Irish Mathematical Society
Cumann Matamaitice na hÉireann

Bulletin

Number 86 **Winter 2020**

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 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
Department of Mathematics and Statistics
Maynooth University
Co. Kildare W23 HW31

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/`

CONTENTS

EDITORIAL

Last year we revived the *News* item in the Bulletin, and invited the Irish Universities to report news to the end of November. Reports were received from just two institutions, and this year was no better. So we have decided to abandon this item. Information submitted may be incorporated here, as appropriate.

There seems to be a problem with the Bulletin item that lists the new PhD theses completed in the various Irish universities. Some administator took the view that this listing violates the EU General Data Protection Regulation. My view is that doctoral theses are among the most quintessentially-public objects known to man, as public and as open to criticism as the bus timetable. Be that as it may, we have rather few responses to the call for data. We continue the item for now, but will drop it if the present level of responses continues.

The reorganisation of the IT sector into Technological Universities is in progress. In Dublin, TUD was formed incorporating Blanchardstown IT, DIT and IT Tallaght. From January 2021, in Munster, MTU will unite CIT and IT Tralee. In prospect is a merger of IT Sligo, GMIT and Letterkenny IT to form another TU, and a similar merger of WIT and Carlow IT.

The 2021 Annual Scientific Meeting (aka the "September Meeting") will be hosted by UCC and MTU on 2–3 September 2021, with one day of activites at UCC and the second on the Cork campus of MTU. The 2020 meeting was deferred due to COVID, and took place on 12-14 January 2021, hosted by DCU. We've taken advantage of a production delay to squeeze in the report in this Winter 2020 Bulletin. I have to apologise for my lapse of attention that resulted in misreporting of the sequence number of these meetings for some years. I failed to check that the number was incremented each year, and an inspection reveals that we have had two each of the 28th meeting, the 27th meeting, and the 26th meetings! Thus we shall never have a 30th, a 31st, or a 32nd meeting. I am grateful to Brien Nolan for correcting this error. One can but hope that the news will not result in rioting members demanding back their missing meetings, in the spirit of the rioters of 1750, when Britain adopted the Gregorian calendar.

JP McCarthy of CIT (now MTU) reports: "Our esteemed colleague and friend Hannah Lordan retired from the Department of Mathematics after over 40 years of service to the institute. Hannah has been a stalwart of Cork IT and her experience, dedication, honesty, kindness and personality will be greatly missed by both staff and students of the institute."

This issue includes two letters received. These are from JP McCarthy, about an interesting initiative at his Department, and from our outgoing President, Pauline Mellon, about the gender gap.

Two of the four 2020 conferences supported by the society were postponed due to the epidemic. We include reports from those two and reports from three 2019 conferences that came to hand too late for the last Winter issue. We remind organisers and other contributors that the normal deadline for submissions is 15 December for the Winter issue and 15 May for the Summer issue.

Natalia Kopteva, reporting on the Numerical Method Workshop hosted by UL remarks: "This workshop was the 17th in a sequence of annual workshops, but the 1st to be held online instead of physically. Its success opened our eyes to the possibility of organising

talks by speakers located in any part of the globe. Thus, in collaboration with other Irish researchers, we have now created the (virtual) **Irish Numerical Analysis Forum**[1] which will include fortnightly seminars in all areas of numerical analysis that are aligned with the interests of the Irish numerical analysis community. Its aim will be to solicit lectures from leading international numerical analysts who will discuss their research area in a style that is accessible to most numerical analysts (i.e., not just those who are already familiar with the subject of the lecture)." This is just one example of the way the COVID-19 epidemic has accelerated the use of the web for education and collaboration. Clearly, the whole academic community has undergone a phase change.

Despite the difficulties, the International Mathematical Olympiad for 2020 was held in late September. The next IMO is scheduled for 14-24 July 2021 in St. Petersburg.

As before, to facilitate members who might wish to print the whole issue, the website will carry a pdf file of the whole Bulletin, in addition to the usual pdf files of the individual articles. As a further convenience (which may suit some Departments and Libraries), for a limited time a printed and bound copy of this Bulletin may be ordered online on a print-on-demand basis at a minimal price[2].

Links for Postgraduate Study

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

DCU: mailto://maths@dcu.ie
DIT: mailto://chris.hills@dit.ie
IT Sligo: mailto://creedon.leo@itsligo.ie
IT Tralee:
http://www.ittralee.ie/en/CareersOffice/StudentsandGraduates/PostgraduateStudy/
NUIG: mailto://james.cruickshank@nuigalway.ie
MU: mailto://mathsstatspg@mu.ie
QUB:
http://web.am.qub.ac.uk/wp/msrc/msrc-home-page/postgrad_opportunities/postgrad_opportunities_2020_additional/
TCD: http://www.maths.tcd.ie/postgraduate/
UCC: http://www.ucc.ie/en/matsci/postgraduate/
UCD: mailto://nuria.garcia@ucd.ie
UL: mailto://sarah.mitchell@ul.ie

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

Editor, Bulletin IMS, Department of Mathematics and Statistics, Maynooth University, Co. Kildare W23 HW31, Ireland.
E-mail address: ims.bulletin@gmail.com

[1] https://staff.ul.ie/natalia/node/1210
[2] Go to www.lulu.com and search for *Irish Mathematical Society Bulletin*.

Letters to the Editor

The Lee Fields Medal
A CIT Mathematics Competition
From J.P. McCarthy

Introduction. Save for a Higher Diploma and a Masters in Data Science & Analytics, the Department of Mathematics at Cork Institute of Technology is primarily in the business of service teaching, with the mathematics taught taking an applied and sometimes even vocational slant. However for a number of years the Department has offered a module — MATH6028 Mathematical Explorations — (conceived by Michael Brennan) that students can take as a free choice elective. As can be seen from the module descriptor:

> *The objective of this module is to capture the beauty and power of mathematics through various explorations,*

this module provides the CIT student with something very different to their programme-aligned mathematics modules. Mathematical Explorations runs in both Semesters I and II, and is always enrolled to capacity. The ongoing popularity of Mathematical Explorations proves that there is an appetite amongst CIT students for more mathematics, mathematics for enjoyment.

The other side of the coin is that there can sometimes be a feeling within our department, and perhaps further afield in the IoT sector in general, that while we (rightfully) expend a lot of our energy on student retention, and on those struggling, that perhaps some of our students that are more interested and more capable in mathematics might be missing out on some attention.

For these reasons, the CIT Department of Mathematics established a mathematics competition, open to all currently registered CIT students. Called the Lee Fields Medal, the contest consists of a paper of ten questions, based on mathematics no more advanced than Ordinary Level Leaving Certificate Mathematics.

A Call-to-Arms. Are you lecturing mathematics in an Irish IoT? Do you feel some of your students would appreciate a similar outlet? Perhaps, and you don't necessarily need a local competition to do this, you would be interested in setting up an inter-IoT mathematics competition? If yes, please get in touch with J.P. McCarthy, `jeremiah.mccarthy@cit.ie`

Year One. The inaugural competition was held in October 2018, where 18 intrepid students sat the paper. An evening Software Development student, Damien Murphy, prevailed with a fine score of 83%. The toughest question on the paper was the Birthday Problem. Paschal Mullins, a first year student of Mechanical Engineering (Hons) was the only student to get full marks in that question, and went on to win the best first year prize with a score of 74%. The paper also contained questions designed to try and get students to think a little harder. Consider the following question:

> *A piece of wire 10 m long is cut into two pieces. One piece is bent into a square and the other is bent into an equilateral triangle. How should the wire be cut so that the total area enclosed is maximised?*

Quite a number of students proffered what might be called a Pavlovian solution, immediately cutting the wire into lengths of x and $10 - x$, finding an expression for the total area as a function of x, setting the derivative equal to zero, and declaring that the maximum...

Given that the students would attend a Results & Solutions Night afterwards, we were also in a position to, e.g., explain (and correct) the logical error of answering:

> *Professor Oldie does not believe in calculators. You have to prove it to him on paper, using mathematical considerations, that*
>
> $$\sqrt{10} > \sqrt{2} + \sqrt{3}.$$
>
> *You may not use approximations nor your calculator,*

by assuming the proposition and deriving a true statement.

Year Two. In October 2019 the competition returned, and 25 students took the paper. The winner of Best First Year in 2018, Paschal Mullins, returned and with 83% took down the title. On this occasion the toughest and second toughest questions were the geometry questions, and Shane Allen, a third year Level 7 Mechanical Engineering student was the only entrant to get full marks on both questions. To encourage more Level 7 students to enter, we added a Best Level 7 prize, and Shane won this award to go with the honour of cracking the two geometry problems. A first year computer science student, Yi Ming Tan, came second overall with a mark of 79%, and so the Best First Year student went to the next highest ranked first year, Sofia Dolera Perez, an Electronic Engineering (Hons) student with a score of 70%.

There was some controversy when a student took issue with an (unintentionally) ambiguous Monty Hall Problem:

> *In a game show you have to choose one of three doors. One conceals a new car and the other two contain angry lions who will attack you. You choose but your chosen door is not opened immediately. Instead the presenter tells you that another door (which you have not picked), contains a lion. You then have the opportunity to change your mind. Is there any benefit to doing so? Justify your answer.*

Once again we saw evidence of students trained to 'react' to questions rather than think, with very few writing down the one line solution to:

> *Suppose that m and c are constants. What is the equation of the tangent to the graph $y = mx + c$ at $x = 1$?*

We also saw some inventiveness. The following question was answered very easily by those with Higher Level Mathematics (and with a bit of work by those without):

> *If you expand*
>
> $$(1 + x)^{2019} = a_0 + a_1x + a_2x^2 + a_3x^3 + \cdots + a_{2019}x^{2019},$$
>
> *what is the coefficient of x^2, a_2?*

One student gave a lovely solution, differentiating both polynomials twice, and evaluating at $x = 0$.

See `https://mathematics.cit.ie/let_s-do-maths` for the 2018 and 2019 papers.

Organisation. The competition is organised in a collaborative manner by an organising committee (OC). A bank of questions in ten categories has been developed, and there is an annual call to departmental colleagues to submit further questions. The competition is held relatively early in Semester I, with students invited via an "all-students" email.

The paper is chosen democratically, with two rounds of voting. First the OC each pick three questions from each category, and then the two top-voted questions are ran off against each other in a second vote. On the night the students receive a pack containing instructional cover sheet, question paper, ten answer sheets, and formula booklet. We also use the opportunity to advertise elective modules run by the department with a brochure.

Key to the process are the answer sheets: only one question per sheet, and this makes the process of divvying up the corrections very straightforward. Members of the OC each mark two or three questions, and submit marks to an online spreadsheet. Two weeks after the students sit the paper, we have a Results & Solutions night where the prizes are presented. Furthermore, on the night of CIT Faculty of Engineering and Science Awards, the winner is presented with a rather fetching gold medal, suitably inscribed with Euler's Identity.

FIGURE 1. Paschal Mullins, 2nd Year Mechanical Engineering (Hons), receiving the Lee Fields Medal at the CIT Faculty of Science and Engineering Awards from J.P. McCarthy (left) and HoD David Goulding (right).

The Lee Fields Organising Committee:
Dr Michael Brennan: michael.brennan@cit.ie
Dr David Goulding: david.goulding@cit.ie
Dr Seán Lacey: sean.lacey@cit.ie
Dr J.P. McCarthy: jeremiah.mccarthy@cit.ie
Dr Violeta Morari: violeta.morari@cit.ie
Dr Catherine Palmer: catherine.palmer@cit.ie

J.P. McCarthy
Mathematics Department, CIT
Received 16-6-2020
Jeremiah.McCarthy@cit.ie

Reducing the Gender Gap in the Mathematical Sciences
From Pauline Mellon

Gender gaps are ubiquitous. The gender pay gap in 2017 in Ireland was 14.4%, equivalent to women effectively working from November 9th until year end for free, relative to their male counterparts [1]. A gender pensions gap in Ireland sees the average weekly value of a man's pension more than 54% higher than a woman's [2].

Although it is hardly surprising, therefore, that there is a gender gap in higher education in Ireland, the scale of it may shock. In 2003-2004, across all Irish universities, women comprised 62% of our postgraduate students but only 8% of our professors, with a broadly similar pattern in our Institutes of Technology [3]. The situation surprised the authors of a recent HEA report into gender equality in higher education in Ireland, as its executive summary states "the Expert Group developed recommendations which they themselves would not have believed necessary at the beginning of this process. However, given the current situation and the international evidence which demonstrates that progression towards gender equality is not automatically linear or inevitable, ambitious and radical recommendations for all key stakeholders are essential"[3].

The wide gender gap in higher education only worsens if you move to the STEM areas of Science, Technology, Engineering and Mathematics [4]. My guess is that it may be even worse in mathematics than in STEM generally, at least in Ireland.

Nonetheless, one might hope that those resilient women who persist and succeed in STEM would flourish, after completing degrees and PhDs and postdocs to get full-time employment as scientists in the STEM area. A recent article in Nature suggests otherwise [5]. Its authors state that "STEM work is often culturally less tolerant and supportive of caregiving responsibilities than other occupations, so mothers - and fathers - may feel squeezed out of STEM work and pulled into full-time work in non-STEM fields". It reports, from a US study, that while 23% of men employed as full-time scientists in the STEM area leave STEM after their first child, the figure for women is almost double that. In other words, almost half US female scientists leave full-time science after their first child. STEM, it seems, is significantly less parent friendly overall than other employment sectors.

The culture in academia is no different in Ireland. Lynch [6] argues that there is a long history in higher education generally of a culture of 'carelessness', that is, being free from the work of having to take care of others. She states that the recent new managerialism in higher education has only exacerbated this endemic culture of carelessness, according it almost a moral status and that "given the moral imperative on women to do care work, [7], and on men to be care-less, the carelessness of higher education has highly gendered outcomes".

Let me illustrate this culture of carelessness. At drinks the night before a conference, I joined a group laughing as someone recounted another's tale of how an invited seminar speaker from abroad had the audacity to ask if she could bring her mother and baby with her. I, however, recognized the story as referring (unbeknownst to the raconteur) to myself, my breast-fed newborn and my own lovely mother. My offer to pay my mother's expenses wasn't part of the amusing tale, nor was the fact that the invitation had been withdrawn. While that baby his now an adult, not enough has changed in the culture of academe.

We must do better. A project 'A global approach to the Gender Gap in Mathematical, Computing and Natural Sciences', initiated and led by the International Mathematical Union's (IMU) Committee for Women in Mathematics, and funded largely by the International Science Council, has produced a short and easily implementable list of

recommendations: just four recommendation for 'instructors and parents', seven for 'local educational organisations' and ten for 'scientific unions'. Simple recommendations, such as 'take care of the issues of families attending with children' and 'put a budget in place to offer childcare solutions', might have spared my humiliation in the above encounter had they been in place. Others are surprisingly basic, such as, 'track who you are engaging in class to ensure that every student has a chance to participate and that girls feel comfortable in speaking up'.

This gender gap in our own mathematical sciences community in Ireland is something we should act quickly to close. There is evidence that it has, surprisingly, already been largely eliminated for students at second level [8]. Let's work together to reduce the gender gap in mathematics and STEM in Ireland by immediately implementing the IMU recommendations [1].

1: O'Halloran, M., Irish Times, Nov 8, 2020, 'Irish women are essentially working for free for rest of year due to pay gap, campaign says'. Also `equalpay.ie`

2: Nolan, A., Whelan, A., McGuinness, S., Matre, B., 'Gender, pensions and income in retirement', ESRI Research Series, September 2019.

3: Report of the Expert Group: HEA National Review of Gender Equality in Irish Higher Education Institutions, 2016, Figure 7 page 32 and Figure 11 page 36.

4: Clancy, P., 2001, 'College Entry in Focus: A Fourth National Survey of Access to Higher Education', Dublin: Higher Education Authority.

5: Nature, News, February 2019 'Nearly half of US female scientists leave full-time science after first child'.

6: Lynch, K., 'Carelessness: A hidden doxa of higher education', Arts and Humanities in Higher Education, 2010, (9), 1, 54-67.

7: O'Brien, M. (2007) 'Mothers' emotional care work in education and its moral imperative', Gender and Education 19(2): 159-77.

8: Lyons, M., Lynch, K., Close, S., Sheerin, E., Boland, P, 2002, 'Inside Classrooms'. Institute of Public Administration.

Pauline Mellon
School of Mathematics and Statistics
University College Dublin
Received 3-1-2021
pauline.mellon@ucd.ie

---

[1]Editor: A copy of the document listing these recommendations may be downloaded from the project website `https://gender-gap-in-science.org/`. By kind permission of the IMU, you may also download it from the IMS website at `http://irishmathsoc.org/bull86/resources/IMU.pdf`.

NOTICES FROM THE SOCIETY

Officers and Committee Members 2020

President	Dr Pauline Mellon	UCD
Vice-President	Dr Tom Carroll	UCC
Secretary	Dr D. Malone	Maynooth University
Treasurer	Dr C. Kelly	UCC

Prof S. Buckley, Dr L. Creedon, Dr R. Flatley, Dr D. Mackey, Dr M. Mathieu, Dr R. Ryan, Dr H. Smigoc, Dr N. Snigireva .

Officers and Committee Members 2021

President	Dr Tom Carroll	UCD
Vice-President	Dr Leo Creedon	IT Sligo
Secretary	Dr D. Malone	Maynooth University
Treasurer	Dr C. Kelly	UCC

Dr L. Creedon, Dr R. Flatley, Dr R. Gaburro, Dr D. Mackey, Dr M. Mathieu, Dr A. O'Shea, Dr R. Ryan, Dr H. Smigoc, Dr N. Snigireva .

Local Representatives

Belfast	QUB	Dr M. Mathieu
Carlow	IT	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	Dr B. Nolan
	TCD	Prof K. Soodhalter
	UCD	Dr R. Levene
Dundalk	IT	Mr Seamus Bellew
Galway	NUIG	Dr J. Cruickshank
Limerick	MIC	Dr B. Kreussler
	UL	Mr G. Lessells
Maynooth	MU	Prof S. Buckley
Sligo	IT	Dr L. Creedon
Tralee	MTU	Prof B. Guilfoyle
Waterford	IT	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	€200
Ordinary member	€30
Student member	€15
DMV, I.M.T.A., NZMS or RSME reciprocity member	€15
AMS reciprocity member	$20

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.

