than n_1, and we are done. In other instances of this argument, $\mu(n - n_1, m') + \nu(K_1) =$

K, but taking a value of n_A smaller than K_1 increases $\mu(n_B, m')$ strictly more than $\mu(n_A)$ decreases, so we conclude that n_A must equal n_1 and $n_B = n - n_1$, as we are seeking to prove in such instances.

5.3. A technical lemma.

5.3. A technical lemma. We now give a lemma which makes no mentions of wirings and vertices but which we will need later. In this lemma, $|u|$ denotes the Hamming norm of a vector $u \in \mathbb{F}_2^N$, as defined in Section 1.

Lemma 5.3. *Let n, N and M be positive integers. Then the following are equivalent:*
(1) There exist vectors $a_j = (a_{i,j})_{i=1}^N \in \mathbb{F}_2^N$, $1 \le j \le n$ such that

$$\left|\sum_{j=1}^{n} \lambda_j a_j\right| = M \in \mathbb{N}\,, \qquad \text{for all } \lambda = (\lambda_j) \in F_n := \mathbb{F}_2^n \setminus \{0\}\,. \tag{5.3.1}$$

(2) $M = 2^{n-1}q$ for some $q \in \mathbb{N}$, and $N \ge 2M - 2^{1-n}M$.
Assuming these conditions are fulfilled, all solutions $(a_{i,j})$ to (5.3.1) are equivalent modulo permutations of the i and j indices.

Proof. Assuming the conditions (2) are fulfilled, with $M = 2^{n-1}q$, we see that $N \ge (2^n - 1)q$, so we can allocate $(2^n - 1)q$ vertices into $2^n - 1$ pairwise disjoint sets of q vertices each. We label these sets S_k for $1 \le k \le 2^n - 1$, and write $S = \bigcup_{i=1}^{2^n-1} S_k$. Writing $d_{n-1;k} \dots d_{1;k} d_{0;k}$ for the binary expansion of $1 \le k \le 2^n - 1$, we let $a_{i,j} := d_{j-1;k}$ for all $i \in S_k$, and $a_{i,j} = 0$ of $i \notin S$. It is readily verified that (5.3.1) holds with this choice of $(a_{i,j})$.

Conversely, suppose that $A := (a_{i,j})$ satisfy (5.3.1). Note that this condition implies the same condition with n replaced by any number $1 \le n' \le n$, and if we take $n' = n-1$, we can replace a_{n-1} by either a_n or $a_{n-1} + a_n$ and the condition remains true. For each $u = (u_j) \in F_n$, we write $S_n(u; A)$ for the set of indices $1 \le i \le n$ such that $a_{i,j} = u_j$ for all j. Trivially, such sets $S_n(u; A)$ are pairwise disjoint. Writing $\#(\cdot)$ for set cardinality, we claim that $\#(S_n(u; A)) = 2^{1-n}M$. Since $\#(F_n) = 2^n - 1$, it follows from the claim that $N \ge 2M - 2^{1-n}M$. Also, the fact that $\#(S_n(u; A))$ is independent of $u \in F_n$ means that there is essentially only one such solution, modulo permutations of the indices, so the result follows from the claim. We prove this by induction on n.

If $n = 1$, the claim is trivial. For $n = 2$, note that $|a_1 + a_2| = |a_1| + |a_2| - 2K = 2M - 2K$, where K is the number of indices i for which $a_{i,1} = a_{i,2} = 1$. Since $2M - 2K = M$, we must have $K = M/2$. This readily implies the result for $n = 2$.

Suppose inductively that the result is true for $n < m$, where $m > 2$, and we want to prove it for $n = m$. Let us define the following matrices

$$A_1 = (a_{i,j})_{\substack{1 \le i \le N \\ 1 \le j \le m-2}}\,, \quad A_2 = (a_{i,j})_{\substack{1 \le i \le N \\ 1 \le j \le m-1}}\,, \quad A_3 = (b_{i,j})_{\substack{1 \le i \le N \\ 1 \le j \le m-1}}\,, \quad A_4 = (c_{i,j})_{\substack{1 \le i \le N \\ 1 \le j \le m-1}}\,,$$

where

$$b_{i,j} = \begin{cases} a_{i,j}, & j \le m-2\,, \\ a_{i,m}, & j = m-1\,, \end{cases}$$

$$c_{i,j} = \begin{cases} a_{i,j}, & j \le m-2\,, \\ a_{i,m-1} + a_{i,m}, & j = m-1\,, \end{cases}$$

We assume that $A := (a_{i,j})_{\substack{1 \le i \le N \\ 1 \le j \le m}}$ satisfies (5.3.1) for $n = m$, so certainly A_s satisfies (5.3.1) for $1 \le s \le 4$ (for $n = m-2$ or $n = m-1$).

By the inductive assumption $\#(S_{m-1}(u; A_s)) = 2^{2-m}M$ for each $u \in F_{m-1}$ and $2 \le s \le 4$. Considering separately those $u = (u', u_{m-1}, u_m) \in F_{m-2} \times F_1 \times F_1 = F_m$

such that $u' \neq 0$ and $u' = 0$, we can in both cases argue as for $n = 2$ above that $\#(S_m(u)) = 2^{1-n}M$, as required. □

5.4. Towers again. We return to the special wirings V_k discussed in Subsection 3.8. For the rest of this section, a $\overline{K}_i$ will mean a $\hat{K}_{2^i}$, i.e. an augmented complete graph on 2^i vertices. The wiring $V_k \in A^*(2^{k+1}-1, 2^k)$ consists of augmented complete subgraphs $\overline{K}_0$, $\overline{K}_1$, $\overline{K}_2$,. . .,$\overline{K}_k$, such that each vertex of each $\overline{K}_i$ toggles zero vertices in $\overline{K}_j$ for $j < i$ and toggles 2^{j-1} vertices in each $\overline{K}_j$, $i < j \leq k$. In addition the set of vertices toggled in $\overline{K}_j$ by any $\overline{K}_i$ vertex for $i < j$ is independent of which vertex in $\overline{K}_i$ is chosen, so we may as well restrict ourselves to considering vertex press sets where we are allowed to press only one vertex, which we call the *designated vertex*, in each $\overline{K}_i$. We say that $\overline{K}_i$ is *activated* if its designated vertex is pressed. Thus, each $\overline{K}_i$ can be viewed as a single switch which toggles 2^{j-1} indices in $\overline{K}_j$ for each $j > i$. We assume that this wiring is arranged so that activating one or more of the $\overline{K}_i$, $i < j$, always lights exactly 2^{j-1} of the vertices in $\overline{K}_j$. This is possible by Lemma 5.3. In view of the uniqueness in Lemma 5.3, this defines the wiring V_k uniquely up to relabeling of the vertices within each $\overline{K}_j$, $1 \leq j \leq k$.