(3) 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$ 40.00.

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 of subscription.

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

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

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

(9) Please send the completed application form with one year's subscription to:

Dr Cónall Kelly
School of Mathematical Sciences
Western Gateway Building, Western Road
University College Cork
Cork, T12 XF62
Ireland

Deceased Members

It is with regret that we report the deaths of members:

Brian H. Murdoch, the Erasmus Smith Professor of Mathematics in TCD 1966–1989, died on 9 December 2020.

Patrick D. Barry, formerly the Professor of Mathematics at UCC, died on 2 January 2021.

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

PRESIDENT'S REPORT 2020

Committee Changes: The IMS committee had a change of Treasurer, with Goetz Pfeiffer (NUIG) being replaced by Cónall Kelly (UCC). Many thanks to the outgoing Treasurer for his years of excellent work in securing the Society's finances. I welcome Ronan Flatley (MIC), Ray Ryan (NUIG), Helena Smigoc (UCD) and Nina Snigireva (NUIG) to the committee and I thank Paul Barry (WIT), Rupert Levene (UCD), Anca Mustata (UCC) and James O'Shea (DCU) who left the committee after years of dedicated work to the Society.

IMS Bulletin: I extend the Society's continuing thanks to Tony O'Farrell for his work as Editor of the Bulletin and I also thank the editorial board of the Bulletin. We are also grateful to Michael Mackey for his considerable work in managing the Society's webpages.

IMS meetings: The Society's 2020 annual "September Meeting", which was scheduled to take place in Dublin City University, August 27-28, 2020 was, like countless other events, postponed due to the coronavirus pandemic. It will now take place online January 13-15, 2021, with sessions on Wednesday and Thursday afternoon (1.30pm - 5pm) and Friday morning (9.30am-12.30pm). A number of the talks are linked by the theme of epidemiological and environmental modelling. Sincere thanks to Brien Nolan and Niamh O'Sullivan for organising this conference under challenging circumstances and to DCU for hosting.

The Society's 2021 annual conference is due to take place in Cork, hosted by UCC and MTU. Many thanks to Cónall Kelly and J.P. McCarthy for stepping in to organise the 2021 conference at short notice.

IMS Conference Support: Due to the Covid-19 pandemic, there were no requests for conference support in 2020. Thanks to our treasurer, Cónall Kelly, for managing our finances.

Other: The European Mathematical Society 'Meeting of Presidents' due to be held at CIRM, Luminy, Marseille on March 14-15, 2020 was cancelled, days beforehand, due to the coronavirus pandemic.

International Mathematical Union: The Royal Irish Academy communicated in late 2019 that it would no longer fund Ireland's participation in the International Mathematical Union (IMU) for 2020 or thereafter. The committee of the Irish Mathematical Society therefore agreed that the Society should take over as the adhering body for Ireland to the International Mathematical Union. This transfer was completed in late February 2020. While a process of seeking private sponsorship had begun, it had to be postponed due to the Covid-19 pandemic and lockdown. Contact made with the then Minister for Education, Joe McHugh, during months of a long government formation process, was unproductive. The Society therefore had to seek emergency funding for Ireland's 2020 IMU membership fees of €2,860. We are sincerely grateful to the following institutions and their directors for their immense generosity in contributing to Ireland's 2020 IMU Fees, which were paid in September 2020:

- The Boole Centre for Research in Informatics at UCC and Prof. John Morrison;
- The Hamilton Mathematics Institute at TCD and Prof. Samson Shatashvili;
- The Maynooth Hamilton Institute at MU and Prof. Ken Duffy;
- The SFI Connect Research Centre at Waterford IT and Prof. Brendan Jennings;
- The Department of Mathematics and Statistics at UL and Professors James Gleeson and Sarah Mitchell;
- The School of Mathematics and Statistics at UCD and Prof. Ted Cox;
- The Irish Mathematical Society.

The Society aims to seek more sustainable funding, ideally from government, for the longer term.

Closing Comments: I feel immensely privileged to have served as President of the Irish Mathematical Society; even more so, to have served as the first woman President. I sincerely thank the members of the Society for this opportunity. I am grateful to my fellow officers, David, Tom and Cnall, and earlier Goetz, and the rest of the committee for their support and co-operation.

I am delighted to leave behind a committee for 2021 that is almost gender balanced, with five women to seven men. I welcome to the 2021 committee, Romina Gaburro (UL), Ireland's contact for 'European Women in Mathematics' and also Ann O'Shea (MU), who will chair our newly established 'Irish Committee for Mathematics Education', which comprises more women than men. I am proud that the Society has endorsed an open letter from 'European Women in Mathematics' on 'Corona Crisis: Impact on junior and women mathematicians' and also of the multi-institutional Athena Swan initiative in the mathematical sciences being led by Niall Madden of NUIG. These are all welcome trends that I hope will continue.

Pauline Mellon,
December, 2020.
E-mail address: pauline.mellon@ucd.ie

IRISH DOCTORATES COMPLETED

The following are the names and thesis titles for PhD degrees in Mathematics completed at Irish universities in the period from April 2019 to March 2020, inclusive. Departments are requested to send the information for each year to the end of March to the editor at the address below.

DCU:
Vasiliki Pitsia. Investigating high achievement in mathematics and science in Ireland: An in-depth analysis of national and international assessment data.

IT Sligo:
Kieran Hughes. Derivations of Group Algebras with Applications.

UCD:
Conor Finnegan. Projective Characters of Extra-Special and Metacyclic p-Groups and Other Related Topics.
Emma Howard. Learning Analytics and Mathematics Education: Complementary Approaches to Supporting Non-Specialist Students at Undergraduate Level
Jelena Janjic. Wave Energy Resource Of The Northeast Atlantic Ocean
Keefe Murphy. Beyond the Standard Mixture Model: Novel Families of Parsimonious Model-Based Clustering Methods
Daniela O'Hara. The Elliptic Curve Discrete Logarithm Problem and Systems of Polynomial Equations
Shane Walsh. Finite-amplitude phenomena in wave turbulent systems

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

Minutes of the Irish Mathematical Society Annual General Meeting held on December 11, 2020 on Zoom (due to Covid)

Present: C. Boyd, S. Buckley, M. Bustmante, A. Carnevale, T. Carroll L. Creedon, A. Cronin, S. Dineen, N. Dobbs, R. Flatley, R. Gaburro, E. Gill, J. Granell, C. Kelly B. Kreußler, G. Lessells, P. Lynch, D. Mackey, M. Mackey, N. Madden, D. Malone, M. Manolaki, M. Mathieu JP. McCarthy, A. McCluskey, P. Mellon, A. O'Farrell, M. O'Reilly, A. O'Shea, C. O'Sullivan, K. Pfeiffer, R. Quinlan, M. Roosbon, M. Rosbotham, T. Rossman, R. Ryan, N. Snigireva, H. Šmigoc.

(1) **Minutes**
Minutes of the last meeting, as in the bulletin, were accepted.

(2) **Matters Arising**
All matters will come up later.

(3) **Correspondence**
- We received a message about the open letter written by the European Women in Mathematics group regarding treatment of untenured mathematicians, women and parents during the Covid crisis. The letter had already been signed by a number of societies, and the committee had decided to sign the letter also.
- The EMS have requested news items from members. Items can be sent to the president.

(4) **Membership Applications**
Four new members had been approved: H. Akyamba, R. Neururer, K.C. Chim and M. Kerin.

(5) **President's Report** The president gave a summary of her report (the full report is included in the bulletin).

(6) **Treasurer's Report**
A report on finances was virtually circulated. Printing costs are now low. We had also supported awards for tutors organised by the Irish Mathematics Learning Support Network. The Irish subscription to the IMU had been paid using a combination of donations and the society's own resources. The society was also going to place some funds in saving certificates. Thanks was extended to the treasurer and local reps.

(7) **International Mathematical Union**
As described in the editorial of the summer bulletin, the Royal Irish Academy withdrew from paying Ireland's subscription late in 2019. The IMS had decided to act, in order to prevent membership from lapsing and became the adhering body.

The committee had begun to seek private sponsorship to cover the subscription, but the Covid lockdown had interrupted this process. As an interim measure, the committee approached a number of the mathematical research centres and departments in the country and was lucky to receive support. The committee extended its thanks to The Boole Centre for Research in Informatics at UCC (Prof. Morrison); The Hamilton Mathematics Institute at TCD (Prof. Shatashvili); Hamilton Institute at MU (Prof. Duffy); SFI Connect Research Centre (Prof. Jennings); The Department of Mathematics and Statistics at UL (Prof. Gleeson and Dr. Mitchell); The School of Mathematics and Statistics at UCD (Prof. Cox). With this support, the committee was able to cover the subscription for this year. However, the committee are seeking a longer term solution and are contacting the government in this respect.

(8) **Scientific Meeting**
The September meeting had been moved to January and will take place virtually in DCU, thanks to B. Nolan and N. O'Sullivan. The 2021 meeting will take place in UCC and MTU, hosted by C. Kelly and J.P. McCarthy.

(9) **Bulletin**
The bulletin is operating well. As always, the bulletin welcomes good material, including papers, surveys, reviews and book reviews. Departments are encouraged to submit news, including new staff members and graduating students.

(10) **Educational Subcommittee**
The previous education subcommittee had been dissolved after five years of operation, and members of the subcommittee had been thanked for their service. New terms of reference had been drawn up, and the new committee will be the Irish Committee for Mathematics Education. A. O'Shea had been invited to chair. Expressions of interest had been sought for membership. The new committee will start its work in January.

M. O'Reilly welcomed the new committee, and noted that the name should be presented so that it is clear that it is a subcommittee of the IMS.

(11) **Elections**
P. Mellon, T. Carroll, S. Buckley and D. Mackey have reached the end of their terms. Both T. Carroll and D. Mackey are happy to run again and we had received additional nominations for A. O'Shea and R. Gaburro. All were elected unanimously, with T. Carroll serving as the new president and L. Creedon serving as the new vice-president.

(12) **AOB**

- E. Gill extended thanks to all outgoing committee members. A. O'Farrell extended particular thanks to P. Mellon who had moved quickly to ensure continuity of Ireland's membership of the IMU. These thanks were echoed by many members.
- P. Mellon noted that, though she hadn't though much about it in advance, she had been the first woman president of the IMS, and that the good geographical and gender representation was present on all committees. M. O'Reilly noted that the society might be interested in the WITS organisation.
- J. Granell thanked A. O'Farrell for his role in chairing the outgoing education subcommittee.
- P. Mellon thanked A. O'Farrell and M. Mackey for looking after the bulletin and the website. Thanks was also extended to N. Madden who was coordinating a group of IMS members interested in AthenaSWAN and who had recently submitted a proposal to the HEA to collect pertinent statistics.

David Malone
david.malone@mu.ie

IMS Annual Scientific Meeting 2020
Dublin City University

January 13th-15th

The 33rd annual scientific meeting of the society - the 2020 September meeting - was hosted by the School of Mathematical Sciences, Dublin City University. Due to the disruption to normal academic activity caused by the Covid-19 pandemic, the meeting was held in January 2021 and took place online. The organisers were Brien Nolan and Niamh O'Sullivan, supported by the School administrators, Karen O'Shea and Bernadette Feeney.

Opening welcome remarks were made by Niamh O'Sullivan and by Tom Carroll, the incoming President of the IMS.

The meeting consisted of a mixture of short and long talks on a wide variety of mathematical topics, with speakers from across Ireland and from the UK. Talks took place over three sessions of four talks each, on the afternoons of Wednesday 13th and Thursday 14th January, and on the morning of Friday 15th January. A full list of talks is given below. Acknowledging the contribution of mathematicians to research on the global pandemic, a number of talks were dedicated to epidemiological modelling.

This year's meeting included a competition for research students who were invited to submit a short video recording of a presentation on their research. The submissions were of a very high quality, and the judges (incoming and outgoing IMS presidents Tom Carroll and Pauline Mellon) selected the following as winner and runner-up respectively:

Giuseppe Cotardo (UCC)
- *Tensor Decomposition in Coding Theory.*

Jason Curran (UL)
- *Diffuse Optical Tomography.*

The web page for the meeting, which includes abstracts and slides of presented talks, as well as the submissions to the research student competition, is available at

`https://www.dcu.ie/maths/ims-september-meeting-2020`

The organisers are grateful to all who participated in the meeting, and we are especially grateful to our speakers whose lectures were given in the following sequence. The number of participants seems not to have been significantly depleted relative to previous years due to the migration to an online setting. This proved an adequate substitute for a face-to-face meeting, but we will welcome the return to the traditional format at the 2021 meeting due to be jointly hosted by UCC and MTU on 2nd-3rd September.

Wednesday 13th January

Robert Heffernan (MTU/CIT)
- *Cayley's Theorem Revisited: Embeddings of Small Finite Groups.*

Rossen Ivanov (TU Dublin)
- *Mathematical Models for Internal Ocean Waves Interacting with Currents.*

James Gleeson (UL)
- *Differential Equations Modelling and Covid-19.*

Arundhathi Krishnan (University of Waterloo/UCC)
- *Markovianity and the Thompson Monoid F^+.*

Thursday 14th January

Paul Razafimandimby (DCU)
- *On the Strong Solutions to the 2D Stochastic Ericksen-Leslie System: a Ginzburg-Landau Approximation Approach.*

Áine Byrne (UCD)
- *Elimination Versus Mitigation: What's the Optimal Strategy for Controlling Covid-19?*

Niamh Cahill (MU)
- *A Bayesian Statistical Model for Recontructing and Analysing Former Sea Levels.*

Déirdre Hollingsworth (University of Oxford)
- *Trade-offs in Covid-19 Interventions.*

Friday 15th January

Merrilyn Goos (UL)
- *Meeting the Challenge of Teaching Mathematics 'Out of Field': the Professional Diploma in Mathematics for Teaching.*

Angela Carnevale (NUIG)
- *Growth in Nilpotent Lie Rings.*

Clifford Gilmore (UCC)
- *Dynamics of Weighted Composition Operators on Fock Spaces.*

Martin Mathieu (QUB)
- *Characterising Jordan Homomorphisms.*

Report by B. Nolan (email: brien.nolan@dcu.ie)

Reports of Sponsored Meetings

Maynooth Conference in the History of Mathematics
1–2 August 2019, Maynooth University

This two day conference was a joint Irish History of Mathematics (IHoM) and British Society for the History of Mathematics (BSHM) Conference.

Day 1 focused on invited talks on a selection of mathematical texts from the Russell Library, it also featured a visit to the Russell Library to view their collections, which include works of Galileo, Copernicus, Fermat, and Newton, to name but a few.

Invited speakers who delivered a lecture were:

- Niccolò Guicciardini (University of Milan)
  On two early editions of Isaac Newton's mathematical correspondence and works: William Jones's *Analysis per quantitatum, series, fluxiones ac differentias* (1711) and the Royal Society's *Commercium epistolicum* (1713).
- Yelda Nasifoglu (University of Oxford)
  Clavius and Compass: Mathematics education in early modern Jesuit colleges.
- Catherine Goldstein (CNRS, Institut de mathématiques de Jussieu-Paris Gauche)
  Jean Prestet's *Elements of mathematics: algebra* as a basis for mathematics at the end of the 17th century.
- Boris Jardine (University of Cambridge)
  The Seven Ages of a Manual: Samuel Sturmy's *Mariner's Mirror* (1669), from conception to reception.
- Philip Beeley (University of Oxford)
  20 yeares spare hours in algebra. John Kersey's *Elements of that Mathematical Art* and its contemporary reception.
- Benjamin Wardhaugh (University of Oxford)
  Reading Euclid in the Maynooth collection.

The conference organisers have agreed a book deal with Birkhäuser which will focus on Day 1 contributions (including several from authors who could not attend). This is expected to be published in early 2021 as part of their *Trends in the History of Science* series.

Day 2 followed a format similar to previous IHoM conferences and served as IHoM5. There were ten talks, and full details including titles, abstracts and some of the presentations are available from `https://bit.ly/38HHkx6`.

Fifty-one individuals registered for the conference, though several other local people also attended.

The conference was supported by the BSHM, the Irish Mathematical Society (IMS) and Maynooth university (Library, Department of Mathematics and Statistics, and Research Office).

Conference Organisers were Dr Ciarán Mac an Bhaird and Dr. Philip Beeley, in collaboration with Barbara McCormack (Special Collections Librarian). Report by

Ciarán Mac an Bháird, Maynooth University
ciaran.macanbhaird@mu.ie

15th International Conference of The Mathematics Education for the Future Project
4–9 August 2019, Maynooth University

The Mathematics Education for the Future Project was founded in 1986 as an international non-profit body to encourage innovation in mathematics, statistics, science and computer education. Since 1999 there have been 15 conferences throughout the world culminating in the Maynooth Conference in August 2019, attended by 188 people from 31 countries.

The 13 sessions over five days at Maynooth were extremely productive, with over 130 workshops, short paper and long paper contributions. There were also peer reviewed conference proceedings.

The plenary keynote *Can Technology make a Difference to Mathematics Education?* was delivered by Douglas Butler of the ICT Training Centre (Oundle) in the UK. This keynote was accompanied by two workshops *Helping Statistical Education through Visualisation* and *Exploring Concepts through a friendly User-interface*.

Delegates also got an opportunity to join local (the Russell Library, the National Science Museum, Maynooth Castle) and slightly less local (Hill of Tara) tours. The Russell Library tours included an exhibition of old mathematical texts.

The conference was supported by the Autograph, Fáilte Ireland, the Irish Mathematical Society and World Scientific.

Local Organising Committee: Dr. Ciarán Mac an Bhaird (Chair), Dr Fiona Faulkner (Co-chair), Dr Mark Prendergast (Co-chair) and Dr. Niamh O'Meara. Conference Organising Committee: Dr. Alan Rogerson, Poland/UK and Mgr. Janina Morska, Poland.

Report by Ciarán Mac an Bháird, Maynooth University
ciaran.macanbhaird@mu.ie

CETL-MSOR Bringing together mathematics communities
5–6 September 2019, DCU

CETL-MSOR brings together those involved in mathematics, statistics and operations research teaching, learning and support in higher education in an annual conference to share and support good practice in the area. This year the conference focussed on enhancements based on reflective and evidence-informed practice in relation to the following themes:

- developing communities of learners in mathematics and statistics support within, and across, the disciplines,
- teaching specialist mathematicians,
- inclusive design for mathematics learning,
- supporting students on the transition into and out of higher education.