The next theorem generalises our remark that the Sylvester-Hadamard wiring W_k can be pivoted to obtain V_k. In this theorem, we push further with the ideas in the proof of Theorem 5.2 to show that if $\mu(\cdot, p) = U(\cdot, p)$ for $p < 2^k$ then, modulo (full and partial) pivoting, there really is only one optimal wiring in $A(n, 2^k)$ for each $n = q(2^{k+1} - 1)$, $q \in \mathbb{N}$, namely q disjoint copies of V_k.

Theorem 5.4. *Suppose that $\mu(\cdot, p) = U(\cdot, p)$ for all $p < m := 2^k$, for some $k \in \mathbb{N}$. If $n = q(2m - 1)$ for some $q \in \mathbb{N}$, and if $W \in A(n, m)$ is such that $M(W, 0) = \mu(n, m)$, then W can be pivoted to the block diagonal wiring* $\operatorname{diag}(V_k, \ldots, V_k)$*, where $V_k \in A^*(2m-1, m)$ is as above; both full and partial pivoting operations may be required.*

Proof. We will construct a chain of restricted wirings, so let us write W_k in place of W for our initial wiring, and we also write N_k in place of n. We assume without loss of generality that W_k has the property that no additional $\overline{K}_k$ subgraphs can be obtained by pivoting. We denote by B_k the set of all N_k vertices.

We do a Partition by Degree argument, partitioning the N_k vertices into two sets: A_k, of cardinality n_k, contains all vertices in any $\overline{K}_k$, and B_{k-1}, of cardinality N_{k-1}, contains all the other vertices. We denote by W_{k-1} the wiring W_k restricted to B_{k-1}. Then, $W_{k-1} \in A(N_{k-1}, 2^k-1)$, since otherwise we could create an extra $\overline{K}_k$ by pivoting.

As usual, we have $n_k \leq \mu(n, 2^k) = q2^k$ and

$$\mu(N_{k-1}, 2^k - 1) + \frac{n_k}{2} \leq \mu(n, 2^k) = q2^k\,. \tag{5.4.1}$$

The first inequality forces $n_k \leq q2^k$, so $N_{k-1} \geq q(2^k - 1)$. If $N_{k-1} = q(2^k - 1)$, we get equality in (5.4.1), but this inequality cannot hold if $n_k < q2^k$, since it would force the inequality $U(i2^k, 2^{k-1}) \leq i2^{k-1}$ for some $i \in \mathbb{N}$, which itself can be reduced to $U(i, 2^{k-1}) \leq 0$, $i \in \mathbb{N}$, which we know to be false. Thus, the only possible value for (n_k, N_{k-1}) is $(q2^k, q(2^k - 1))$.

The fact that this choice of (n_k, N_{k-1}) only satisfies (5.4.1) with equality means that we can analyze the wiring more closely and rule out any wiring that creates any slippage in the left-hand side bounds. In particular, if there were a vertex in W_{k-1} of degree $j > 2^{k-1}$, we could pivot about it relative to A_k to get a $\hat{K}_j$. Vertices in the $\hat{K}_j$ have at most $2^k - j$ links outside the $\hat{K}_j$, which must all be in A_k because of the pivoting process). By pressing a $\hat{K}_j$ vertex and then one vertex in every $\overline{K}_k$, we light all the vertices in the $\hat{K}_j$ and all except at most 2^k-j vertices in A_k, thus giving a contradiction since $q2^k - (2^k - j) + j > q2^k$. A $\overline{K}_{k-1}$ also leads to a contradiction unless its vertices link to exactly 2^{k-1} vertices in A_k.

Thus, $W_{k-1} \in A(q(2^k-1), 2^{k-1})$ and (5.4.1) forces $M(W_{k-1}, 0) = \mu(q(2^k-1), 2^{k-1})$. Thus, W_{k-1} satisfies assumptions similar to those of W_k, but with k replaced by $k-1$. We can continue this process, creating a chain of restricted wirings W_j and associated partition sets A_j consisting of the vertices in q copies of $\overline{K}_j$ and B_j of cardinality $N_{j-1} = q(2^j - 1)$ such that $W_{j-1} := W_{B_{j_1}} \in A(N_{j-1}, 2^{j-1})$, for $j = 0, \ldots, k$.

Since all $\overline{K}_j$s are obtained by (partial or full) pivoting, all vertices in any one $\overline{K}_j$ link to the same set of vertices. As in the discussion of V_k before this theorem, we may as well restrict to vertex press sets where we are only allowed to press a single *designated vertex* in each $\overline{K}_j$, and we say that $\overline{K}_j$ is *activated* if its designated vertex is pressed. We also talk about a $\overline{K}_j$ being *switched* if its designated vertex is one of the vertices given by a perturbation y of an existing vertex press set x, thus yielding a vertex press set $x + y$.

For $1 \le j \le k$, we know that the designated vertex in any one $\overline{K}_{j-1}$ links to 2^{j-1} vertices in A_j. By activating every $\overline{K}_{j-1}$, and then activating any $\overline{K}_j$s in which fewer than 2^{j-1} vertices are lit, we could light strictly more than $q2^j = \mu(N_j, 2^j)$ vertices in A_j if there were at least one $\overline{K}_j$ that had either strictly more, or strictly less, than 2^{j-1} lit vertices after every $\overline{K}_{j-1}$ had been activated. It follows that the links from any two different K_{j-1}s must be to distinct sets of vertices in A_j, and that these links must be evenly distributed, in the sense that there must be 2^{j-1} of them in each $\overline{K}_j$.

Suppose now that $1 < j \le k$. By activating every $\overline{K}_{j-2}$ and every $\overline{K}_j$, we light $q2^{j-2}$ vertices in A_{j-2} and the same number in A_{j-1}, and arguing as above we see that there must be exactly 2^{j-1} vertices lit in each $\overline{K}_j$. We can continue this argument to deduce inductively that any one vertex in $A_{j'}$ is linked to exactly 2^{j-1} vertices in A_j if $j \ge j'$, and to no vertices in A_j if $j < j'$. Furthermore there are links to 2^{j-1} vertices in any given $\overline{K}_j$ from designated $\overline{K}_{j'}$ vertices whenever $j' < j$.

We next prove that all of these $\overline{K}_j$s are arranged in V_ks. This is trivial if $k = 1$, since each $\overline{K}_0$ has only one link to A_1, and each $\overline{K}_1$ has a link from one of the $\overline{K}_0$s. Suppose inductively that all the A_js for $j \le k-1$ are arranged into q copies of V_{k-1}. We wish to prove the same with $k-1$ replaced by k.

We fix one particular $\overline{K}_{k-1}$, which we call L_{k-1} and, for each $0 \le j < k-1$, denote by L_j the copy of $\overline{K}_j$ that is linked to L_{k-1}. The sets L_j, $0 \le j \le k-1$ lie in a particular copy of V_{k-1} that we will call U_{k-1}. For each $0 \le j < k-1$, let x_j be the vertex press sets where we activate every $\overline{K}_{k-1}$ other than L_{k-1}, and we also activate L_j. By the properties of the V_{k-1}, this results in having 2^{k-1} vertices lit in each V_{k-1}, and some vertices in A_k are also lit as a result of the 2^{k-1} links from each $\overline{K}_{k-1}$ and from L_j into A_k. By then activating any $\overline{K}_k$ where fewer than half of the vertices are lit, we get at least $q(2^{k-1} + 2^{k-1}) = q2^k$ vertices lit in B_k, the maximum amount allowed.

But we would get strictly more than this if the vertex press set x_j resulted in any number of lit vertices other than 2^{k-1} in any A_k. Thus, x_j must result in $q2^{k-1}$ lit vertices in A_k, with exactly 2^{k-1} of these in each $\overline{K}_k$. But there are only 2^{k-1} links from each $\overline{K}_k$ or from L_j to A_k, so it must be that no two of these links are to the same vertex in A_k, since otherwise there would be fewer than $q2^{k-1}$ vertices lit in A_k as a result of x_j.

Consider more generally a vertex press set x where we press the designated vertex in $\overline{K}_{k-1}$ in all cases except L_{k-1}, and we also press the designated vertex in one or more of the sets L_j, $0 \le j \le k-1$. For all such x, we get 2^{k-1} lit vertices in each V_{k-1}, so again we must have $q2^{k-1}$ lit vertices in A_k, with exactly 2^{k-1} of these in each $\overline{K}_k$. Since we have seen that the links to A_k from U_{k-1} are disjoint from the links to A_k from every

$\overline{K}_{k-1}$ other than L_{k-1}, it follows that any nontrivial combination of activations of the sets L_j, $0 \le j \le k-1$ toggles the same number of vertices in each $\overline{K}_k$ and 2^{k-1} such vertices across the union all all $\overline{K}_k$s.

Denoting by L_k some particular $\overline{K}_k$ where nontrivial combination of activations of the sets L_j toggle at least one vertex, we assume the number of such toggles is M. Viewing our designated vertices in L_j as switches for $0 \le j \le k-1$, we now apply Lemma 5.3 and the fact that $1 \le M \le 2^{k-1}$ to deduce that $M = 2^{k-1}$. This uses up all the available links from U_{k-1} to A_k. Now U_{k-1} is a fixed but arbitrary V_{k-1}, so it follows that each V_{k-1} is linked only to a single $\overline{K}_k$, and so our full wiring consists of q copies of V_k, as required. □

6. The cases $m = 4, 5$

6.1. In this section, we prove Theorem 1.1. Throughout, an n-optimal wiring is a wiring $W \in A(n,m)$ for which $M(W,0) = \mu(n,m)$; the parameter m is in all such cases understood.

Proof of Theorem 1.1. Part (a) can be restated as $\mu(\cdot,p) = U(\cdot,p)$ for $p = 4,5$. It is readily verified from Theorem B(a) that $\mu(\cdot,p) = U(\cdot,p)$ when $p = 3$, so it extends to $p = 4,5$ by Theorem 5.2.

We now prove Part (b). The desired formula for $\mu^*(n,4) - 4k$, $n = 7k + i \ge 4$, is given by a_i in the following table:

i	1	2	3	4	5	6	7
a_i	2	2	2	4	4	4	4

It is readily verified that a_i equals the least even integer not less than $\mu(7k+i,4) - 4k$. Since pressing any vertex for a wiring in $A^*(n,4)$ preserves the parity of the number of lit vertices, $\mu(7k+i,4)$ must be even. Thus $\mu^*(n,4) \ge 4k + a_i$.

We now prove the converse by induction. The nontrivial part is to prove it for $4 \le n \le 10$. Once this is proved, it follows inductively for all $n = 7k + i > 10$ using (2.2.1):

$$\mu^*(7k+i,4) \le \mu^*(7(k-1)+i,4) + \mu^*(7,4) \le (4(k-1)+a_i) + 4 = 4k + a_i\,.$$

It remains to prove that $\mu^*(n,4) \le 4k + a_i$ when $4 \le n \le 10$. Trivially $\mu^*(4,4) = 4$ and

$$\begin{aligned}
\mu^*(5,4) &\le \mu^*(4,3) + 1 = 4 && \text{(Lemma F)}\,,\\
\mu^*(6,4) &\le 2\mu^*(3,2) = 4 && \text{(Lemma 3.1)}\,,\\
\mu^*(7,4) &= 4 && \text{(Theorem 3.3)}\,,\\
\mu^*(8,4) &\le \mu^*(7,3) + 1 = 6 && \text{(Lemma F)}\,,\\
\mu^*(9,4) &\le \mu^*(8,3) + 1 = 7 && \text{(Lemma F)}\,.
\end{aligned}$$

All except the last of these is sharp, and parity considerations allow us to improve the last one to the sharp $\mu^*(9,4) \le 6$.