Approximately 125 delegates participated in the conference: these came from all over Ireland and the United Kingdom, with some travelling from as far away as Australia and the United States. The conference had never taken place in Ireland before, although many Irish delegates have travelled to it in previous years. The keynote talks were:

- *The development of the mathematics and statistics support community: an objective, subjective, pragmatic and theoretical reflection* by Prof. Duncan Lawson, Coventry University,

FIGURE 1. Keynote speakers Duncan Lawson, Alice Rogers and Joe Kyle together with Eabhnat Ní Fhloinn (organising committee Chair) at CETL-MSOR 2019

- *Over the threshold: how schools, colleges and unviersities can work together to build mathematical foundations for successful progression* by Prof. Alice Rogers OBE, Kings College London.

Dr. Joe Kyle from the University of Birmingham also gave a keynote address to close the conference, summarising the contributions over the course of the conference.

The full programme can be found at `http://www.sigma-network.ac.uk/wp-content/uploads/2019/09/CETL-MSOR-Final-Timetable-2019.pdf`.

Report by Sinéad Breen, DCU
sinead.breen@dcu.ie

17th Workshop on Numerical Methods for Problems with Layer Phenomena
11-13 November 2020, University of Limerick

A three-day workshop was organised by the Department of Mathematics and Statistics at the University of Limerick, Limerick, in cooperation with MACSI (the Mathematics Applications Consortium for Science and Industry), with financial support by the Irish Mathematical Society. The aim of the workshop is to bring together people, in the mathematics and general scientific community, who have particular interests in the

development and applications of numerical methods for problems that exhibit layer phenomena, such as boundary/interior layers in fluid flow and other applications.

This year, the workshop was dedicated to the memory of our dear friend Piet Hemker who passed away in May 2019. Piet worked at CWI (the Centre for Mathematics & Computer Science) in Amsterdam from 1970 until his retirement in 2006 and was a CWI Fellow since 2001. From 1989 until his retirement, he was also an endowed professor at the University of Amsterdam. Piet contributed with important innovative scientific research to many areas of numerical mathematics, including, inter alia, multigrid methods, defect correction, numerical methods for compressible flows, and manifold mapping. Of particular relevance to this workshop, he published more than 20 papers with G.I. Shishkin on singular perturbation problems and proposed the famous Hemker test problem in J. Comput. Appl. Math. in 1996. In 2006 Piet became a Knight in the Order of the Netherlands Lion (Ridder in de Orde van de Nederlandse Leeuw).

The meeting was initially planned for April 2020, but was postponed, and finally held virtually on 11-13 November 2020. It featured 12 Irish and international speakers, and attracted more than 50 participants from Canada, China, Cyprus, Germany, India, Ireland, Russia, Serbia, Spain, and the UK.

2020 Speakers

- Faiza Alssaedi (National University of Ireland Galway, Ireland)
  Numerical solution of fourth-order real and complex-valued singularly perturbed problems
- Gabriel Barrenechea (Univeristy of Strathclyde, Scotland, UK)
  Divergence-free finite element methods for an inviscid flow model
- José Luis Gracia (University of Zaragoza, Spain)
  Numerical approximations to singularly perturbed convection-diffusion parabolic problems with a discontinuous initial condition
- Róisín Hill (National University of Ireland Galway, Ireland)
  Generating layer-adapted meshes using MPDEs
- Natalia Kopteva (University of Limerick, Ireland)
  Upper and lower solutions in the numerical analysis of semilinear singularly perturbed differential equations
- Scott MacLachlan (Memorial University of Newfoundland, Canada)
  Parameter-robust preconditioners for singularly perturbed convection-diffusion equations
- Nikolai Nefedov (Lomonosov Moscow State University, Russia)
  Periodic and stationary solutions of nonlinear reaction-diffusion problems with singularly perturbed boundary conditions
- Eugene ORiordan (Dublin City University, Ireland)
  Singularly perturbed convection-diffusion parabolic problems with a discontinuous initial condition
- Martin Stynes (Beijing Computational Science Research Center, China)
  A weighted and balanced finite element method for singularly perturbed reaction-diffusion problems
- Vladimir Volkov (Lomonosov Moscow State University, Russia)
  Asymptotic solution of the coefficient inverse problems for Burgers type equations
- Christos Xenophontos (University of Cyprus)
  Isogeometric analysis for singularly perturbed high-order, two-point boundary value problems of reaction-diffusion type
- Alexander Zadorin (Sobolev Institute of Mathematics, Novosibirsk, Russia)
  Approaches to calculating derivatives in the presence of a boundary layer

The book of abstracts is accessible from the workshop website[1] or using the direct link[2].

This workshop was the 17th in a sequence of annual workshops, but the 1st to be held online instead of physically. Its success opened our eyes to the possibility of organising talks by speakers located in any part of the globe. Thus, in collaboration with other Irish researchers, we have now created the (virtual) **Irish Numerical Analysis Forum**[3] which will include fortnightly seminars in all areas of numerical analysis that are aligned with the interests of the Irish numerical analysis community. Its aim will be to solicit lectures from leading international numerical analysts who will discuss their research area in a style that is accessible to most numerical analysts (i.e., not just those who are already familiar with the subject of the lecture).

Report by Alan Hegarty and Natalia Kopteva, University of Limerick
alan.hegarty@ul.ie, natalia.kopteva@ul.ie

Groups in Galway 2020: Online edition
9–11 September 2020, NUI Galway

Groups in Galway 2020 was organised by Angela Carnevale and Tobias Rossmann (both from NUI Galway). The organisers are grateful to the Irish Mathematical Society for supporting this event. Due to the ongoing pandemic, the conference took place online. There were three sessions, spread over as many days. The times of the sessions were chosen to accommodate a wide audience from across the world. Well over 200 people registered to virtually attend the meeting, and the total number of active participants exceeded 100 during some of the sessions.

As the non-mathematical highlight of the conference, John Burns, Richard Hennessey, Michael Mc Gettrick, and Cathal Seoighe very kindly provided the participants with a socially-distanced live performance of traditional Irish music, supported by a view of the scenic NUI Galway campus.

The conference featured a total of eight invited talks covering a wide range of topics in contemporary group theory and related fields:

(1) Matteo Cavaleri (Niccolò Cusano University Rome):
Gain graphs, group algebra valued matrices and Fourier transform
(2) Joanna B. Fawcett (Imperial College London):
Tree-homogeneous graphs
(3) Meinolf Geck (University of Stuttgart):
What is bad about bad primes? Some remarks about unipotent classes
(4) Radhika Gupta (University of Bristol):
Uniform exponential growth for CAT(0) *cube complexes*
(5) Joshua Maglione (Bielefeld University):
Isomorphism via derivations
(6) John Murray (Maynooth University):
Clifford theory of 2*-Brauer characters*
(7) Emily Norton (TU Kaiserslautern):
Some decomposition matrices of finite classical groups
(8) Anitha Thillaisundaram (University of Lincoln):
Groups acting on rooted trees of growing degrees

[1] https://staff.ul.ie/natalia/node/1209
[2] https://staff.ul.ie/natalia/sites/default/files//LimerickWorkshop2020_abstracts.pdf
[3] https://staff.ul.ie/natalia/node/1210

The conference website (`http://www.maths.nuigalway.ie/conferences/gig20/`) contains abstracts of the talks and further information, including links to videos of some of the talks.

Report by Tobias Rossmann, NUI Galway
tobias.rossmann@nuigalway.ie

Irish Math. Soc. Bulletin
Number 86, Winter 2020, 17–46
ISSN 0791-5578

Ring learning with errors: a crossroads between post-quantum cryptography, machine learning and number theory

IVÁN BLANCO-CHACÓN

Abstract. The present survey is intended to serve as a comprehensive account of the main areas of the cryptography based on the Ring Learning With Errors Problem. We cover the major topics, from their mathematical foundations to the main primitives, as well as several open ends and recent progress with an emphasis in the connections with algebraic number theory. This work is based to a certain extent on an invited course and a seminar given by the author at the Basque Center for Applied Mathematics in 2018 and at the ICIAM 2019.

1. Introduction

According to MIRACL Labs, it is estimated that a quantum computer capable of breaking most of modern cryptography will be built in the next 10-15 years (20-25 years according to estimates made public in the last NIST call for the standardisation of post-quantum primitives). All of cryptography is built on supposedly *hard*[1] mathematical problems, most of which, like integer factorisation or the discrete logarithm problem, become relatively easy in the context of a working quantum computer. In response to this threat there is a need to migrate from these vulnerable constructs to constructs known to remain strong even in a post-quantum world.

An example of such a hard problem is the shortest vector problem in general lattices, which is known to be NP-hard (at least for a very small approximation factor). While there already exist post-quantum solutions for much of standard cryptography, like public key encryption and digital signature, it is currently unclear how some of the more elaborate protocols, like those seeking for integrity or non-repudiation can be successfully migrated. In particular in the last 10+ years bilinear pairings on elliptic curves have opened up many new possibilities, which might likely be rendered insecure in a post-quantum world. Already commercial products based on bilinear pairings have found applications in the 'real world', and so much work must be done to ensure that we will be able to retain this functionality into the future.

At the same time there is much fundamental work to be done on the post-quantum primitives themselves. A major decision is to choose between one or various of the following technologies, for each security/integrity demand:

a) Code based cryptography ([31]) is built on the infeasibility of syndrome decoding for general linear error-correcting codes over finite fields.

2020 *Mathematics Subject Classification.* 11T71,11Z05, 94A60.

Key words and phrases. Ring Learning With Errors, Post-quantum cryptography, Lattice based cryptography, Cyclotomic polynomials, Condition number.

Received on 16-12-2020.

This work has been partially supported by Science Foundation Ireland 13/IA/1914 and MTM2016-79400-P.

[1]In a sense which will be made clear in Section 2.

b) Multivariate based cryptography ([14]) is based on the fact that solving general systems of multivariate polynomial equations over finite fields is proved to be NP-hard.

c) Supersingular isogeny based cryptography ([19]), is a protocol for key exchange, analogous to Diffie-Hellman, but the cyclic groups present here are attached to supersingular elliptic curves defined over finite fields.

d) Finally, lattice based cryptography, admits a large number of different formulations and constructions. This report focuses on one of the most promising lattice-based technologies: Ring Learning With Errors (RLWE). This scheme is based on the RLWE problem, which is based in turn on the difficulty of solving the shortest vector problem (SVP) on ideal lattices.

At the time of writing, code, lattice and multivariate-based methods seem to be the strongest contenders, as they appear to have the flexible structure needed on which to base more complex protocols. Within these three categories, the lattice-based one has by far a larger number of non-broken primitives/protocols.

Lattice-based cryptography has a relatively mature history, primarily due to the work done by the early proponents of the related NTRU cryptosystem ([24]). This was a patented technology which enjoyed some minor success, but never really gained traction, as when it was invented, a quantum computer still seemed very far off. Its patents have now expired.

RLWE first came to prominence with the paper by Lyubashevsky, Peikert and Regev ([28]). A key-exchange algorithm proposed by them has been recently optimized and implemented by Alkim, Ducas, Pöppelmann, and Schwabe ([1]). This has been implemented by Google in a well-publicised experiment ([10]). In recent times there have been many implementation improvements, see for example the recent paper by Scott ([38]). So there can be no doubting the practicality of the technology, opinions supporting this view include those of a good number of researchers in Intel Labs and MIRACL Labs.

RLWE is built on an earlier scheme: the Learning with Errors (LWE) problem, which admits a security reduction from the SVP on arbitrary lattices, but with a much larger approximation factor than the one for which SVP is proved to be NP-hard. Of course, this is not a formal hardness guarantee for LWE but it can be regarded as a clue of its strength. Moreover, no polynomial-time attack has been found against LWE yet.

The main disadvantage of LWE is a quadratic overhead in the key sizes, which is overcome in the RLWE scenario, at the cost of being backed in the SVP over just ideal lattices, which even if based on experience is widely believed to be intractable, there is no formal proof at the moment, and for no approximation factor.

In spite of that, the RLWE variant appears to be eminently practical: like most post-quantum proposals, RLWE key sizes are much larger than those of non post-quantum methods, but the required computing power is usually much smaller. For example while an elliptic curve based cryptosystem might use keys of 256 bits, an equivalent system based on RLWE might require keys of 4096 bits to grant the same security level, while running maybe 10-100 times faster ([27]). These differences might be seen as balancing each other out. Furthermore, 30% of the surviving proposals for the NIST are based on RLWE.

We have tried to make our report accessible by a broad audience with no more knowledge than some basics in finite fields, linear algebra, probability and group/ring theory. Thus, we have structured our report as follows:

In section 2 we provide a quick introduction to the different features of cryptography and introduce the main terms and facts on complexity as they show up in the literature. We provide several examples, elaborating on those presented in the course by the author.

In section 3 we expose the main concepts of lattice-based cryptography. We focus on the classical LWE, over which RLWE is built and discuss its advantadges and drawbacks, as well as different attacks against weak instantiations, which will be exploited in the RLWE scenario in Section 6.

Section 4 is a quick overview of a few key concepts in algebraic number theory: rings of integers, canonical embedding, and other topics. These pieces make the foundations of RLWE, but the reader who is familiar with this material can safely skip it. Several examples are worked out there, and in addition, we provide some comprehensible references for the topic.

Section 5 introduces the RLWE problem in its various formulations. In particular, we carefully discuss the Polynomial Learning With Errors problem (PLWE), which appeared in the literature before RLWE ([40]). We discuss the equivalence between both problems and explain some recent advances in this topic: in particular we comment on recent work by the author ([6]) which gives a partial answer in the cyclotomic case, the most interesting from a cryptographic point of view. Besides, we explain the hardness result which backs RLWE and describe in full detail the LPR crypstosystem, as presented in [28]. We close the chapter by presenting a key exchange protocol based in RLWE ([15]).

Section 6 is a summary of several attacks against the RLWE cryptosystem. They reduce to LWE or to PLWE attacks and allow to discard insecure choices of parameters. The search for secure instantiations motivates some number theoretical problems and conjectures which we also discuss.

Section 7 is for RLWE-based digital signatures and homomorphic encryption, a functionality which is gaining much interest nowadays, since it allows to solve a good number of logistic and security problems in cloud computing and storing. We close the survey by discussing in detail some (second round) NIST figures.

A couple of remarks to end this introduction: first, by a *polynomial time algorithm* we mean an algorithm for which there exists a polynomial $p(x) \in \mathbb{R}[x]$ and a *size* function on the family of the algorithm inputs $x(n)$, such that the time it takes to run the algorithm on input n is $p(x(n))$. Second, we will use sometimes the $\tilde{O}$-notation: a function $f(x)$ is $\tilde{O}(g(x))$ if it is $O(g(x)log^k(x))$ for some k.

Acknowledgements: The author thanks Gary McGuire for carefully reading a preliminary version of this survey, to Mike Scott for providing most of the practical highlights on RLWE and to the Basque Center for Applied Mathematics for their invitation to give this course and to take part in the post-quantum cryptography mini-symposum at ICIAM 2019. Active and insightful discussion with the audience of the course and seminar, and in particular with Sebastiá Xambó set the author to write this work. This work has been partially supported by Science Foundation Ireland 13/IA/1914 and MTM2016-79400-P.

2. Post-quantum cryptography

2.1. **Cryptography features.** Requirements such as confidentiality and proofs of identity are crucial in electronic financial and legal transactions, while some other features like non-repudiation or operating on encrypted data (homomorphic encryption) are gaining much traction within the last few years. We examine here most of these functionalities.

The best known cryptographic problem is confidentiality. This is attained by the use of well-designed encryption/decription schemes.

To start with, we fix a finite alphabet $\mathcal{A}$, with some mathematical structure such as an abelian group or a field (e.g. the finite field $\mathbb{F}_q$ for $q = p^t$ and p prime, or an elliptic curve over this field). We consider three sets $\mathcal{K} \subset \mathcal{A}^n$ (keys), $\mathcal{M} \subset \mathcal{A}^N$ (plaintexts) and $\mathcal{C} \subset \mathcal{A}^N$ (ciphertexts) with $n \ll N$. Finally, we consider a set $\Lambda \subset \mathbb{N}$ which parametrizes the level of security, i.e., the larger $\lambda \in \Lambda$, the safer the scheme.

Definition 2.1 (Cipher schemes)**.** A cipher over $(\mathcal{K}, \mathcal{M}, \mathcal{C})$ is a family of pairs of efficiently computable functions $\{(E_\lambda, D_\lambda)\}_{\lambda\in\Lambda}$ where for each λ, $E_\lambda : \mathcal{K} \times \mathcal{M} \to \mathcal{C}$ (encryption function) and $D_\lambda : \mathcal{K} \times \mathcal{C} \to \mathcal{M}$ (decryption function) are such that for each key $k \in \mathcal{K}$ and for each plaintext $m \in \mathcal{M}$, the following correctness property holds:

$$D_\lambda(k, E_\lambda(k, m)) = m.$$

That is to say, decryption undoes encryption.

Efficiently computable means that both E_λ and D_λ can be computed by an algorithm which is polynomial in the security parameter λ, i.e., there exist polynomials $p(x), q(x) \in \mathbb{R}[x]$ only depending on the scheme, such that for each $\lambda \in \Lambda$, $k \in \mathcal{K}$, $m \in \mathcal{M}$, and $c \in \mathcal{C}$, the number of steps to compute $E_\lambda(k, m)$ (resp. $D_\lambda(k, c)$) is upper bounded by $p(\lambda)$ (resp. $q(\lambda)$). Moreover, the algorithm for E_λ can be probabilistic, while D_λ should always be deterministic.

Since in our definition both the encryption and decryption parties have the same key (i.e., the scheme is symmetric), they should agree beforehand on that key somehow. For instance, they might do it physically in a secret meeting but they can also use a digital key exchange protocol. As usual, any arbitrary legitimate sender (receiver) will be called Alice (Bob), and any arbitrary eavesdropper will be called Eve.