Finally, $\mu^*(10,4) \le 6$ follows by consideration of the wiring

$$W_{10} = \begin{pmatrix} 1&0&0&0&0&0&0&0&0&0\\ 1&1&1&0&0&0&0&0&0&0\\ 0&1&1&0&0&0&0&0&0&0\\ 1&0&0&1&1&1&0&0&0&0\\ 0&1&1&1&1&1&0&0&0&0\\ 0&0&0&1&1&1&0&0&0&0\\ 1&0&0&0&0&0&1&1&1&1\\ 0&1&1&0&0&0&1&1&1&1\\ 0&0&0&1&1&1&1&1&1&1\\ 0&0&0&0&0&0&1&1&1&1 \end{pmatrix}$$

(cf. Figure 7 All columns except columns 1, 2, 4, and 7 are duplicates of these columns, so we can restrict ourselves to sets of vertex presses involving only these four vertices. With this restriction, we can proceed to list all sixteen possible values of x, and deduce that $M(W_{10},0) = 6$. □

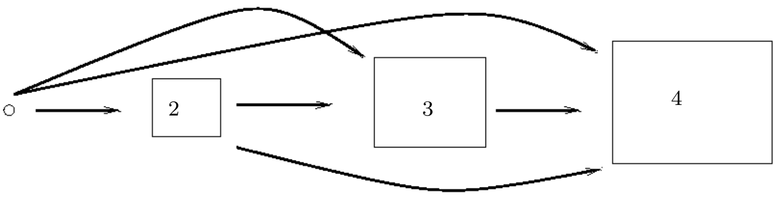


Figure 7. W_{10}

6.2. Let us mention an alternative, more instructive, way of proving that $M(W_{10},0) \le 6$. Again, we may restrict ourselves to pressing only some combination of vertices 1,2,4, and 7. Note first that W_{10} consists of one copy each of a $\hat{K}_1$, $\hat{K}_2$, $\hat{K}_3$, and $\hat{K}_4$ (vertices 1, 2–3, 4–6, and 7–10, respectively), and $\hat{K}_i$ is connected to $\hat{K}_j$ only if $i < j$. The subwiring for vertices 1–3 is such that we can never light all three vertices (by parity, since all vertices have degree 2), and to get only one unlit vertex, we must press vertex 1 and/or vertex 2. But all three of these possibilities throws both the $\hat{K}_3$ and $\hat{K}_4$ out of sync since the links from vertices 1 and 2 into the $\hat{K}_3$ are different from each other, and similarly for the links into the $\hat{K}_4$. Furthermore, the $\hat{K}_3$ and $\hat{K}_4$ vertices remain out of sync regardless of whether we press vertices 4, 7, or both. Thus, the unlit vertices always include either all of 1–3, or at least one vertex each from 1–3, 4–6, and 7–10. Thus, $M(W_{10},0) \le 7$ and parity considerations improve this to $M(W_{10},0) \le 6$.

6.3. Questions. So far, we know this:

Theorem 6.1. *For $m \in \mathbb{N}$, $m \le 5$, we have $\mu(\cdot,m) = U(\cdot,m)$.*

This naturally prompts the following question, which we cannot answer.

Question 6.2. *Is it true that $\mu(\cdot,m) = U(\cdot,m)$ when $m > 5$?*

Theorem 3.3 states that if m is a power of 2, then there exists wirings for $(n,m) = (2m-1,m)$ that are optimal in the sense that $\mu^*(n,m)$ and $\mu(n,m)$ both equal to $(n+1)/2$ (the smallest possible value for $\mu(n,m)$ according to Lemma D). This is evidence that powers of 2 are significant boundaries for the behavior of $m \mapsto \mu(\cdot,m)$ and $m \mapsto \mu^*(\cdot,m)$. This fact motivates the following pair of open questions with which we close the article. Note that the first one is simply a weaker version of Question 6.2.

Question 6.3. *Is it true that $\mu(n,m)$ is independent of m for all $2^k \le m \le 2^{k+1}-1$, $k \in \mathbb{N}$?*

The answer to the above question is affirmative if we restrict to $m \le 5$.

Question 6.4. *Is it true that $\mu(n,m_1) - \mu^*(n,m_2)$ is bounded independent of $n, k \in \mathbb{N}$ for all $2^k \le m_1, m_2 \le 2^{k+1}-1$, $k \in \mathbb{N}$?*

The answer to this last question is affirmative if we restrict to $m_1, m_2 \le 4$.

References

[1] A046699, The Online Encyclopedia of Integer Sequences, http://oeis.org/A046699.

[2] S.M. Buckley and A.G. O'Farrell, *Wiring switches to light bulbs.* Bulletin IMS 94 (2025) 69–88.

[3] B.W. Conolly, *Meta-Fibonacci sequences*, in S. Vajda, ed., Fibonacci and Lucas Numbers and the Golden Section, Wiley, New York, 1986, pp. 127–137.

[4] J. Conway, *Some Crazy Sequences*, Lecture at AT&T Bell Labs, July 15, 1988.

[5] C. Deugau and F. Ruskey, *Complete k-ary trees and generalized meta-Fibonacci sequences*, in Fourth Colloquium on Mathematics and Computer Science: Algorithms, Trees, Combinatorics and Probabilities, Discrete Math. Theor. Comput. Sci. Proc., Assoc. Discrete Math. Theor. Comput. Sci., Nancy, 2006, pp. 203–213.