Definition 2.2 (Key exchange protocol)**.** A key exchange protocol is an efficient method for Alice and Bob to agree on a key through a (potentially non-safe) channel. One of the most famous protocols is Diffie-Hellman's (DH)[1], where Alice and Bob start by agreeing on a finite feld $\mathbb{F}_q$ and a primitive root g, namely, a generator of the cyclic multiplicative group $\mathbb{F}_q^*$. The pair (q, g) is made public, and to agree on a private key, Alice selects an integer a and Bob selects an integer b. Then, Alice sends g^a modulo q to Bob, who on receiving it, raises it to b modulo q, getting g^{ab} modulo q. Next, Bob sends g^b modulo q to Alice, who raises it to a, obtaining also g^{ab} modulo q, the agreed private key.

Notice that without knowledge of a or b, Eve cannot obtain g^{ab} from g^a and g^b in an efficient manner (on a classic computer!), the main obstruction being the unfeasibility of the discrete logarithm, namely, to obtain a from g^a modulo q, if g is known. Nowadays, a combined usage of Diffie-Hellman (or some variant) with a suitable symmetric cipher is used in most internet protocols, like TLS or TCP/IP. A variant of DH is ECDH, where the multiplicative group $\mathbb{F}_q^*$ is replaced by the additive group of an elliptic curve over $\mathbb{F}_q$.

Definition 2.3 (Digital signatures)**.** A signature scheme is a pair (G, D), where $G : \Lambda \to \mathcal{K}$ is an efficient key generating probabilistic algorithm, and $D = \{(S_\lambda, V_\lambda)\}_{\lambda\in\Lambda}$ is a family of pairs of efficiently computable[2] functions $S_\lambda : \mathcal{K} \times \mathcal{M} \to \mathcal{T} \subseteq \mathcal{A}^r$ (space of *tags*) and $V_\lambda : \mathcal{K} \times \mathcal{M} \times \mathcal{T} \to \{0, 1\}$ such that whenever k_s (secret key) and k_p (public key) are sampled from G on security level λ, then, for every message $m \in \mathcal{M}$:

$$pr\left[V_\lambda(k_p, m, S_\lambda(k_s, m)) = 1\right] = 1,$$

[1]There are more general versions of the Diffie-Hellman problem, not known to be equivalent to a discrete logarithm problem, but here we stick to its version over finite fields, which by construction is so.

[2]by polynomial-time probabilistic algorithms.

For a security level λ, S_λ is called the signature function and V_λ the verification function, which returns 1 if the signature is valid and 0 otherwise, and the correctness of the scheme means that on a message m and a secret key k_s, the signature function produces a tag $S_\lambda(k_s, m)$, which is verified as valid by the verifying function with probability 1, given the message m and the public key k_p. This scheme provides a proof that the message was signed by a known signatory (authentication) and the signatory cannot deny having signed the message (non-repudiation). Classic designs of digital signature schemes include Rabin's algorithm, Lamport schemes and Merkle trees, as well as RSA-based protocols ([7] 13.3.1).

Integrated Encryption Schemes (signcryption schemes) implement both encryption and authentication. Two of the most commonly used are ECIES, which operates with elliptic curves and DLIES, which operates over $\mathbb{F}_q$.

Definition 2.4 (Homomorphic encryption[3])**.** Let (E, D) be a cipher over $(\mathcal{K}, \mathcal{M}, \mathcal{C})$ where $\mathcal{M}$ and $\mathcal{C}$ are abelian groups under the operations $*_\mathcal{M}$ and $*_\mathcal{C}$ respectively. The cipher is said to be homomorphic if for each key $k \in \mathcal{K}$ and plaintexts $m_1, m_2 \in \mathcal{M}$, it is

$$E(k, m_1) *_\mathcal{C} E(k, m_2) = E(k, m_1 *_\mathcal{M} m_2).$$

Example 2.1. RSA encryption is homomorphic. Indeed, for an RSA integer $N = pq > 1$ and an exponent e modulo $\phi(N)$ with inverse d, encryption goes as $x \mapsto x^e \pmod N$, which clearly commutes with the product modulo N, but not with the sum.

When in addition, $\mathcal{M}$ and $\mathcal{C}$ have ring structure and encryption commutes with both ring operations, the cipher is said to be fully homomorphic (FHE). Notice that RSA is not fully homomorphic.

Homomorphic encryption allows to perform operations on the plaintext by operating directly on the ciphertexts, i.e., without decrypting first. This is relevant when the operations are outsourced and performed over a non-trustable server. Applications of homomorphic encryption include encrypted database queries, cloud computing, genetic computing, health data management or outsourced generation of blockchain addresses.

2.2. **P, NP, NP-hard and NP-complete.** The author has often seen that the terms *intractable*, *unfeasible*, and *hard*, are used in the postquantum cryptography literature in a rather loose (at best!) manner and this may lead to believe that certain computational problems enjoy certain complexity guarantees that they simply have not. We make here precise the main terms that usually appear in the problems which back lattice cryptography.

Definition 2.5 (The P and NP classes)**.** The P class consists of the decission problems whose solution can be found on a deterministic Turing machine in polynomial time in the input size. The NP class consists of the decission problems for which a putative solution can be checked to be a real solution or not in polynomial time on a deterministic Turing machine on the input size.

Equivalently, the NP-class consists of the decission problems such that a solution can be found in polynomial time on a non-deterministic Turing machine: indeed, assuming Definition 2.5 for the NP class, an algorithm based on a non-deterministic Turing Machine can be built in two steps; the first is a non-determininstic guess about the solution, and the second consists of a polynomial deterministic algorithm that verifies if the guess is a solution(cf. [2] pag. 283 for details). A common misconception is that the *NP* term stands for *non-polynomial* when in fact it stands for *non-deterministic polynomial acceptable problems*.

[3]From now on, to ease notation, we will omit the λ-subscripts unless it results in ambiguity.

A note of caution: as we pointed out at the end of the introduction, the term *in polynomial time* means that the time it takes to solve a problem is, on input n, upper bounded by a polynomial in $x(n)$ where x is a *size* function. The most used size function is the logarithm, as we can regard it, essentially as the number of digits, a *true size* of the input. Hence, a brute force attack on DLP for $\mathbb{F}_p$ takes $p-1$ powers and checks, which is polynomial in p but exponential in $\log(p)$. There are classical (non-quantum) algorithms which drastically reduce the order, like the number field sieve (subexponential), but none of them is polynomial in $\log(p)$. We refer the reader to Chapter 4 of this work for a summary on number fields and their key properties and to [25] for an exposition of the number field sieve method.

Example 2.2. The problem of primality testing, i.e. deciding whether a positive integer is prime or not is NP: indeed, given a natural number $n > 1$ and $b \leq n$, the Euclidean algorithm can be used to check if $b \mid n$ in approximalety $\log(b)$ operations. Moreover, in a major breakthrough, Agrawal, Kayal and Saxena proved that primality testing is also a P problem.

Example 2.3. The problem of factoring, namely to return a proper factorisation $n = pq$ with $1 < p, q < n$ of an input $n \in \mathbb{N}$ is also NP: a pair $(p, q) \in \mathbb{N}^2$ can be checked to be (or not) a non trivial factorisation of n by performing approximately $\log(q)^2$ multiplications, if $q \geq p$.

Two celebrated algorithms due to Peter Shor solve the factoring problem and the DLP in polynomial time on a quantum computer ([39]). To factor a positive integer n, Shor's algorithm runs over all the integers in the range $\{1, .., n\}$. For $1 < a < n$, if a is a unit modulo n, the algorithm calls a sub-routine to compute the order of a modulo n. With this period, the algorithm produces a non-trivial factor of n with arbitrarily large probability in polynomial time. The order-finding sub-routine is run on a quantum computer, but the use of the order to produce a factor is classical.

In fairness, this does not mean that the problem of factoring is in the P-class, as a (probabilistic) quantum algorithm is not equivalent, in general, to a Turing or sequential machine.

Definition 2.6 (Reduction)**.** We say that a problem A admits a reduction to a problem B if any instance of A can be transformed to an instance of B in polynomial time, namely, if solving B suffices for solving A with the same order of complexity.[4]

Informally, NP-hard and NP-complete problems are those at least as hard as those in the NP-class, but while NP-complete problems belong to NP, NP-hard ones need not to. More precisely:

Definition 2.7. The NP-hard class consists of those problems A such that every problem in NP can be reduced to A in polynomial time. The NP-complete class consists of those NP problems which are NP-hard.

Example 2.4. The prime factorisation problem, i.e. to return all the prime factors with multiplicity of an input $n \geq 1$, is clearly NP: checking if a putative solution is a prime factorisation of n can be done in (deterministic) polynomial time. However it is not known if the prime factorisation is NP-hard (and hence NP-complete). It is expected, moreover, not to be in the P class.

So, a quantum computer would render insecure both RSA and Diffie-Hellman. Even more, Tate and Weil's pairings allow to reduce ECDLP to DLP ([29]), a reduction which

[4]By *order of complexity* we mean *polynomial, superpolynomial, subexponential* and *exponential*. We stick to these orders as they are enough for our analysis.

is even polynomial (although probabilistic) on supersingular curves, hence, the elliptic version on Diffie-Hellman should also be avoided in a post-quantum scenario. This is a reason to consider schemes which use pairing-free abelian varieties, hence other than elliptic curves. Jacobians of hyperelliptic curves are known to be good candidates but beyond genus 3, the complexity of finding explicit equations and explicit computations for the addition law render them unfeasible.

Finally, another well-known problem is whether $P \neq NP$ or not. If equality held, all cryptographic (classic and postquantum) primitives based on NP problems would be useless. On the contrary, if, as it is widely believed, $P \neq NP$, then every NP-hard problem would be non-polynomial, hence suitable for cryptography: indeed, if Λ is NP-hard, in case $P \neq NP$, take B in $NP \setminus P$. Then Λ cannot be polynomial (otherwise, B would be so).

But for the moment, lacking a proof of $P \neq NP$, all we can say is that NP-hard problems are *strongly* expected to be suitable for (postquantum) cryptography.

3. Lattice based cryptography

The security of lattice-based schemes relies on two problems which are expected to be intractable on a quantum computer, as we explain next. By length, we mean Euclidean length, denoted $||\ ||$.

Definition 3.1. A lattice in $\mathbb{R}^n$ is a pair (Λ, ρ) where Λ is a finitely generated and free subgroup of the additive group $(\mathbb{R}^n, +)$ and $\rho : \Lambda \to \mathbb{Z}^n$ is an isomorphism. We denote by $\lambda_1(\Lambda)$ the minimal length among the set of non-zero elements of Λ.

Notice that our definition has implicit the feature of being of full rank. There are more general definitions but this will be enough for us.

Example 3.1. In the ring of Gaussian integers $\mathbb{Z}[i] = \{a + bi; a, b \in \mathbb{Z}\}$, identifying $(\mathbb{C}, +)$ with $(\mathbb{R}^2, +)$, we can impose a lattice structure in (at least) two ways:

$$\begin{array}{ccc} \rho_1 : \mathbb{Z}[i] & \to & \mathbb{Z}^2 \\ a + bi & \mapsto & (a, b) \end{array} \tag{3.1}$$

or

$$\begin{array}{ccc} \rho_2 : \mathbb{Z}[i] & \to & \mathbb{Z}^2 \\ a + bi & \mapsto & (a + b, a - b). \end{array} \tag{3.2}$$

Definition 3.2. Let (Λ, ρ) be a lattice in $\mathbb{R}^n$ with basis $\mathcal{B} = \{v_1, ..., v_n\}$. The fundamental parallelogram of Λ associated to $\mathcal{B}$ is:

$$\mathcal{F}(\mathcal{B}) = \left\{ \sum_{i=1}^{n} \lambda_i v_i : \text{ with } 0 \leq \lambda < 1 \right\}.$$

Problem 3.3 (SVP)**.** The shortest vector problem (SVP) is, on input of an arbitrary lattice Λ in $\mathbb{R}^n$, together with a basis, to determine a vector $x \in \Lambda$ with length $\lambda_1(\Lambda)$. For $\gamma > 0$, the γ-approximate shortest vector problem (γ-SVP) is to determine a non-zero vector $x \in \Lambda$ with $||x|| \leq \gamma \lambda_1(\Lambda)$.

Problem 3.4 (CVP)**.** The closest vector problem (CVP) is, on input of an arbitrary lattice Λ in $\mathbb{R}^n$, together with a basis and a point $y \in \mathbb{R}^n$, to find $x_y \in \Lambda$ such that

$$||y - x_y|| = \min_{x \in \Lambda} ||x - y||.$$

In [30], it is proved that γ-SVP is NP-hard for $\gamma < \sqrt{2}$ and in [9], it is proved that CVP is NP-complete, hence if $P \neq NP$, these two problems cannot be solved in polynomial time, even with the aid of a quantum computer.

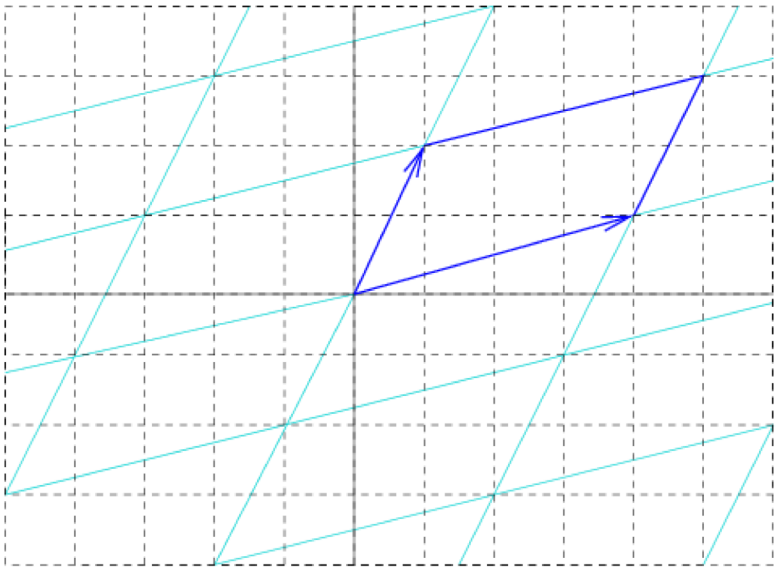


FIGURE 1. Fundamental parallelogram, in darker blue. Source: Wikipedia (by Álvaro Lozano Robledo)

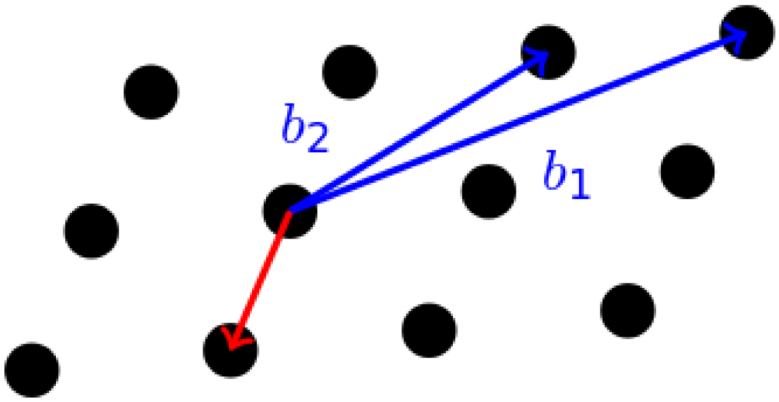


FIGURE 2. Illustration of the shortest vector problem (basis vectors in blue, shortest vector in red). Source: Wikipedia (by Sebastian Schmittner)

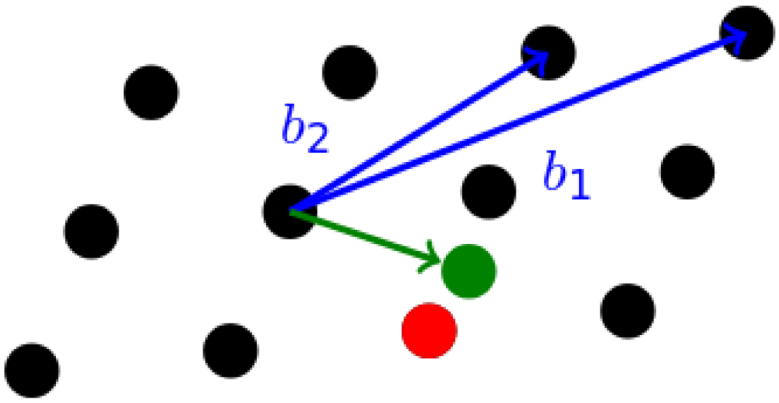


FIGURE 3. Illustration of the closest vector problem (basis vectors in blue, external vector in green, closest vector in red). Source: Wikipedia (by Sebastian Schmittner)

3.1. **The Learning With Errors problem (LWE).** Let q be a rational prime for which a suitable choice will be made later.

Definition 3.5. The real torus of dimension 1 is the quotient group $\mathbb{T} = \mathbb{R}/\mathbb{Z}$, its elements are equivalence classes of the form $x + \mathbb{Z}$ with $x \in [0, 1)$.

Lemma 3.6. *The following map is a group monomorphism:*

$$\begin{array}{ccc} \mathbb{F}_q & \hookrightarrow & \mathbb{T} \\ a + q\mathbb{Z} & \mapsto & \frac{a}{q} + \mathbb{Z}. \end{array}$$

A realization of lattice-based cryptography immune to all current quantum attacks and with a good chance of being NP-hard relies on the LWE problem, which we describe in this subsection.

Definition 3.7 (LWE-oracles)**.** Let χ be a discrete random variable with values in $\mathbb{T}$. For $s \in \mathbb{F}_q^n$, chosen uniformly at random, a LWE-oracle with respect to s and χ is a probabilistic algorithm $A_{s,\chi}$ which, at each execution, performs the following steps:

1. Samples a vector a uniformly at random from $\mathbb{F}_q^n$.
2. Computes the scalar product $\langle a, s\rangle$.
3. Samples $e \in \mathbb{T}$ from χ.
4. Outputs the vector $\left[a, \frac{1}{q}\langle a, s\rangle + e\right] \in \mathbb{F}_q^n \times \mathbb{T}$.