[6] N.D. Emerson, *A family of meta-Fibonacci sequences defined by variable-order recursions*, J. Integer Seq. **9** (2006), Article 06.1.8.

[7] D.R. Hofstadter, *Gödel, Escher, Bach: An Eternal Golden Braid*, Basic Books, 1979.

[8] A. Isgur, D. Reiss, and S.Tanny, *Trees and meta-Fibonacci sequences*, Electron. J. Combin., **16** (2009), #R129.

[9] B. Jackson and F. Ruskey, *Meta-Fibonacci sequences, binary trees, and extremal compact codes*, Electron. J. Combin., **13** (2006), #R26.

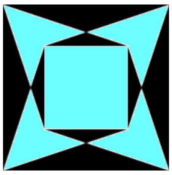
[10] N.J. Sloane. Library of Hadamard Matrices. http://neilsloane.com/hadamard/. Accessed 4 October 2024.

Stephen Buckley MRIA studied at UCC and Chicago, and worked at the University of Michigan before coming to Maynooth. He has been Head of the Department of Mathematics and Statistics since 2007. More at https://archive.maths.nuim.ie/staff/sbuckley/.

Anthony G. O'Farrell MRIA studied at UCD and Brown, and worked at UCLA before taking the Chair of Mathematics in Maynooth, where he served for 37 years and continues as Professor Emeritus. More at https://www.logicpress.ie/aof.

(Both authors) Department of Mathematics and Statistics, Maynooth University, Maynooth, Co. Kildare, W23 HW31, Ireland

E-mail address: stephen.m.buckley@mu.ie, anthony.ofarrell@mu.ie



Irish Math. Soc. Bulletin
Number 95, Summer 2025, 65– 67
ISSN 0791-5578

Tom Carroll: Geometric Function Theory: A Second Course in Complex Analysis, Springer, 2024. ISBN: 978-3-031-73726-8, GBP 39.99, 353+xi pp.

REVIEWED BY CHRISTOPHER J. BISHOP

What is geometric function theory (or GFT for brevity)? Saying it is the "geometric bits of function theory" sounds like an unhelpful rearrangement of the words. A little more precise is "the parts of mathematics that utilize the theory of conformal mappings in the plane or their generalizations to higher dimensions and metric spaces". A broader attempt would be "the study of mappings that distort geometry by only a bounded amount". However, perhaps it is safest to paraphrase US Supreme Court Justice Stewart's description of a different topic: "I know it when I see it".

Assuming I know geometric function theory when I see it, I will list several topics I consider to be part of, or very close to, GFT (a highly personal and debatable list).

- **Complex dynamics:** The Fatou set of a polynomial p is defined as the largest open set where the iterates of p form a normal family, a concept at the center of geometric function theory. The Julia set is the complement; the set where the iterates are "chaotic". Any non-linear polynomial introduces some geometric distortion, which we might expect to accumulate as we iterate p, but because the iterates of small disks are conformal (as long as they avoid critical points), the distortion remains uniformly bounded by Koebe's 1/4-theorem, another central pillar of GFT. This explains the approximately self-similar character of Julia sets and the importance of understanding the critical orbits. Approximation results, such as Runge's theorem, are often used to create examples with novel properties, and the connectedness of the Mandelbrot set follows from constructing the Riemann map onto its complement. Thus holomorphic dynamics incorporates many tools of GFT.
- **Hyperbolic manifolds:** The disk has a natural hyperbolic metric and the Schwarz lemma says that holomorphic self-maps of the unit disk, $\mathbb{D}$, are contractions for this metric, binding GFT tightly to hyperbolic geometry. By the uniformization theorem, most Riemann surfaces are of the form $R = \mathbb{D}/G$ where G is a discrete group of Möbius transformations acting on the disk (called a Fuchsian group). These are hyperbolic isometries of the disk, and they extend to a group of isometries on the hyperbolic upper half-plane (this is called a Kleinian group), giving a quotient that is a hyperbolic 3-manifold. Replacing the disk by others planar domains (usually with a fractal boundary) gives rise to other hyperbolic 3-manifolds. The study of such Kleinian groups and hyperbolic 3-manifolds is a rich mixture of GFT and topology, much of it inspired by the work of William Thurston.
- **Brownian motion:** A Brownian motion is a random continuous path in the plane (although it also makes sense in other dimensions). This seems firmly within real analysis and probability theory, but Brownian motion in a planar domain Ω is conformally invariant: it is mapped to another Brownian path by any conformal map on Ω. This means that theorems about the the first hitting distribution of Brownian motion on the boundary of a domain (called harmonic measure) can, in the simply connected

Received on 21-04-2025; revised 20-05-2025.
DOI: 10.33232/BIMS.0095.65.67.

case, often be reduced to results about the boundary behavior of conformal mappings $f : \mathbb{D} \to \Omega$. This allows the tools of GFT to be applied, often with spectacular results. For example, Makarov used this approach to prove that harmonic measure on simply connected domains is always 1-dimensional in a precise sense, even if the boundary of Ω is not, e.g., it is a fractal. Extending such results to higher dimensions has been daunting, but remarkable recent progress has occurred because of advances in harmonic analysis, PDE and geometric measure theory.

• **SLE:** A Brownian motion is allowed to intersect itself, but defining random Jordan curves (non-self-intersecting paths) is much harder, and was not successfully done until Oded Schramm invented SLE [Sch00] using random conformal maps. He applied a differential equation of Loewner (very classic GFT) using Brownian motion as data. Schramm called these "stochastic Loewner Evolutions" but they are now known as "Schramm-Loewner evolutions", and for the last twenty years SLE has been one of the hottest topics in mathematics and physics (several Fields medals for related work).

• **Traveling salesman theorem:** The classical traveling salesman problem (TSP) in computer science is to find the shortest path that visits each point of a given finite set, but there is also an analytical version that asks which infinite sets E can be visited by some finite length curve. Peter Jones [Jon90] defined an infinite series whose terms measure how close E is to lying on a straight line at different points and scales and proved that the shortest curve containing E has length bounded by a fixed multiple of this series. Jones's theorem has been extended to higher dimensions, Hilbert space and certain metric spaces, but his original proof was based on conformal maps and other basic tools of GFT, and has itself become a pillar of modern GFT with numerous applications to Julia sets, metric space analysis, Kleinian groups and Brownian motion.

Tom Carroll's book *Geometric Function Theory* does not deal directly with any of the applications of GFT mentioned above, but it does prepare a student for the study of all these topics by presenting many of the essential tools: spherical and hyperbolic geometry, normal families, the Riemann mapping theorem, Runge's approximation theorem, the distortion properties of conformal mappings (including Koebe's 1/4-theorem), Carathéodory convergence, and the uniformization theorem. Several of these topics can be found in other textbooks, though they are not generally covered in an undergraduate course. For example, the results on univalent functions and Carathéodory convergence are usually only found in more advanced books, such as [GM08] or [Pom92], and Carroll's book is an excellent preparation for reading these graduate level texts.

One non-standard example that caught my eye is Theorem 9.4, that says a Euclidean disk (which is obviously convex for the Euclidean metric) is also convex for the hyperbolic metric on any simply connected planar domain Ω containing D. This is a very pretty result of Jørgensen, and it is certainly a prototypical result of geometric function theory, but not one I have seen in a textbook before. Jørgensen's theorem follows a discussion of the differential equation $\Delta u = e^{2u}$ satisfied by the hyperbolic metric, another important topic not usually covered by a first course in complex analysis.

Another nice feature is the inclusion of Zalcman's lemma, along with more standard results about normal families, such as the theorems of Marty and Montel. Zalcman's lemma says that a family of holomorphic maps is not normal if we can extract a subsequence that has "blow-ups" that converge to a non-constant limit in a precise sense. The result is elementary, but extremely useful in holomorphic dynamics, but is not often included in introductory textbooks.

I do have a few minor quibbles. For example, conformal maps from the disk to a Jordan domain extend continuously to the boundary, but Carroll only proves this in a special case he calls "geometrically simple". A remark on page 175 gives the impression that this includes all Jordan domains, but this is not true; even a mild mannered fractal curve like the von Koch snowflake is not simple in the sense of Definition 6.4 (and much worse behavior is possible). Moreover, Carroll's proof takes eight pages, whereas the general case takes only two pages in [GM08] (assuming the Jordan curve theorem) and seven pages in [Mar19] (including a proof of the Jordan curve theorem).

There are 121 exercises, but I would have preferred even more. For example, the chapter on Runge's theorem has only three problems, and none utilize Runge's theorem itself. This is a pity, since Runge's theorem is a marvelous machine for generating unexpected examples, e.g., a sequence of polynomials converging pointwise on the plane to a discontinuous limit, a holomorphic function on the disk that has radial limits nowhere on the boundary, or a "universal" entire function whose translates can approximate any entire function. Learning Runge's theorem should include learning how to wield it.

A notable feature of Carroll's book is that it is carefully written, with plenty of discussion, motivation and extended explanations, in addition to the actual proofs; it has a conversational tone, and it is well suited for independent reading. This aspect is enhanced because it also contains introductions to many of the necessary parts of geometry and topology, as well as providing solutions to all the exercises. I recently taught complex analysis for first year PhD students, covering most of Marshall's more concise text [Mar19] in one semester, by assuming material from the parallel real analysis and topology classes. Several undergraduates attempted this class, but because of the rapid pace I set, only a few continued for the whole semester. In the future, I would recommend such students take our standard undergraduate complex variables course, followed by a reading course from Carroll's book. Such a plan would leave them well prepared to tackle books, papers or research projects in the areas mentioned earlier in this review. There are few (if any) books that fill the gap between the standard undergraduate material and more advanced texts as well as Carroll's book does. I am currently teaching a graduate course on quasiconformal mappings, and I recommended his book to any students needing to brush up on the essential prerequisites from classical GFT. It is a well organized, well written gateway to an enormous number of exciting topics in modern mathematics.

References

[GM08] John B. Garnett and Donald E. Marshall. *Harmonic measure*, volume 2 of *New Mathematical Monographs*. Cambridge University Press, Cambridge, 2008. Reprint of the 2005 original.

[Jon90] Peter W. Jones. Rectifiable sets and the traveling salesman problem. *Invent. Math.*, 102(1):1–15, 1990.

[Mar19] Donald E. Marshall. *Complex analysis*. Cambridge Mathematical Textbooks. Cambridge University Press, Cambridge, 2019.

[Pom92] Ch. Pommerenke. *Boundary behaviour of conformal maps*, volume 299 of *Grundlehren der mathematischen Wissenschaften [Fundamental Principles of Mathematical Sciences]*. Springer-Verlag, Berlin, 1992.

[Sch00] Oded Schramm. Scaling limits of loop-erased random walks and uniform spanning trees. *Israel J. Math.*, 118:221–288, 2000.

Christopher J. Bishop began his schooling (grades 1-3) in Shannon, Ireland and (somewhat later) received a bachelors degree from Michigan State University, did Part III at Cambridge University, and earned a PhD from the University of Chicago, advised by Peter W. Jones. He is currently Distinguished Professor of Mathematics at Stony Brook University, and was awarded the Senior Berwick Prize by the London Mathematical Society in 2024, for work in geometric function theory. Several of his favorite research interests are mentioned in the review.

Department of Mathematics, Stony Brook University
E-mail address: bishop@math.stonybrook.edu

Irish Math. Soc. Bulletin
Number 95, Summer 2025, 68– 69
ISSN 0791-5578

Susan M. C. Mac Donald: Euclid Transmogrified: A National Scandal, Logic Press, 2024. ISBN: 978-1-4461-5218-8, EUR 34.07/24.64 Hardcover/Paperback, 529+xvi pp.

REVIEWED BY BRENDAN MASTERSON

As the title suggests this book details a national scandal centred on Euclidean geometry in schools. Specifically, the book is concerned with changes to the geometry syllabus for the Inter. Cert. and later the Junior Cert. from the 1940s to the late 1980s and how these changes were influenced by the opinion of the Department of Education inspectorate rather than professional mathematicians and teachers. What is particularly surprising is the length of time these problems were allowed to persist across two syllabuses from the mid 1960s to the late 1980s with ramifications that extend to the present day.