Definition 3.8 (The LWE problem)**.** Let χ be a discrete random variable with values in $\mathbb{T}$ as before. The LWE problem for χ and q is defined as follows:

a) Search version: for an element $s \in \mathbb{F}_q^n$ chosen uniformly at random and a LWE-oracle $A_{s,\chi}$, if an adversary is given access to arbitrarily many samples of the LWE distribution, this adversary must recover s with non-negligible advantage.

a) Decissional version: for an element $s \in \mathbb{F}_q^n$ chosen uniformly at random and a LWE oracle $A_{s,\chi}$, the adversary is asked to distinguish, with non-negligible advantage, between arbitrarily many samples from $A_{s,\chi}$ and the same number of samples $(a_i, b_i) \in \mathbb{F}_q^n \times \mathbb{T}$ where a_i and b_i are chosen independently and uniformly at random from $\mathbb{F}_q^n$ and $\mathbb{T}$.

From now on, χ will be an $\mathbb{F}_q$-valued Gaussian variable, which can be thought of as having values on $\mathbb{T}$ via Lemma 3.6. Such a variable is defined as follows: For $\sigma, c \in \mathbb{R}$ we set $\rho_{\sigma,c}(x) = \exp \frac{-(x-c)^2}{2\sigma^2}$. Write

$$S_{\sigma,c} = \rho_{\sigma,c}(\mathbb{Z}) = \sum_{k=-\infty}^{\infty} \rho_{\sigma,c}(k),$$

and define $D_{\sigma,c}$ to be the distribution on $\mathbb{Z}$ such that the probability of $x \in \mathbb{Z}$ is $\rho_{\sigma,c}(x)/S_{\sigma,c}$. Finally, the discrete Gaussian distribution χ with values in $\mathbb{F}_q$, mean 0, and parameter σ is defined by the probability function

$$Pr\left[\chi = k\right] = \sum_{n \equiv k \pmod q} pr\left[D_{\sigma,0} = n\right].$$

Some words of caution: first, the variance of χ should be very close to σ^2, but not neccesarily must be equal: in lattice-based cryptography one speaks about discrete random variables of parameter (rather than variance) σ^2. Second, effective sampling from discrete Gaussian distributions is a difficult topic and in practical cases it is approached only by numerical approximation (see [17]).

We conclude here with the following result due to Regev ([35]): a polynomial time quantum reduction from the SVP problem to the LWE problem, which backs the hardness of LWE and makes it a candidate to sustain a cryptosystem from it, as we will see in the next subsection.

Theorem 3.9 (Regev, [35])**.** *Let χ_r be a discrete Gaussian of parameter r^2, q a prime and $s \in \mathbb{F}_q^n$. Assume $r \geq 2\sqrt{n}$. Then, there is a quantum polynomial time reduction from γ-SVP, with $\gamma = \tilde{O}(nq/r)$to the search LWE problem attached to the LWE oracle A_{s,χ_r}.*

3.2. **Attacks against LWE.** In the language of Machine Learning, due to Theorem 3.9, a training algorithm for the LWE problem can be turned, in polynomial time (on a quantum computer), into an algorithm (of the same complexity) which solves the SVP problem. If the γ-SVP problem were NP-hard for the value of γ given in Theorem 3.9, it would follow the NP-hardness of the LWE problem. However, that value of γ depends on r^2, the parameter of χ_r, and the values of r for which the LWE-problem for A_{s,χ_r} results in a correct cryptosystem is bigger than $\sqrt{2}$, the value for which SVP is NP-hard. Hence, Regev's reduction cannot be used to prove NP-hardness of SVP. Nevertheless, this kind of result can be seen as a clue towards its security.

However, LWE has not been yet broken and there is a wide consense of the problem being *intractable*. Nevertheless, some ad-hoc instantiations may be insecure against very simple attacks. Given m LWE samples $\{(a_i, b_i = \frac{1}{q}\langle s, a_i\rangle + e_i)\}_{i=1}^m$, we can put them in columns to obtain a matrix $A = [a_1|...|a_m] \in \mathbb{F}_q^{n\times m}$ and set $\mathbf{b} = \frac{1}{q}A^t s + \mathbf{e}$, where $\mathbf{e}$ is the column vector of errors. We analyze three vulnerable instantiations:

1. If χ is identically zero (errorless LWE), s can be recovered via Gaussian elimination as long as the rows of A are linearly independent, which holds with high probability for $m > n$.
2. If χ takes values in $z + [-1/2, 1/2)$ with fixed $z \in \mathbb{R}$, we can round away each coordinate of $\mathbf{b}$ and subtract z to reduce to errorless LWE.
3. If each group of k samples has an error vector drawn from some distribution κ in $\mathbb{R}^k$ and some discretized error coordinate is always 0 under κ, we can ignore the samples corresponding to the other coordinates and since we have access to unlimited samples by hypothesis, we can equally reduce ourselves to errorless LWE. Analogously, we can reduce to errorless LWE if the sum (or a linear combination) of the k error coordinates in each group is 0.

Remark 3.10. Generalizing Case 2 in the above analysis, the error distribution χ is said *not to wrap around* $\mathbb{Z}$ if $Pr_{e\leftarrow\chi}\left\{e \notin z + [\frac{1}{2}, \frac{1}{2})\right\}$ is small enough for some known $z \in \mathbb{R}$. In this case, again by our unlimited access to the LWE oracle, the same attack as in Case 2 has good chance of success.

Other instantiations of LWE can be attacked by more sophisticated means. For instance, as described in [3], if all the discretized errors in our samples (i.e. seen not in the torus but in $\mathbb{F}_q^n$, after rounding to the closest integer) lie in a known set of size d, then search LWE can be broken in approximately n^d time and space, using n^d samples. If $d = O(1)$, the attack is polynomial in the dimension, while if $d = n^{1-\varepsilon}$, the attack is sub-exponential. For details cf. [32], Section 2.

What these attacks should make us learn is that the distribution χ should be very carefully chosen, to avoid falling in a low dimensional subspace of $\mathbb{F}_q^n$, in which case, reduction to errorless LWE might have a good chance of success.

3.3. **The LWE cryptosystem.** Based on the hardness guarantee in Theorem 3.9, and avoiding the above problematic instantiations, the LWE problem can be used to build the following cryptosystem:

Construction 3.11 (LWE cryptosystem, Regev ([35]))**.**

1. Parameters: $n, m \in \mathbb{N}$, $\alpha > 0$.
2. Private key: $s \in \mathbb{F}_q^n$ chosen uniformly at random.
3. Public key:
   3.1 Sample $a_1, ..., a_m \in \mathbb{F}_q^n$, independently and uniformly at random.
   3.2 Sample $e_1, ..., e_m \in \mathbb{F}_q$, independently from χ, which is assumed here to be a discrete Gaussian of zero mean and parameter $\frac{\alpha q}{2\pi}$.
   3.3 Publish $\{[a_i, b_i = \langle a_i, s\rangle + e_i]\}_{i=1}^m$.
4. Encryption: for a bit $z \in \mathbb{F}_2$, consider it as an element of $\mathbb{F}_q$ by mapping the 0 and 1 of $\mathbb{F}_2$ to the 0 and 1 of $\mathbb{F}_q$. Select a random subset $S \subseteq \{1, ..., m\}$ and map
$$z \mapsto [u, v] = \left[\sum_{i\in S} a_i, z\lfloor\frac{q}{2}\rfloor + \sum_{i\in S} b_i\right].$$
5. Decryption: on receiving an encrypted message $[u, v]$, compute $d := v - \langle u, s\rangle$. This equals $z\lfloor\frac{q}{2}\rfloor + \sum_{i\in S} e_i$. If $z = 0$, then d has absolute value below $\lfloor\frac{q}{4}\rfloor$ with probability as close to 1 as desired, depending on how we choose the parameter α. So, if this is the case, decrypt to 0, otherwise, decrypt to 1.

The right choice of q, m and α is given in the following result, whose proof is omited since it is very similar to the cryptographic scheme presented in the next subsection, whose proof we will discuss.

Theorem 3.12. *If $q \in \{n^2, ..., 2n^2\}$, $\alpha = \frac{1}{\sqrt{n}\log^2(n)}$ and m is of the order of $n\log(q)$, then the LWE cryptosystem is correct and pseudorandom*[5]*.*

As we can see, a public key for LWE has m vectors in $\mathbb{F}_q^n$, since m is of the order of $n\log(n)$, it turns out that a public key has an $\mathbb{F}_q$-size of the order $n^2\log(n)$. This quadratic overhead is an unfeasible constrain from a practical point of view, in particular in settings such as hand-held digital broadcasting, mobile encryption and small devices in tentative applications of the IoT (Internet of Things), where the hardware has a relatively small memory. Moreover, in other recent scenarios where homomorphic encryption is desirable, LWE cannot fit well if the plaintext space is big enough. Such a scenario is that of electronic elections (e-voting and i-voting), which has to combine encryption with signature and authentication. For a large enough country, the size of the keys (which even if a pseudorandom generator is used, must grow with the size of the plaintext space) is certainly to be taken into account.

A variation of the LWE problem, the ring learning with errors (RLWE) problem was introduced to tackle this quadratic overhead in the key sizes. The foundations of the problem require several notions from algebraic number theory, which we present next.

4. Some basics of algebraic number theory

Here we present the notions of algebraic number theory used to build the RLWE cryptosystem. Readers who are familiar with them can safely skip this section, since all our notations are standard. Readers who are not so familiar are referred to [41], Chapter 2 for more details.

4.1. **Algebraic number fields.** An algebraic number field (number field, for short) is a field extension $K = \mathbb{Q}(\theta)/\mathbb{Q}$ of finite degree n, where θ satisfies a relation $f(\theta) = 0$ for some irreducible polynomial $f(x) \in \mathbb{Q}[x]$, which is monic without loss of generality. The polynomial f is called the minimal polynomial of θ, and n is also the degree of f. Notice that K is in particular an n-dimensional $\mathbb{Q}$-vector space and the set $\{1, \theta, ..., \theta^{n-1}\}$ is a

[5]I.e. statistically indistinguishable from a uniform distribution.

$\mathbb{Q}$-basis of K called a power basis. Notice that associating θ with the unknown x yields a natural isomorphism between K and $\mathbb{Q}[x]/f(x)$.

Let $\overline{\mathbb{Q}}$ denote an algebraic closure of $\mathbb{Q}$ fixed from now on. A number field $K = \mathbb{Q}(\theta)$ of degree n has exactly n field embeddings (injective field homomorphisms) $\sigma_i : K \to \overline{\mathbb{Q}}$ fixing $\mathbb{Q}$. Each embedding σ_i is determined by $\sigma_i(\theta) = \theta_i$, where $\{\theta_i\}_{i=1}^n$ are the different roots of f. The number field is said to be Galois if K is the splitting field of f.

Example 4.1. Denote by $\sqrt[3]{2}$ the unique real cubic root of 2. The number field $K = \mathbb{Q}(\sqrt[3]{2})$ is not Galois: indeed, the other two roots of the minimal polynomial, $X^3 - 2$ do not belong to K. To make it Galois, we need to adjoin ω_3, a non-real cubic root of 1.

An embedding whose image lies in $\mathbb{R}$ (corresponding to a real root of f) is called a real embedding; otherwise it is called a complex embedding. Since complex roots of f come in conjugate pairs, so do the complex embeddings. The number of real embeddings is denoted s_1 and the number of pairs of complex embeddings is denoted s_2, so we have $n = s_1 + 2s_2$. If $s_2 = 0$ (resp. $s_1 = 0$) K is said to be totally real (resp. totally imaginary).

Definition 4.1. The canonical embedding $\sigma : K \to \mathbb{R}^{s_1} \times \mathbb{C}^{2s_2}$ is then defined as

$$\sigma(x) = (\sigma_1(x), ..., \sigma_n(x)).$$

4.2. **Algebraic integers.** An algebraic integer is an element of $\overline{\mathbb{Q}}$ whose minimal polynomial over $\mathbb{Q}$ has integer coefficients. For a number field K of degree n, let $\mathcal{O}_K \subset K$ denote the set of all algebraic integers in K. This set forms a ring under addition and multiplication in K ([41], Theorem 2.9), called the ring of integers of K. It happens that $\mathcal{O}_K$ is a free $\mathbb{Z}$-module of rank n, i.e., it is the set of all $\mathbb{Z}$-linear combinations of some basis $\mathcal{B} = \{b_1, ..., b_n\} \subset \mathcal{O}_K$ of K ([41], Theorem 2.16). Such a set $\mathcal{B}$ is called an integral basis.

Example 4.2. Let $n > 1$ be an integer. The set of primitive n-th roots of unity (those of the form $\theta_k = exp(2\pi ik/n)$, with $1 \leq k \leq n$ coprime to n) forms a multiplicative group of order $m = \phi(n)$. The n-th cyclotomic polynomial is

$$\Phi_n(x) = \prod_{k \in \mathbb{Z}_n^*} (x - \theta_k).$$

This is the minimal polynomial of θ_k for each k, so that $K = \mathbb{Q}(\theta_k)$ is a number field of degree m. It can be proved ([41] Chap 3) that the ring of integers of K is precisely $\mathbb{Z}[\theta]$ for each $\theta = \theta_k$, with $k \in \mathbb{Z}_n^*$.

Definition 4.2. A number field K such that $\mathcal{O}_K = \mathbb{Z}[\alpha]$ for some $\alpha \in \mathcal{O}_K$ is said to be monogenic.

Example 4.3. Let d be a square-free integer. Consider the number field $\mathbb{Q}(\sqrt{d})$. It can be shown that the ring of integers of K is $\mathbb{Z}[\sqrt{d}]$ if $d \not\equiv 1 \pmod 4$ and $\mathbb{Z}[\frac{1+\sqrt{d}}{2}]$ otherwise.

Definition 4.3 (Norm, trace and discriminant)**.** For a number field K of degree n, given an element $\alpha \in K$, its norm is defined as the product

$$N(\alpha) = \sigma_1(\alpha) \cdots \sigma_n(\alpha), \tag{4.1}$$

and the trace is

$$Tr(\alpha) = \sigma_1(\alpha) + ... + \sigma_n(\alpha). \tag{4.2}$$

The discriminant of K, denoted Δ_K is the square of the determinant of the following matrix:

$$\begin{pmatrix} \sigma_1(\theta_1) & ... & \sigma_n(\theta_1) \\ \vdots & \ddots & \vdots \\ \sigma_1(\theta_n) & ... & \sigma_n(\theta_n) \end{pmatrix},$$

where $\{\theta_1, ...\theta_n\}$ is an integral basis of $\mathcal{O}_K$. Notice that since lattice base-change matrices are unimodular, the definition does not depend on the choice of the basis[6].

Example 4.4 ([42] Prop. 2.7)**.** Let K_n denote the n-th cyclotomic field. Then, the discriminant of K equals

$$\Delta_{K_n} = (-1)^{\phi(n)/2} \frac{n^{\phi(n)}}{\prod_{p|n} p^{\frac{\phi(n)}{p-1}}}.$$

Norm and trace and discriminant are rational numbers Moreover, they are integers when restricted to $\mathcal{O}_K$.

4.3. **Ideals and ideal lattices.** Recall that an ideal of a ring R is an additive subgroup $I \subseteq R$ such that for each $\alpha \in R$ and each $\beta \in I$, it is $\alpha\beta \in I$. For instance, for $d \equiv 1 \pmod 4$, the subring $\mathbb{Z}[\sqrt{d}]$ is not an ideal of the ring of integers, just a subring with finite index.

Unlike $\mathbb{Z}$, in the ring of integers $\mathcal{O}_K$ of a number field K, it is not true that every element $\alpha \in \mathcal{O}_K$ is a unique product, up to order and units, of different irreducible elements[7]. For example, in $\mathbb{Z}[\sqrt{-6}]$, we have $6 = 2 \cdot 3 = \sqrt{-6} \cdot \sqrt{-6}$, where $2, 3$ and $\sqrt{-6}$ are irreducible elements. However, this generalisation holds if we replace *(irreducible) elements* by *(prime) ideals*:

Theorem 4.4 ([41], Theorem 5.6)**.** *$\mathcal{O}_K$ is a Dedekind domain. In particular, for each ideal $I \subseteq \mathcal{O}_K$, there exist unique prime ideals $\mathfrak{p}_1, ..., \mathfrak{p}_r$ and unique integers $e_1, ..., e_r \in \mathbb{Z}_{\geq 0}$ such that*

$$I = \mathfrak{p}_1^{e_1} ... \mathfrak{p}_r^{eg_r}.$$

Moreover, denoting $f_i = |\mathcal{O}_K/\mathfrak{p}_i|$, for $i = 1, ..., r$, it is

$$n = e_1 f_1 + ... + e_r f_r.$$

Example 4.5. In $\mathbb{Z}[\sqrt{-17}]$, we can express the principal ideal $\langle 18 \rangle$ as the product $\mathfrak{p}_1^2 \mathfrak{p}_2^2 \mathfrak{p}_3^2$, with $\mathfrak{p}_1 = \langle 2, 1 + \sqrt{-17} \rangle$, $\mathfrak{p}_2 = \langle 3, 1 + \sqrt{-17} \rangle$ and $\mathfrak{p}_3 = \langle 3, 1 - \sqrt{-17} \rangle$.

Definition 4.5. Let $p \in \mathbb{Z}$ be a rational prime decomposed as $(p) = \mathfrak{p}_1^{e_1} ... \mathfrak{p}_r^{e_r}$ in $\mathcal{O}_K$ with $\mathfrak{p}_i$ prime ideals. The number e_i is called the ramification index of p at $\mathfrak{p}_i$ and if $e_i > 1$, then p is said to ramify at $\mathfrak{p}_i$. The number $f_i = |\mathcal{O}_K/\mathfrak{p}_i|$ is called inertia degree of p at $\mathfrak{p}_i$. If $r = n$, then all the e_i and f_i equal 1 and p is said to be totally split.

A theorem by Minkowski states that every number field has only finitely many ramifying primes, which are precisely the rational primes dividing the discriminant. Hence, going back to Example 4.4, we see that for the $n - th$ cyclotomic field the ramifying primes are those which divide n.

[6] In most algebraic number theory texts our Δ_k is called the minimal discriminant, since it is possible to define such a determinant for each K-basis (not necessarily integral). We will only consider integral bases and minimal discriminants.

[7] An element α of a ring R is irreducible if for any $\beta, \gamma \in R$ such that $\alpha = \beta\gamma$, either β or γ is a unit.

Definition 4.6. Let R be a discrete ring (free and finitely generated as abelian group) and $\sigma : R \to \mathbb{R}^n$ an additive monomorphism. Nottice that $\sigma(R)$ is a lattice. The family of ideal lattices (for the ring R and embedding σ) is the set of all lattices $\sigma(I)$ for ideals I in R.

For instance, for $R = \mathbb{Z}[x]/f(x)$, the coefficient embedding maps any element of R to the integer vector in $\mathbb{Z}^n$ whose coordinates are exactly the coefficients of that element when viewed as a polynomial residue. When $R = \mathcal{O}_K$, the canonical embedding σ provides in a natural way an ideal lattice for each ideal I of R.

Notice that for the canonical embedding, multiplication and addition are preserved componentwise. On the contrary, for instance, for the ring $R = \mathbb{Z}[x]/(x^n + 1)$, the componentwise multiplication in $\mathbb{Z}_q^n$ doesn't correspond with multiplication in R: multiplying by x, is equivalent to shifting the coordinates and negate the independent term. This is one of the advantages of using the canonical embedding.

Moreover, one has the following connection between the fundamental parallelotope of $\sigma(\mathcal{O}_K)$ and the discriminant Δ_K:

Theorem 4.7 ([41], cf. Theorem 8.1)**.** *Assume that the number field K has s pairs of complex embeddings. Then, the Euclidean measure of the fundamental parallelotope of $\sigma(\mathcal{O}_K)$ equals $2^s\sqrt{\Delta_K}$.*

5. Ring learning with errors: problems, cryptosystem and key exchange

To define the ring learning with errors problem (RLWE), let K be a number field of degree n and ring of integers $\mathcal{O}_K$, regarded as a lattice in $\mathbb{R}^n$, by means of the canonical embedding. Closely connected with RLWE is the polynomial learning with errors problem (PLWE). Next we formally introduce both problems and explore their relation.

5.1. **Statement of the problems.** In the rest of this subsection $f(x) \in \mathbb{Z}[x]$ is supposed to be a monic irreducible polynomial of degree n and q is a rational prime which we will choose later. Define, further, $\mathcal{O} := \mathbb{Z}[x]/(f(x))$, which can also be regarded as a lattice in $\mathbb{R}^n$ by means of the coordinate embedding

$$\begin{array}{rcl} \sigma : \mathcal{O} & \to & \mathbb{R}^n \\ \sum_{i=0}^{n-1} a_i \overline{x}^i & \mapsto & (a_0, ..., a_{n-1}). \end{array} \tag{5.1}$$

Each root α of f defines a number field $K_\alpha = \mathbb{Q}(\alpha)$. Moreover, the ring $\mathbb{Z}[\alpha]$ is a finite index suborder of the ring of integers $\mathcal{O}_{K_\alpha}$. The restriction of the canonical embedding to $\mathbb{Z}[\alpha]$ also provides a lattice in $\mathbb{R}^n$. A very common choice is $f(x) = x^{2^k} + 1$, the 2^{k+1}-th cyclotomic polynomial (cf. [40]).

The n-dimensional torus attached to $\mathcal{O}_K$ is $\mathbb{T} := (K \otimes_{\mathbb{Q}} \mathbb{R})/\mathcal{O}_K$, and the f-torus is defined to be $\mathbb{T}_f := \mathbb{R}_q[X]/(f(X))$, with $\mathbb{R}_q := \mathbb{R}/\mathbb{Z}$. As in Lemma 3.6, there are embeddings $\mathcal{O}_K/q\mathcal{O}_K \hookrightarrow \mathbb{T}$ and $\mathcal{O}/q\mathcal{O} \hookrightarrow \mathbb{T}_f$.

Definition 5.1 (RLWE and PLWE-oracles)**.**

1. Let χ be a discrete random variable with values in $\mathcal{O}_K/q\mathcal{O}_K$ (which we regard as taking values in $\mathbb{T}$). For $s \in \mathcal{O}_K/q\mathcal{O}_K$ chosen uniformly at random, a RLWE-oracle with respect to s and χ is a probabilistic algorithm $A_{s,\chi}$ which, at each execution performs the following steps:
   1. Samples an element $a \in \mathcal{O}_K/q\mathcal{O}_K$ uniformly at random,
   2. Samples an element e from χ,
   3. Outputs the pair $(a, as + e) \in \mathcal{O}_K/q\mathcal{O}_K \times \mathbb{T}$.

2. Let $f(x) \in \mathbb{Z}[x]$ be monic irreducible as above and χ a discrete random variable with values in $\mathcal{O}/q\mathcal{O}$ (which we regard as taking values in $\mathbb{T}_f$) . For $s \in \mathcal{O}/q\mathcal{O}$ chosen uniformly at random, a PLWE-oracle with respect to s and χ is a probabilistic algorithm $A_{s,\chi}$ which, at each execution performs:
   1. Samples an element $a \in \mathcal{O}/q\mathcal{O}$ uniformly at random,
   2. Samples an element e from χ,
   3. Outputs the pair $(a, as + e) \in \mathcal{O}/q\mathcal{O} \times \mathbb{T}_f$.

Definition 5.2 (The RLWE/PLWE problem)**.** Let χ be a discrete random variable with values in $\mathcal{O}_K/q\mathcal{O}_K$ (in $\mathcal{O}/q\mathcal{O}$). The RLWE (PLWE) problem for χ is defined as follows:

a) Search version: for an element $s \in \mathcal{O}_K/q\mathcal{O}_K$ ($\mathcal{O}/q\mathcal{O}$) chosen uniformly at random and a RLWE (PLWE)-oracle $A_{s,\chi}$, if an adversary is given access to arbitrarily many samples $(a_i, a_i s + e_i)$ of the RLWE (PLWE) distribution, this adversary must recover s with non-negligible advantage.

a) Decisional version: for an element $s \in \mathcal{O}_K/q\mathcal{O}_K$ ($\mathcal{O}/q\mathcal{O}$) chosen uniformly at random and a RLWE (PLWE)-oracle $A_{s,\chi}$, the adversary is asked to distinguish, with non-negligible advantage, between arbitrarily many samples from $A_{s,\chi}$ and the same number of samples (a_i, b_i), taken uniformly at randon from $\mathcal{O}_K/q\mathcal{O}_K \times \mathbb{T}$ ($\mathcal{O}/q\mathcal{O} \times \mathbb{T}_f$).

Some words on the class of distributions we will use from now: first, notice that if q is totally split, what we will frequently assume, a RLWE-sample can be seen as an n-tuple of coordinates with values in $\mathbb{F}_q$. However, such a RLWE-sample is indeed *much more* than n LWE-samples: $\mathcal{O}_K/q\mathcal{O}_K$ is not only an $\mathbb{F}_q$- vector space; it also has a ring structure. The flexibility and power of RLWE comes from exploiting the ring structure instead of the sheer lattice structure. This is the reason why instead of taking n-independent discrete one-dimensional Gaussians, we rather use an n-dimensional one.

As in the 1-dimensional case, the mean will also be supposed 0, but in the RLWE scenario, the variance-covariance matrix (or rather, the multidmensional parameter) is normallly chosen, depending on the application, a) either to be diagonal, which is referred to as saying that the distribution is elliptic[8], or b) to have the diagonal elements bounded in absolute value by $\alpha n^{1/4}$, for α a parameter which will be made explicit in the next theorem, which backs the security of the decisional RLWE-problem (hence of the search RLWE-problem) in the security of the SVP over ideal lattices.

Hence, from now on, we assume that χ_α is an elliptic n-dimensional discrete $\mathbb{T}$-valued Gaussian of 0-mean and the elements of the diagonal are bounded as explained. The details are delicate and can be omited in a first study, since the aforementioned bound is what really matters for most proofs, but the reader is referred to [28], p. 19 for more information.

Theorem 5.3 ([28], page 19)**.** *Let K be the m-th cyclotomic number field of degree $n = \phi(m)$ and $R = \mathcal{O}_K$ its ring of integers. Let $\alpha < \sqrt{\log n/n}$ and let $q = q(n) \geq 2$, $q \equiv 1 \pmod{m}$ be a prime bounded by a polynomial in n such that $\alpha q \geq \omega(\sqrt{\log n})$[9]. There is a polynomial time quantum reduction from $\tilde{O}(\sqrt{n}/\alpha)$-SVP on ideal lattices of K to the decisional RLWE problem for K and χ_α.*

The proof consists of two parts: the first is a quantum reduction from worst case approximate SVP on ideal lattices to the search version of RLWE. The reduction works

[8]This is useful when carrying out security-reduction proofs.

[9]A function $f : \mathbb{N} \to \mathbb{R}$ is $\omega(g)$, for $g : \mathbb{N} \to \mathbb{R}$ (denoted as $f = \omega(g)$) if for each integer $k > 0$ there exists an integer $n_0 > 0$ such that for each $n \geq n_0$, it is $|f(n)| \geq k|g(n)|$. The notation $f(n) \geq \omega(g(n))$ means that the asymptotic behaviour of f is at least as fast as $\omega(g(n))$.

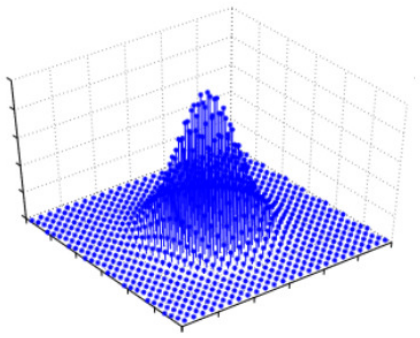


FIGURE 4. Discrete bivariate normal distribution supported on a lattice. Source: [35], with permission given by the author.

in general, not for just cyclotomic number fields. It uses the iterative quantum reduction for general lattices in [35] as a black box, the main effort being the classical (non-quantum) part, which requires a careful handling of the canonical embedding and a smart use of the Chinese Remainder Theorem.

The second part shows that the RLWE distribution is pseudorandom via a classical reduction from the search version, which has been shown at least as hard as SVP for ideal lattices in the first part. It uses the fact that the cyclotomic field is Galois and the fact that $q \equiv 1 \pmod{n}$, namely, that the ideal qR splits totally into n different prime ideals in R.

In [34] Theorem 6.2, the authors build on the same number-theoretical kind of arguments as in [28] to prove an analogue of Theorem 5.3 for non-cyclotomic Galois number fields.

5.2. **Equivalence between formulations.** In [28], the RLWE problem is introduced via $\mathcal{O}_K^\vee/q\mathcal{O}_K^\vee$ as sample space, instead of $\mathcal{O}_K/q\mathcal{O}_K$, where $\mathcal{O}_K^\vee$ means the dual of $\mathcal{O}_K$ with respect to the trace map, namely:

$$\mathcal{O}_K^\vee = \{\alpha \in K : Tr(\alpha) \in \mathbb{Z}\}.$$

We have avoided this formulation to spare the definition of the different ideal and, no less important, for the sake of the extension of our presentation. In any case, both formulations are equivalent ([37] Theorem 2.13). By equivalence we mean that every solution for primal-RLWE can be turned in polynomial time into a solution for dual-RLWE (and viceversa, but this is immediate, since $\mathcal{O}_K \subseteq \mathcal{O}_K^\vee$), incurring in a noise increase which is polynomial in the number field degree.

Before speaking about the RLWE/PLWE equivalence we need to introduce a key concept: the condition number, which measures the distortion between the lattices given by the canonical embedding and the coordinate embeding. Let's do that.

For a monic irreducible polynomial of degree n, $f(x) \in \mathbb{Z}[x]$ and θ a root of $f(x)$, consider again the subring $\mathbb{Z}[x]/(f(x)) \cong \mathbb{Z}[\theta] \subseteq \mathcal{O}_K$. As lattices, $\mathbb{Z}[x]/(f(x))$ is endowed with the coordinate embedding while $\mathbb{Z}[\theta]$ is endowed with the canonical embedding inherited from $\mathcal{O}_K$, and the evaluation-at-θ morphism causes a distortion between both.

Explicitly, the transformation between the embeddings is given by

$$\begin{array}{rcl} V_f : \mathbb{Z}[x]/(f(x)) & \to & \sigma_1(\mathcal{O}_K) \times \cdots \times \sigma_n(\mathcal{O}_K) \\ \sum_{i=0}^{n-1} a_i \overline{x}^i & \mapsto & \begin{pmatrix} 1 & \theta_1 & \cdots & \theta_1^{n-1} \\ 1 & \theta_2 & \cdots & \theta_2^{n-1} \\ \vdots & \vdots & \ddots & \vdots \\ 1 & \theta_n & \cdots & \theta_n^{n-1} \end{pmatrix} \begin{pmatrix} a_0 \\ a_1 \\ \vdots \\ a_{n-1} \end{pmatrix}, \end{array} \tag{5.2}$$

where $\theta = \theta_1, \theta_2, ..., \theta_n$ are the Galois conjugates of θ. As we see, the transformation V_f is given by a Vandermonde matrix.

For any matrix $A = (a_{ij}) \in M_{n\times n}(\mathbb{C})$, denote its transposed conjugate by A^*. The Frobenius norm is defined as

$$||A|| := \sqrt{Tr(AA^*)} = \sqrt{\sum_{i,j=1}^{n} |a_{ij}|^2}. \tag{5.3}$$

The noise provoked by V_f will remain *controlled* whenever $||V_f||$ and $||V_f^{-1}||$ remain so, and the product $||V_f||||V_f^{-1}||$ serves as a reasonable measure of this control (cf. [37] Ch. 4).

Definition 5.4. The condition number of an invertible matrix $A \in \mathrm{M}_n(\mathbb{C})$ is defined as $\mathrm{Cond}(A) := ||A|||A^{-1}||$.

Thus, in the monogenic case, the problem of the equivalence is the problem of showing that $Cond(V_f) = O(n^r)$ for some r independent of n. The non-monogenic case needs an intermediate reduction that we will not address here.

In the above mentioned paper [37], the authors introduce the framework to study the RLWE/PLWE-equivalence in general and prove it for the following family of polynomials:

Theorem 5.5 ([37], pag. 4 and Theorem 4.7)**.** *There is a polynomial time reduction algorithm from RLWE over $K_{f_{n,p}}$ to PLWE for $f_{n,p}(x)$ where $K_{f_{n,p}}$ is the splitting field of $f_{n,p}(x) = x^n + xp(x) - r$ where $n \geq 1$, $p(x)$ runs over polynomials with $deg(p(x)) < n/2$ and r runs over primes such that $25||p||_1^2 \leq r \leq s(n)$, with $s(x)$ a polynomial. Notice that there is a trivial reduction from PLWE to RLWE.*[10]

The argument to prove this theorem is, first, to consider the family of polynomials $\phi_{n,a}(x) := x^n - a$, with $a \in \mathbb{Z} \setminus \{0\}$ square-free. Denoting by $K_{\phi_{n,a}}$ the splitting field of $\phi_{n,a}(x) := x^n - a$, the authors check in first place the equivalence for $K_{\phi_{n,a}}$ and they show, via a careful use of Rouché theorem, that when $\phi_{n,a}(x)$ is perturbed by adding another polynomial with degree smaller than $n/2$ the roots of both polynomials are close enough.

A reason to be interested in such an equivalence is that working with polynomial rings instead of rings of integers of number fields is more amenable for computer implementations. In [8], it is shown how the arithmetic of several polynomial rings leads to very efficient cryptographic designs.

5.3. **The cyclotomic case.** In practice, the number fields we are the most interested in cryptography are the cyclotomic number fields: they are very well understood and enjoy very nice arithmetic guatantees, like monogeneicity, which allows an amenable and efficient use for implementations. However, until recently, very little was known regarding the equivalence, apart from the power-of-two case: the ideas in [16] can be

[10] For $p(x) = \sum_{i=0}^{n} p_i x^i \in \mathbb{R}[x]$, the 1-norm is defined as $||p||_1 = \sum_{i=0}^{n} |p_i|$

applied to show the equivalence for cyclotomic number fields of degree $2^k p$ or $2^k pq$ with p, q primes and $q < p$. Besides that, the family in Theorem 5.5 is somehow artificially constructed, but, some of the ideas have been used by this author to give a partial proof of the equivalence in the cyclotomic case ([6]). This proof is, to our knowledge, the first given for general cyclotomic degree (but with the caveat of imposing a condition which we comment next).

Before that, let us examine first the power-of-two degree.

Theorem 5.6. *Let $n = 2^k$ and $m = \phi(n) = 2^{k-1}$. Then, the map V_{Φ_n} is a scaled isommetry. In addition, $Cond(V_{\Phi_n}) = m$.*

Proof. To see that V_{Φ_n} is a scaled isometry, observe that when we multiply V_{Φ_n} by its conjugate transposed, the elements over the diagonal in the product matrix are identically m, and outside the diagonal, the element in position (i, j) in the product matrix equals

$$\sum_{k=0}^{m-1} \zeta_i^k \overline{\zeta_j}^k = \frac{1 - \zeta_i^m \overline{\zeta_j}^m}{1 - \zeta_i \overline{\zeta_j}}.$$

But since ζ_i are n-primitive roots (and so are $\overline{\zeta_i}$), then $\zeta_i^m = -1$ and the sum vanishes. Hence, we have that

$$V_{\Phi_n} V_{\Phi_n}^* = mId,$$

and $m^{-1/2} V_{\Phi_n}$ is an isometry. For the condition number, we write $V_{\Phi_n}^{-1} = m^{-1} V_{\Phi_n}^*$, hence $||V_{\Phi_n}^{-1}|| = 1$. By Lemma 5.3, the result follows. □

The main result in [6] is a polynomial bound on the condition number for cyclotomic number fields which only depends on a) the number of different primes dividing the conductor and b) the degree of the number field, and what is more important, the dependence on the degree is polynomial once the number of different prime divisors has been fixed. Let us see how.