Mac Donald has split the book into four sections: Setting, Phase One, Phase Two, and Aftermath. The first of these, Setting, places a recently independent Ireland in a changing world mathematically when it comes to geometry education. At the time Ireland was primarily promoting the education of the Irish language and had separate Intermediate Certificate mathematics for boys and girls, with the girls' syllabus called 'Elementary Mathematics (for girls only)' and of a lower standard than the 'Mathematics' syllabus for boys. I found this to be a very interesting and accessible introduction to the state of education in Ireland post-independence. Some aspects of this will be familiar to many readers but that does not detract from the book and undoubtedly there will still be something new for everyone.

At the time, an international debate was taking place about how to reform the mathematics syllabus in secondary schools. Some mathematicians endorsed models that sought to 'fix' Euclid such as Hilbert's axioms, whereas others sought to replace the geometry of Euclid with a linear algebra based approach. Georges Papy was a prominent figure in the latter movement.

The Phase One section of the book outlines how the Department of Education inspectorate reacted to these international developments and the policy of the government of the day. The resulting syllabus, which Mac Donald calls Syllabus II, had some positive aspects: it removed 'Elementary Mathematics (for girls only)', it ran at a lower and higher level ensuring girls had access to the more advanced material, while less able boys could take the lower level. This also happened at a time when secondary education became free to Leaving Certificate level, and a common Intermediate Certificate was introduced for secondary and vocational schools. However, for the geometry content of Syllabus II, the inspectorate developed a hybrid system where existing aspects of Euclid ran alongside parts of Papy's mathematics.

Syllabus II was met with a large number of teachers who were unfamiliar and unprepared to teach this new mathematics, while no textbook in English was available to teachers of Syllabus II until two years after its introduction. This resulted in a lot of confusion for teachers and for students.

Received on 05-06-2025; revised 09-06-2025.
DOI: 10.33232/BIMS.0095.68.69.

In Phase Two, Mac Donald outlines the development of Syllabus III. After seven years of Syllabus II, the Department of Education inspectorate decided to double-down on the use of Papy's mathematics in places, while also not following it entirely. Papy's mathematics seems to require being followed precisely or not at all. This led to a logically unsound mathematics syllabus with undefined terms and theorems that could not be proved from the course material. This happened against the protests of many university lecturers, most notably Prof. Anthony O'Farrell and Prof. Patrick Barry, who were quick to point out the flaws within Syllabus III. Yet despite all this, Syllabus III ran for fourteen years. This seems to be due to a concentration of power in the inspectorate when writing these syllabuses. The inspectors seemed to be confident in their ability to design a mathematical system by borrowing parts from several others. They did not recognise the flaws in their system, and were unwilling to listen to any dissenting voices from professional mathematicians when they pointed out these flaws. The inspectorate did not feel they needed to listen to these mathematicians because students sitting the Inter. Cert. were not going directly to university and these were therefore none of their concern.

The fact that this could happen in the first place and then persist for so long is, as Mac Donald states, a national scandal. The ramifications of these syllabuses are still being felt today with elements of them remaining in subsequent syllabuses and many of the teachers working today having themselves been taught with this flawed geometry.

The book is extremely well-researched. To support her work Mac Donald uses summaries of committee meetings, articles, conference reports, records from the Dáil, and interviews. These sources add a lot of colour to the argument. However, at times, particularly in the Phase One and Phase Two sections of the book, it can be difficult to keep track of the various timelines and organisations. For a book that provides a detailed history on a topic spanning about fifty years, this is probably inevitable. It is worth persevering through these periods as Mac Donald does tie things together in the end and she helpfully provides a list of all the abbreviations at the beginning of the book. The book is also nicely supplemented with appendices of the geometry syllabuses discussed and extracts from the various geometric models that were under consideration.

I think anyone with an interest in the history of secondary school education in Ireland would find this to be a good and insightful read.

Brendan Masterson is a senior lecturer in mathematics at Middlesex University. He received his PhD in computational group theory from the University of Galway. Since joining Middlesex he has also become interested in mathematics education.

Department of Design Engineering and Mathematics, Middlesex University
E-mail address: B.Masterson@mdx.ac.uk

Irish Math. Soc. Bulletin
Number 95, Summer 2025, 70– 72
ISSN 0791-5578

PROBLEM PAGE

J.P. MCCARTHY

Problems

Let us start with a thank you to all contributors, and then a call for more problems; at the moment the problem bank is running low.

The first of this edition's problems comes courtesy of Finbarr Holland of University College Cork.

Problem 95.1. Suppose p is a positive integer, and

$$u_n = \frac{p^{pn}\,(n!)^p}{(pn)!n^{(p-1)/2}}, \qquad (n = 1, 2, \ldots).$$

Prove that $(u_n)_{n\geq 1}$ is a strictly decreasing sequence, and determine its limit.

The second problem was sent in by Tran Quang Hung of the Vietnam National University at Hanoi, Vietnam. Given points X, Y in Euclidean space, the *ray* XY is the set of points Z satisfying $\overrightarrow{XZ} = t\,\overrightarrow{XY}$ for some $t \geq 0$. Similarly the *opposite ray* of XY is the set of points W satisfying $\overrightarrow{XW} = -t\overrightarrow{XY}$.

Problem 95.2. Let $\mathcal{A}$ be a regular polytope in n-dimensional Euclidean space $\mathbb{E}^n$ with $n \geq 2$. Let O be the centroid of $\mathcal{A}$, and $\mathcal{S}$ a hypersphere in $\mathbb{E}^n$ with O in its interior. Let $\{A_i\}_{i\in I}$ be the set of vertices of $\mathcal{A}$. For all $i \in I$, say ray OA_i meets $\mathcal{S}$ at B_i, and the opposite ray of OA_i meets $\mathcal{S}$ at C_i.