For $n \geq 1$, denote by $rad(n)$ the product of all the different primes dividing n (without exponents). For the n-th cyclotomic polynomial $\Phi_n(x)$, denote by $A(n)$ the maximum of all the coefficients in absolute value. For instance, for $n = p^r$, prime, $A(n) = 1$, and for $n = pq$, with p, q prime, all the coefficients are $0, \pm 1$, due to a classical result by Migotti, hence $A(n) = 1$. Our result is as follows:

Theorem 5.7 ([6] Thm. 3.10)**.** *Let $n \geq 1$ and $m = \phi(n)$. If $rad(n) = p_1 ... p_k$, then:*

$$Cond(V_{\Phi_n}) \leq 2 rad(n) n^{2^k + k + 2} A(n).$$

Proof. First, from the very definition, one has $||V_{\Phi_n}|| = m$. Second, we use the following identity, a proof of which can be found, for instance, in [42] Ch. 1:

$$\Phi_n(x) = \Phi_{rad(n)}(x^{\frac{n}{rad(n)}}), \tag{5.4}$$

which yields $A(n) = A(rad(n))$. The technical core of the result is a series of upper bounds for the entries w_{ij} of the inverse matrix $V_{\Phi_n}^{-1}$, of which the most important is:

$$|w_{ij}| \leq 2 rad(n) n^{2^k + k} A(n).$$

□

Now, to obtain the polynomial bound, we need to bound $A(rad(n))$, which we do with the aid of a classical result due to Bateman:

Theorem 5.8 (Bateman, [5]). *Let $n = p_1...p_k$ with $p_1 < ... < p_k$. Then*

$$A(n) \leq n^{2^{k-1}}.$$

We can now derive the polynomial bound:

Corollary 5.9 ([6] Cor. 3.11). *Let $k \geq 1$ be fixed. If n is the product of at most k different primes, then $Cond(V_{\Phi_n})$ is polynomial in n. More in general, let $\mathcal{F}_k$ be a family of cyclotomic polynomials whose degree is divisible by at most k different primes. Assume that $A(n) = \mathcal{O}(n^r)$ for polynomials in $\mathcal{F}_k$. Then,*

$$Cond(V_{\Phi_n}) = \mathcal{O}(n^{2^k+k+3+r}).$$

In [6], we also give a subexponential upperbound for the condition number if we do not fix the number of primes as well as more precise upper bounds for conductor divisible up to three primes. Namely:

Theorem 5.10. *For $n \geq 1$ and $m = \phi(n)$, the following bounds hold for the condition number of cyclotomic polynomial $\Phi_n(x)$:*

a) *([6] Thm. 4.1) If $n = p^k$ then*

$$Cond(V_{\Phi_n}) \leq 4(p-1)m.$$

b) *([6] Thm. 4.3) If $n = n = p^r q^l$ then*

$$Cond(V_{\Phi_n}) \leq 2\phi(rad(n))m^2.$$

c) *([6] Thm. 4.6) If $n = p^l q^s r^t$ then*

$$Cond(V_{\Phi_n}) \leq 2\phi(rad(n))^2 m^2.$$

In our proofs, apart from some of the ideas from [37], and some properties from cyclotomic polynomials from [42], we have used results from analytic number theory like the aforementioned Theorem 5.8 due to Bateman and for the case of two and three primes, results by Migotti and Bang ([4]). This should highlight the strong link between ring lattice-based cryptography and number theory.

5.4. **The LPR (Lyubashevsky, Peikert and Regev) RLWE-cryptosystem.**

Both RLWE and PLWE problems can be turned into public key cryptosystems, as we show next. We will focus in the PLWE version here. So, let $f(x) \in \mathbb{Z}[x]$ be a monic irreducible polynomial, q a prime and set $\mathcal{O} = \mathbb{Z}[x]/f(x)$. Let χ_α be an $\mathcal{O}/q\mathcal{O}$-valued discrete Gaussian (seen as taking values on $\mathbb{T}_f$) and as explained in the former subsection, we assume the parameter of χ_α upper bounded entry-wise by $\alpha n^{1/4}$ with $\alpha \leq \sqrt{log(n)/n}$ and $q = q(n)$ as in 5.3. Take n big enough so that $6\sqrt{log(n)/\sqrt{n}} < \frac{q}{4}$ (this will be used to grant the correctness of the cryptosystem).

Construction 5.11 (The PLWE cryptosystem).

1. Key generation: choose $a \in \mathcal{O}/q\mathcal{O}$ uniformly at random and choose s, e sampled from χ_α. The secret key will be s and the public key will be the pair $(a, b = as + e)$.
2. Encryption: take a plaintext z consisting of a stream of bits and regard it as a polynomial in $\mathcal{O}/q\mathcal{O}$, mapping each bit to a coefficient. Choose r, e_1, e_2 sampled from χ_α. Set $u = ar + e_1$ and $v = br + e_2 + \lfloor \frac{q}{2} \rfloor z$. The cyphertext is (u, v).
3. Decryption: On cyphertext (u, v), perform $v - us = er + e_2 - e_1 s + \lfloor \frac{q}{2} \rfloor z$ and round each coefficient either to zero or to $\lfloor \frac{q}{2} \rfloor$, whichever is closest mod q.

Proposition 5.12. *The PLWE cryptosystem is correct (i.e. decryption undoes encryption) and pseudorandom.*

Proof. For correctness, notice that for the chosen values of α, q and n, with arbitrarily large probability, the absolute values of the coefficients of $er + e_2 - e_1 s$ will be below $6\sqrt{log(n)/\sqrt{n}} < q/4$, so each bit of z can be recovered by checking if its position in $v - us$ is less than $\lfloor q/4 \rfloor$, in which case, we decrypt it as 0, and otherwise as 1, as in the LWE scheme.

For pseudorandomness, first note that RLWE samples are pseudorandom even when s is sampled from χ_α, by a transformation to the Hermite normal form. Therefore, public keys (a, b) are pseudorandom and we can replace them by a uniform pair in $\mathcal{O} \times \mathbb{T}_f$. The observations of a passive adversary are (a, u) and (b, v) which are also pseudorandom, since r is also sampled from χ_α. □

Example 5.1. For around 100 bits security, current implementations use a parameter set with number field degree $n = 256$, a 13-bit prime modulus q and a narrow discrete Gaussian distribution with diagonal entries upper-bounded by 4.5.

5.5. **A RLWE-based key exchange protocol.** Next we present a key exchange protocol based on RLWE and due to Ding ([15]). Earlier protocols for key transport were proposed by Peikert ([33]) in 2012 and by Zhang in 2014. This protocol takes place between two devices typically called *initiator* and *respondent*, which we will call Alice and Bob respectively, for the sake of tradition, both of which have access to a discrete Gaussian of parameter α and both of which know $m = \phi(n)$, a prime q, the n-th cyclotomic polynomial $\Phi_n(x)$, hence the rings $\mathcal{O} = \mathbb{Z}[x]/(\Phi_x(x))$ and $\mathcal{O}/q\mathcal{O}$, and another polynomial $a(x) \in \mathcal{O}/q\mathcal{O}$. These data can and must be assumed to be publically known. The algorithm uses the following two functions:

Definition 5.13 (Signalling and binary deletion functions)**.**
Let $E := \{-\lfloor \frac{q}{4} \rfloor, ..., 0, ..., \lfloor \frac{q}{4} \rfloor\}$. The signalling function, denoted Sig, is the characteristic function of $\mathbb{F}_q \setminus E$, namely $Sig(v) = 0$ if and only if $v \in E$, otherwise $Sig(v) = 1$. The binary deletion function is defined as

$$\begin{array}{ccc} Mod_2 : \mathbb{F}_q^2 & \longrightarrow & \mathbb{F}_2 \\ (v, w) & \mapsto & v - \frac{w}{2} \pmod 2. \end{array}$$

The signalling function *signals* the elements of E as *small*, returning 0, while the binary deletion function returns 0 on pairs $(v, w = Sig(v))$ corresponding to error bits, which belong to E (i.e. $w = 0$ and $v = 2k$). The steps of the protocol are as follows:

1. Alice initiates:
   - 1.1 Generates two polynomials s_A and e_A from the discrete Gaussian distribution χ_α.
   - 1.2. Computes $p_A = as_A + 2e_A$.
   - 1.3. Sends Bob the polynomial p_A.
2. Bob responds:
   - 2.1 Generates two polynomials s_B and e_B from the discrete Gaussian distribution χ_α.
   - 2.2. Computes $p_B = as_B + 2e_B$.
   - 2.3. Generates e'_B from χ_α and computes
   $$k_B = p_A s_B + 2e'_B = as_A s_B + 2e_A s_B + 2e'_B.$$
   - 2.4. Uses the signalling function to find $w = Sig(k_B)$ (applying Sig coefficient-wise to k_B)
   - 2.5 Performs $sk_B = Mod_2(k_B, w)$
   - 2. 6 Sends Alice (p_B, w).

3. Alice finishes:
   3.1 Generates e'_A from χ_α.
   3.2. Computes
$$k_A = p_B s_A + 2e'_A = a s_A s_B + 2 e_B s_A + 2 e'_A$$
   3.3. Alice performs $sk_A = Mod_2(k_A, w)$.

Notice that the elements k_A and k_B are only approximately equal, up to even errors, which allows the fuction Mod_2 to detect them. The Sig function indicates the region in which each coefficient of a polynomial lies and helps to make sure that the error terms in k_A and k_B do not result in different mod q operations.

With a carefull choice of the parameter α, it will be $sk_A = sk_B$ with overwhelming probability. The difficulty of breaking this scheme is that from p_A and/or p_B, which is the only thing which a passive adversary is supposed to see, to recover s_A and s_B, the adversary must break PLWE.

Remark 5.14. In November 2015, Alkim, Ducas, Pöpplemann, and Schwabe recommended the parameters $n = 1024$ and $q = 12289$ (see [1]). This represents a significant reduction in public key size over previous schemes, and was submitted to NIST with the name of NewHope. At the time of writing, NewHope has passed unbroken to the second round (see Section 7.3).

6. Attacks on RLWE

Detailed reports on the state of the art of attacks on the RLWE cryptosystem can be found in [18] and [32]. In [18] the authors discuss a list of open questions in algebraic number theory motivated by several attacks on RLWE. This interplay between cryptography and number theory constitutes a fruitful link which is expected to motivate a flow of results from each direction to the other.

On the other hand, in [32], a comprehensive review of the known attacks and vulnerable instantiations is carried out from a geometric viewpoint. We present, at our introductory level, only a few of these attacks and questions, working out some details. Within this subsection, we assume as usual that K is a number field of degree n, and in the PLWE setting, that the defining polynomial $f(x)$ splits totally over $\mathbb{F}_q[x]$. This is unnecessary but it will simplify the exposition, while keeping the essential facts.

6.1. **Reduction to LWE.** Let $\mathcal{B}$ be a $\mathbb{Z}$-basis of $\mathcal{O}$ such that its reduction modulo q, $\overline{\mathcal{B}}$, is an $\mathbb{F}_q$-basis of $\mathcal{O}/q\mathcal{O}$. Given $a \in \mathcal{O}/q\mathcal{O}$, multiplication by a is an $\mathbb{F}_q$-linear map described by a matrix $A_a \in \mathbb{F}_q^{n\times n}$ with respect to $\overline{\mathcal{B}}$. Hence, a public key $(a, b = as + e)$ has attached the pair $(A_a, \mathbf{b} = A_a\mathbf{s} + \mathbf{e})$, where $\mathbf{s}$ and $\mathbf{e}$ are, respectively, the coordinates of s and e with respect to $\overline{\mathcal{B}}$, which implies that one RLWE sample carries n LWE samples. A first attack is based on Case 2 in Section 3.2: if the j-th error coordinate with respect to $\overline{\mathcal{B}}$ does not wrap around $\mathbb{Z}$, namely, if $Pr_{e_j \leftarrow \chi}\left\{e_j \notin [\frac{1}{2}, \frac{1}{2})\right\}$ is small enough, we have errorless LWE in the j-th row of A_a, and with enough samples we can recover s with high probability.

Let now $\mathfrak{q} \subseteq \mathcal{O}_K$ a prime ideal above q of norm $N(\mathfrak{q}) = |\mathcal{O}_K/\mathfrak{q}|$ and let χ be a Gaussian distribution over $K_{\mathbb{R}} = K \otimes \mathbb{R}$. Given RLWE samples $(a, b = as + e)$ where $a \in \mathcal{O}_K/q\mathcal{O}_K$ and e taken from χ, we can reduce them modulo $\mathfrak{q}$ to obtain samples $(a' = a \pmod{\mathfrak{q}}, b' = b \pmod{\mathfrak{q}})$, with $b' = s'a' + e \pmod{\mathfrak{q}}$ with $s' = s \pmod{\mathfrak{q}}$, hence the secret now lies in a set of size $N(\mathfrak{q})$. The following analysis is due to Peikert (cf. [32] Section 3.2) and yields a potentially successful attack when $N(\mathfrak{q})$ is not too large:

1. Since reduction modulo $\mathfrak{q}$ takes uniform samples onto uniform samples, if χ modulo $\mathfrak{q}$ is detectably non-uniform, we have an attack against decission RLWE.

2. If χ has one or more coefficients that do not wrap around $\mathbb{Z}$, then we can attack search RLWE by reducing to errorless LWE and try arbitrarily many samples.

In all cases (both in LWE and RLWE), the insecurity of an instantiation is due to the fact that the error distribution is insufficiently well spread relative to the ring geometry, so, as in Section 3.2, the main lesson to learn here is that the error distribution should be taken with parameters as close as possible to those for which the the hardness theorem works (Theorem 5.3).

6.2. **Reduction and attack to PLWE.** A first fact to mention is that at the time of writing, there is no direct attack against RLWE, i.e., without a reduction to an attack on PLWE or LWE, as described in the previous subsection. So, all the attacks presented here attemp at breaking PLWE first and then to reduce RLWE to PLWE.

Theorem 6.1 (Elias et al. [18])**.** *If K satisfies the following six conditions, there is a polynomial time attack to the search version of the associated RLWE scheme:*

1. *$K = \mathbb{Q}(\beta)$ is Galois of degree n.*
2. *The ideal (q) splits totally in $\mathcal{O}_K$.*
3. *K is monogenic, i.e, $\mathcal{O}_K = \mathbb{Z}[\beta]$.*
4. *The transformation between the canonical embedding of K and the power basis representation of K is given by a scaled orthogonal matrix.*
5. *If f is the minimal polynomial of β, then $f(1) \equiv 0 \pmod{q}$.*
6. *The prime q can be chosen suitably large.*

The first two conditions are sufficient for the RLWE search-to-decision reduction in the case where $q \nmid [\mathcal{O}_K : \mathbb{Z}[\beta]]$, which is implied by the third condition. The third and fourth conditions are sufficient for the RLWE-to-PLWE reduction; indeed, the fourth condition can be relaxed to require that the condition number of the matrix describing the transformation between the embeddings is at most polynomial in n, as we discussed in the previous section.

Finally, the last two conditions are sufficient for the attack on PLWE. Unfortunately (for the attacker's point of view), it is difficult to construct number fields satisfying all six conditions simultaneously. Next, we explain the attack on PLWE if 5 and 6 hold.

Setting a s usual $\mathcal{O} = \mathbb{Z}[x]/(f(x))$, fix a public key $(a(x), b(x)) \in \mathcal{O}/q\mathcal{O} \times \mathbb{T}_f$ and a secret key $s(x) \in \mathcal{O}/q\mathcal{O}$, i.e $b(x) = a(x)s(x) + e(x)$ with $e(x)$ sampled from the discrete Gaussian χ.

For each root $\theta \in \mathbb{F}_q$ of $f(x)$, consider the projection $\pi_\theta : \mathcal{O}/q\mathcal{O} \to \mathbb{F}_q$ given by $p(x) \mapsto p(\theta)$. By *short vector* in $\mathcal{O}/q\mathcal{O}$ we refer to those with *small* coefficients, which in practice means that these are upper bounded, in absolute value, by $q/4$. For suitable parameter, these *short vectors* lie inside a prescribed region with non-negligible probability and are easy to recognise. However, for a pair $(a(x), b(x))$, it is difficult to check if it exists $r(x)$ and a short vector $e(x)$ such that $b(x) = a(x)r(x) + e(x)$, in which case the attacker would guess that $s(x) = r(x)$. The reason is that there are q^n possibilities for $s(x)$ to test, which is prohibitive.

By contrast, in a small ring like $\mathbb{F}_q$, it is easy to examine the possibilities for $s(\theta)$ exhaustively: we can loop through the possibilities for $s(\theta)$, obtaining for each guess s_θ, the putative value $e(\theta) = b(\theta) - a(\theta)s_\theta$. The Decision Problem for PLWE, then, is solved as soon as we can recognize the set of $e(\theta)$ that arise from the Gaussian with high probability.

Again, this is difficult in general, but if 5 holds, i.e., if $\theta = 1$ is a root of $f(x)$, the attacker has a chance:

Let us denote by $\mathcal{S} \subseteq \mathcal{O}/q\mathcal{O}$ the subset of polynomials that are produced by the Gaussian with non-negligible probability. This is a small set, due to the parameter

choice. However, $\mathbb{F}_q$ is also a much smaller set than $\mathcal{O}/q\mathcal{O}$ and one expects that generically, $\pi_\theta(\mathcal{S}) = \mathbb{F}_q$ or something very close. One says that in this case $\mathcal{S}$ *smears* across all of $\mathbb{F}_q$.

But we are supposing that $\theta = 1$. The polynomials $g(x) \in \mathcal{S}$ have small coefficients, and hence have small images $g(1) \in \mathbb{F}_q$. This is simply because n is much smaller than q, due to 6, so that the sum of n small coefficients is still small modulo q. These ideas can be turned into the following algorithm:

Algorithm 6.2. *Suppose $f(1) \equiv 0 \pmod q$. The input is a collection of pairs $\{(a_i(x), b_i(x)) \in \mathcal{O}/q\mathcal{O} \times \mathbb{T}_f\}_{i=1}^m$, where each sample is drawn either uniformly at random or from the PLWE distribution . The output is to decide, for each sample, from which distribution is taken, with non-negligible probability. The algorithm is as follows:*

1 *For $i = 1$ to m do*
Set $S = \mathbb{F}_q$. This is the first guess for $\pi_1(\mathcal{S})$, which will be updated after each iteration.
2 *For each $s \in S$ do*
2.1 *Compute $e_i := b_i(1) - sa_i(1)$;*
2.2 *If e_i is not small in absolute value modulo q, then conclude that the sample cannot be valid for s with nonnegligible probability, and update $S = S \setminus \{s\}$; Next s;*
3 *If $S = \emptyset$, conclude that the sample was random, otherwise declare the sample as valid;*
Next i;

Remark 6.3. Notice that in the inner loop, if the sample is valid, then $e_i = e_i(1) = \sum_{j=1}^{n} e_{ij}$, and if σ is the variance of χ (which is spherical with respect to our embedding, fixed beforehand), then, e_i is sampled from a discrete Gaussian distribution of zero mean and parameter $\sqrt{n}\sigma$. The region of non-negligible probability for this Gaussian, can be taken to be

$$\Lambda := \{s \in \mathbb{F}_q : |s| < n\sigma^2 \leq q/4\}.$$

Notice that the cyclotomic cases are protected against this attack: $\theta = 1$ is never a root modulo q of a cyclotomic polynomial of degree greater than 1 when q is sufficiently large. However, with minor modifications, it is possible to extend the former attack to the case where θ has small order modulo q. Indeed, denote by r the order of θ modulo q. For an unknown polynomial $e(x)$, to decide from a known value $e(\theta)$ if $e(x)$ is sampled from a Gaussian distribution in a similar fashion as in Remark 6.3 is more complicated. However, one can still take advantage of a small r, as we explain next.