Prove that

$$\sum_{i\in I} |OB_i| = \sum_{i\in I} |OC_i|.$$

Finally a problem from Marian Uršarescu, "Roman–Vodă", National College, Roman, Romania. As standard, r and R denote the inradius and circumradius, respectively.

Problem 95.3. In ΔABC, show that:

$$\left(\frac{b}{c}+\frac{c}{b}\right)\cos^2\frac{A}{2}+\left(\frac{a}{c}+\frac{c}{a}\right)\cos^2\frac{B}{2}+\left(\frac{a}{b}+\frac{b}{a}\right)\cos^2\frac{C}{2}\leq\frac{3}{2}\left(\frac{R}{r}+1\right)$$

Received 15-06-2025
DOI: 10.33232/BIMS.0095.70.72.

Solutions

Here are solutions to the problems from *Bulletin* Number 93. In taking over from Ian Short, I may have inadvertently lost some solutions, my apologies if this is the case.

The first problem was solved by the North Kildare Problem Club.

Problem 93.1. Find a simple closed curve in the plane that does not have an inscribed regular pentagon.

Solution 93.1. Take the boundary T of a regular triangle. Suppose the regular pentagon P is inscribed in T. Since no three vertices of P are collinear, there must be at least two vertices of P on each of two sides of T, and hence the angle between two lines joining pairs of vertices of P must be a multiple of $\pi/3$. But in fact all such angles are multiples of $\pi/10$. □

The second problem was solved by Yagub N. Aliyev, of ADA University, Baku, Azerbaijan; and the North Kildare Problem Club. We provide the solution of Yagub:

Problem 93.2. Determine the least positive integer n for which a continued fraction

$$\cfrac{1}{b_1+\cfrac{1}{b_2+\cfrac{1}{b_3+\cdots+\cfrac{1}{b_n}}}}$$

has value ∞, where b_i are Gaussian integers each of modulus greater than 1.

Solution 93.2. $n = 1$ is impossible, because

$$\frac{1}{b_1} = \infty \iff b_1 = 0.$$

$n = 2$ is also impossible, because

$$\frac{1}{b_1 + \frac{1}{b_2}} = \infty \iff b_1 + \frac{1}{b_2} = 0 \iff b_1 b_2 = -1,$$

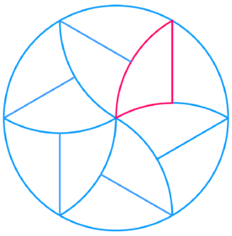
which implies that $|b_1 b_2| = 1$ but $|b_1 b_2| = |b_1| \cdot |b_2| > 1$, a contradiction.

$n = 3$ is possible, with, e.g. $b_1 = 1 + i$, $b_2 = -1 + i$, $b_3 = 1 + i$. □

The third problem was solved by Yagub N. Aliyev, the North Kildare Problem Club, and the proposer Andrei Zabolotskii of the Open University. Here is the solution of the Problem Club:

Problem 93.3. Dissect a disc into a finite number of congruent connected pieces (reflections allowed) in such a way that at least one piece does not contain the centre of the disc inside it or on its boundary.

Solution 93.3. If we represent the disc as the unit disc in the complex plane, the three edges of the piece NE of 0 (coloured red in the below figure) can be parametrized.



The long arc has length $\pi/3$ and is given by

$$1 + e^{it}, \text{ for } 2\pi/3 \leq t \leq \pi.$$

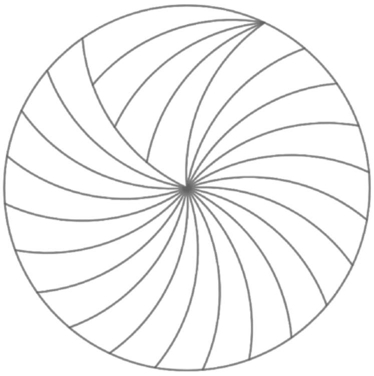
The short arc has length $\pi/6$ and is given by

$$e^{5\pi i/3} + e^{it}, \text{ for } \pi/2 \leq t \leq 2\pi/3.$$

The straight edge has length $\sqrt{3} - 1$ and is given by

$$e^{i\pi/3} - t, \text{ for } 0 \leq t \leq \sqrt{3} - 1.$$

For good measure, here is the construction of Yagub:



□

We invite readers to submit problems and solutions. Please email submissions to `imsproblems@gmail.com` in any format (preferably LaTeX). Submissions for the summer Bulletin should arrive before the end of April, and submissions for the winter Bulletin should arrive by October. The solution to a problem is published two issues after the issue in which the problem first appeared. If possible, please include solutions with your submissions.

Department of Mathematics, Munster Technological University

Instructions to Authors

Papers should be submitted by email to the address:

`ims.bulletin@gmail.com`

In the first instance, authors may submit a pdf version of their paper. Other formats such as MS/Word or RTF are not acceptable. The *Bulletin* is typeset using PDF files produced from LaTeX source; therefore, authors must be ready to supply LaTeX source files (and any ancillary graphics or other files needed) should their paper be accepted. Source files should be suitable for processing using `pdflatex`.

Once a paper is accepted in final form, the author(s) will be responsible for producing an output according to the *Bulletin's* standard layout. Standard template files for articles, abstracts and reviews, and the necessary class and style files may be downloaded from the IMS website `http://www.irishmathsoc.org`, or obtained from the editor in case of difficulty.

Since normally no proofs are sent out before publication, it is the author's responsibility to check carefully for any misprints or other errors.

The submission of a paper carries with it the author's assurance that the text has not been copyrighted or published elsewhere (except in the form of an abstract or as part of a published lecture or thesis); that it is not under consideration for publication elsewhere; that its submission has been approved by all coauthors and that, should it be accepted by the *Bulletin*, it will not be published in another journal. After publication, copyright in the article belongs to the IMS. The IMS will make the pdf file of the article freely available online. The Society grants authors free use of this pdf file; hence they may post it on personal websites or electronic archives. They may reuse the content in other publications, provided they follow academic codes of best practice as these are commonly understood, and provided they explicitly acknowledge that this is being done with the permission of the IMS.