For $e(x) = \sum_{i=0}^{n} e_i x^i$, set $n = rM + l$ with $0 \leq l \leq r-1$. Define $e_{Mr+k} = 0$ for $0 \leq k \neq l \leq r-1$ and write

$$e(\theta) = \sum_{i=0}^{r-1} \sum_{j=0}^{M} e_{jr+i} \theta^i.$$

If $e(x)$ is sampled from a multivariate Gaussian with variance very close to σ^2, then each term $\sum_{j=0}^{M} e_{jr+i}$ is sampled from a 1-dimensional Gaussian of variance very close to $(M+1)\sigma^2$. This defines a *smallness* region , which can be pre-stored as a look-up

table

$$\Lambda = \{\rho = \sum_{i=0}^{r-1}\sum_{j=0}^{M} \rho_{jr+i}\theta^i \subseteq \mathbb{F}_q : |\rho_{jr+i}| \leq (M+1)\sigma^2 \ll q/4\}$$

to look at, in order to guess tentative values of $e(\theta)$. With this observation, we can derive the following algorithm:

Algorithm 6.4. *Suppose $f(\theta) \equiv 0 \pmod q$. The input is a collection of pairs $\{(a_i(x), b_i(x)) \in \mathcal{O}/q\mathcal{O} \times \mathbb{T}_f\}_{i=1}^m$, where each sample is drawn either uniformly at random or from the PLWE distribution . The output is to decide, for each sample, from which distribution is taken, with non-negligible probability. The algorithm is as follows:*

1 *For $i = 1$ to m do*
Set $S = \mathbb{F}_q$;
2 *For each $s \in S$ do*
2.1 *Compute $e_i := b_i(\theta) - sa_i(\theta)$;*
2.2 *If $e_i \notin \Lambda$, then conclude that the sample cannot be valid for s with nonnegligible probability, and update $S = S \setminus \{s\}$;*
Next s;
3 *If $S = \emptyset$, conclude that the sample was random, otherwise declare the sample as valid;*
Next i;

Remark 6.5. The third attack described in [18] is based on the size of the residue of $e_i(\theta)$ modulo q. Although here the errors may take on all values in $\mathbb{F}_q$, it may still be possible to notice if the distribution of samples is not uniform. The attacking algorithm is built on a delicate probability bound in the case that $\theta \neq \pm 1$ and the order of θ modulo q is not small. For example, this third attack is successful for any irreducible polynomial of degree $n = 2^6$, with q of the order of 2^{50}, $\sigma = 8$ and $\theta = 2$.

6.3. **Some number theoretical open questions motivated by attacks on PLWE.** As seen before, being simultaneously Galois and monogenic, having $\theta = 1$ as a root of the minimal polynomial modulo q (or some other root of small order) and the non-smearing under the evaluation map π_α of the set of *small* vectors in $\mathcal{O}/q\mathcal{O}$ can be regarded as weakness conditions to build a RLWE-based cryptosystem. We give next a list of number theoretical problems which are motivated by the search of security in RLWE-based primitives and are still open, up to date.

Question 6.6. Are there any fields of cryptographic size (i.e. $n \geq 2^{10}$) which are Galois and monogenic, other than the cyclotomic number fields and their maximal real subfields? How can one construct such fields explicitly? Is it possible to test algorithmically both features?

Notice that for fields of cryptographic size, the discriminant is too big to test whether or not it is square free, hence to decide if it is monogenic. An algorithmic approach which circumvects this testing is not available at the time of writing. Although for fields of small degree, a complete characterisation may be feasible (sufficient and necessary conditions for a cubic number field have been found by Gras and Archinard), the situation is much different for large degree fields. For instance, cyclic extensions tend to be non-monogenic:

Theorem 6.7. *Any cyclic extension K of prime degree $n \geq 5$ is non-monogenic except for the maximal real subfield of the $(2l+1)$-th cyclotomic field.*

Another result in this direction is as follows:

Theorem 6.8. *Let $n \geq 5$ be relatively prime to $2, 3$. There are only finitely many abelian number fields of degree n that are monogenic.*

Question 6.9. Let θ be a root of $f(x)$ modulo q. For which subsets $\mathcal{S} \subseteq R_q$ it is $\pi_\theta(\mathcal{S}) = \mathbb{F}_q$? Or, at least, can one determine the conditions for non-smearing, like in the case when $\theta = 1$ and $\mathcal{S}$ is a set of *small* vectors in $\mathcal{O}/q\mathcal{O}$?

Finally, as seen before, polynomials with roots of small order modulo q should be avoided. Again, cyclotomic polynomials are safe for attacks built on small order roots, as their roots have maximal order. The problem here is as follows:

Question 6.10. For random polynomials $f(x)$ and random primes q for which $f(x)$ has a root α modulo q, what can one say about the order of α modulo q?

A special instance of this question is this well-known open problem:

Conjecture 6.11 (Artin)**.** *Each $a \in \mathbb{Z}$ is a primitive root modulo infinitely many primes q such that a is not a perfect square or -1 modulo 4. In fact the set of primes for which a is a primitive root has density*

$$\prod_{p \text{ prime}} \left(1 - \frac{1}{p(p-1)}\right).$$

7. Ring Learning With Errors signatures, homomorphic encryption and some NIST figures

7.1. **RLWE Digital Signatures.** We present here a 2012 scheme by Gunyesu, Lyubashevsky and Poppelman (GLP [21]). It has some advantages over more recent ecient post-quantum digital signature proposals such as BLISS and Ring-TESLA, but although not broken, GLP as originally proposed is no longer considered to oer strong levels of security. Building on GLP, A. Chopra presented GLYPH in 2017 another RLWE digital signature schemes: a special instantiation of GLP together with certain modification in the compressing and hash functions,. It is described in [13], where a throughout analysis on its resistance to signature forgery, key-recovery, exhaustive and meet-in-the middle attacks is carried out. However, the main ideas on how to use RLWE for secure signature is already contained in GLP, hence as a first contact with the topic we have chosen this scheme.

We use the same terminology and notions as in Definition 2.3 and subsequent discussion, to which we refer the reader. This scheme uses PLWE in the cyclotomic ring $R_q = \mathbb{F}_q[x]/(\Phi_n(x))$ with q an odd prime congruent to 1 mod 4 or a power of 2.

A first difference to mention here is that instead of discrete Gaussians, the coefficients of *small* polynomials are sampled uniformly from $\{-1, 0, 1\}$ modulo q. This version of RLWE, is called the Compact Knapsack Problem over ideal lattices, whose decisional version backs GLP. Secondly, the lengths of signatures must not exceed a prescribed parameter n, regardless of the size of the message to sign. To attain this, the scheme uses a) a hash function H[11], which accepts bit strings of arbitrary length and returns bit strings of bounded length, and b) a function F from the target of H to the set of polynomials of degree $m = \phi(n)$ with exactly k of their coefficients having absolute in ± 1 and the rest being zero such that the probability of mapping two hash outputs to the same sparse element is less than $1/2^\lambda$, where λ is a security parameter.

Hence, the procedure has a sampling rejection step, which ensures that the output signature is not exploitably correlated with the signer's secret key values: if the infinity norm of a signature polynomial exceeds a fixed bound, β, that polynomial will be

[11]A hash function is $H : \cup_{r \geq 1} \mathbb{F}_2^r \to \mathbb{F}_2^\kappa$ with fixed κ. In GLP/GLYPH, a common choice for H is the function SHA256.

discarded and the signing process starts again. This process will be repeated until the infinity norm of the signature polynomial is less than or equal $\beta = k - 1$, where k is the number of non-zero coefficients allowed in acceptable polynomials.

Third, it is necessary to fix an injective map $I : R_q \to \mathbb{F}_2^N$, with $N \gg 1$. Last, the maximum degree of the signature polynomials will be $m - 1$ so that there are m coefficients. Typical values for m are 512, and 1024. For $m = 1024$, GLYPH sets $q = 59393$, $b = 16383$ and $k = 16$. The scheme is as follows:

1. Key generation:
   - 1.1 Generate, uniformly, two small polynomials $s(x)$ and $e(x)$. The pair $(s(x), e(x))$ is the private key.
   - 1.2 Compute $t(x) = a(x)s(x) + e(x)$, with $a(x)$ chosen uniformly at random. The public key is $(a(x), t(x))$.
2. Signature generation:
   - 2.1 Input: a message $m(x) \in R_q$ and $(a(x), e(x), s(x))$
   - 2.2 Generate two small polynomials $y_1(x)$ and $y_2(x)$.
   - 2.3 Compute $w(x) = a(x)y_1(x) + y_2(x)$.
   - 2.4 Set $\omega = I(w(x))$ and $\mu = I(m(x))$.
   - 2.5 Compute $c(x) = F(H(\omega||\mu))$. The symbol $||$ denotes concatenation of strings.
   - 2.6 Compute $z_1(x) = s(x)c(x) + y_1(x)$ and $z_2(x) = e(x)c(x) + y_2(x)$.
   - 2.7 While the infinity norms of $z_1(x)$ or $z_2(x)$ is greater than β go to step 2.1.
   - 2.8 Output: $(c(x), z_1(x), z_2(x))$. Transmit the signature along with the message $m(x)$. Notice that we are not discussing here signatures of encrypted messages, which is a more sophisticated cryptographic functionality.
3. Signature verification:
   - 3.1 Input: $(c(x), z_1(x), z_2(x), m(x))$.
   - 3.2 Verify that the infinity norms of $z_1(x)$ and $z_2(x)$ do not exceed β. If not, reject the signature.
   - 3.3 Compute $w'(x) = a(x)z_1(x) + z_2(x) - t(x)c(x)$.
   - 3.4 Set $\omega' = I(w'(x))$ and $\mu = I(m(x))$.
   - 3.5 Compute $c'(x) = F(H(\omega'||\mu))$.
   - 3.6 Output: If $c'(x) \neq c(x)$ reject the signature, otherwise accept the signature as valid.

Notice that $a(x)z_1(x) + z_2(x) - t(x)c(x) = w(x)$, hence $c'(x) = c(x)$ if the signature is not tampered, hence the scheme is correct.

Remark 7.1. The private key $(s(x), e(x))$ can be represented in $2n \log_2(3)$ bits of memory, and the public key $a(x)s(x)+e(x)$ can be represented in $n \log_2(q)$ bits, which makes GLP feasible for practical implementations.

Remark 7.2. Both in [13] and in the earlier [21], the application of the hash function H may result unclear for a non experienced reader. The reason is that in what we have labeled steps 2.5 and 3.4, both schemes apply H, defined over a binary domain, to inputs which are not binary. This point is probably not taken very seriously by the experts, for all what matters is that H is a collision resistant function and, more important, that when it comes to comparing $H(\omega||\mu)$ with $H(\omega'||\mu)$, they can only be equal with overwhelming probability if and only if $\omega = \omega'$. But of course one needs to make binary the arguments $w(x)$ and $m(x)$ of H, and this is why we have fixed the innaccuracy by resourcing to a function I which injectively outputs binary strings on polynomial inputs and defined $\omega = I(w(x))$ and $\mu = I(m(x))$. In [21] page 6 it is discussed how forging a signature implies finding a collision on H.

7.2. **RLWE Homomorphic encryption.** Homomorphic encryption was first introduced by Rivest, Adleman and Dertouzos back in the 70's ([36]), where they raised the problem of constructing a fully homomorphic scheme (a *privacy homomorphism*, using their phraseology). This problem was solved by Craig Gentry in 2009 in its seminal paper [20], by using ideal lattices and (essentially) a modified version of PLWE. The possibility of cheap cloud computing and distributed storage has drastically changed how business and individuals process their data and although traditional encryption like AES are very fast, to perform even simple analytics on encrypted data requires either the cloud server to access the secret keys, leading to security concerns or to download the data, decrypt and operate, which is costly. Homomorphic encryption is the solution to this challenge.

Areas where homomorphic encryption has applications include e-voting systems ([12]) and processing or computing on encrypted health, financial or other kinds of sensitive data on external servers like cloud or distributed devices.

Homomorphic and fully homomorphic encryption(FHE) has already been introduced here in Definition 2.5, and Example 2.6 provides an example of a homomorphic but not non-fully homomorphic encryption scheme.

Examples 7.3. Another example of homomorphic encryption is the LWE cryptosystem. To avoid entering into technicalities, choose an odd prime q, so that 2 is invertible in $\mathbb{F}_q$. We observe that a LWE-oracle is *essentially* homomorphic: given a private key $s \in \mathbb{F}_q^n$, two uniformly sampled vectors $a_1, a_2 \in \mathbb{F}_q^n$ and two errors e_1, e_2 taken from a $\mathbb{T}$-valued random variable χ, of 0-mean and variance σ^2, we se that

$$(a_1, \langle a_1, s\rangle + e_1) + (a_2, \langle a_2, s\rangle + e_2) = (a_1 + a_2, \langle (a_1 + a_2), s\rangle + (e_1 + e_2)).$$

Essentially means that the sum $e_1 + e_2$ is taken from the variable 2χ, which has also 0-mean but variance $2\sigma^2$. This easy observation allows to define a homomorphic cryptosystem, which is a minor modification of Regev's scheme presented in Section 3. However, if we keep adding encryption of data, this results in amplifying the error of the final encrypted data, and when this error passes a certain threshold, decryption becomes impossible. This implies that the length of the arithmetic circuit must be known beforehand and the parameters must be set to meet this feature.

An analogous analysis as in the previous example shows that RLWE oracles are also essentially homomorphic both in the additive and multiplicative structure, where, again, essentially means that the error of the sum/product is an amplification of the individual errors of the encrypted data, hence, RLWE provides a FHE scheme, as we see next.

Definition 7.4 (The BGV cryptosystem ([11], Section 3.4))**.**
Denote $R = \mathbb{Z}[x]/(\Phi_n(x))$, with $\Phi_n(x)$ the n-th cyclotomic polynomial and set $R_N := R/NR$. Consider as the space of plaintexts the ring R_{p^r}, for fixed r and prime p. The scheme is parametrized by a sequence of decreasing moduli $q_L > q_{L-1} > ... > q_0$ such that $q_i \leq \min\left\{\sqrt{q_{i+1}}, \frac{q_{i+1}}{2}\right\}$ and an i-th level ciphertext is a vector $(v, w) \in R_{q_i}^2$.

1. Key generation: Chose $s \in R$ by sampling from a discrete Gaussian such that the probability of the set $\{0, \pm 1\}^{\phi(n)}$ is close enough to 1.
2. Encryption/Decryption: A plaintext $\alpha \in R_{p^r}$ is encrypted to $E(s, \alpha) = (p_0, p_1) \in R_{q_i}^2$ if and only if $p_0 + sp_1$ modulo q_i equals $\alpha + p^r\epsilon$ in R with $||\epsilon|| < q_i/p^r$ for some $i \in \{0, ..., L\}$.

Observe that adding or multiplying two i-level ciphertexts results in an $i + 1$-level ciphertext, so computations over level L-ciphertexts are not allowed, as they cannot be decrypted. Several recent refinements to this scheme have been proposed ([22]) and the topic is still under research.

A number of open-source implementations of homomorphic encryption are available. For instance, HELib, a widely used library from IBM that implements the BGV cryptosystem, SEAL, a Microsoft version, $\Lambda O\lambda$ (pronounced LOL), a Haskell library for ring-based lattice cryptography that supports FHE or PALISADE, a general lattice encryption library. it is possible to add new implementations after public review by contacting contact@HomomorphicEncryption.org. In sum, homomorphic encryption is already ripe for mainstream use but the lack of standardisation makes difficult to decide on which implementation to use.

7.3. **NIST figures.** In 2017, the American National Institute of Standards and Technology (NIST), launched an open call (`https://csrc.nist.gov/Projects/Post-Quantum-Cryptography`) to evaluate and standardize one or more quantum-resistant public-key cryptographic algorithms. In their own words:

The question of when a large-scale quantum computer will be built is a complicated one. While in the past it was less clear that large quantum computers are a physical possibility, many scientists now believe it to be merely a significant engineering challenge. Some engineers even predict that within the next twenty or so years sufficiently large quantum computers will be built to break essentially all public key schemes currently in use. Historically, it has taken almost two decades to deploy our modern public key cryptography infrastructure. Therefore, regardless of whether we can estimate the exact time of the arrival of the quantum computing era, we must begin now to prepare our information security systems to be able to resist quantum computing.

The deadline for submission was November 30, 2017. The total number of submissions (for encryption, key exchange and signatures) was 71. In the first round, 14 submissions were attacked or withdrawn. Of the remaining 57, some of the proposals (mainly code-based ones) did merge. Taking this into account, 50 proposals remained unbroken. Some of them were found to have non-fatal attacks, which can be avoided with a right choice of parameters, also in the first round.

Of these 50 proposals: 9 were code-based, 21 lattice-based, 2 hash-based , 9 multivariate-based, 1 supersingular isogeny Diffie-Hellman (SIDH) key-exchange protocol. The remaining 8 submissions were hybrid or based on problems such as random walks (1), braids (2), Chebychev polynomials (1) or hypercomplex numbers (1).

In January 2019, a second round started and taking into account the attacks and feedback to the surviving proposals of the first round, 26 proposals have passed this new sieve. The numbers of remaining proposals (at the time of writing) within each category are listed in Table 1, constructed out of data from `https://www.safecrypto.eu/pqclounge/`:

Addendum: in October 2nd of 2020, the third round phase has started. Comments for the surviving candidates can still be submitted.

References

[1] E. Alkim, L. Ducas, T. Pöppelmann, P. Schwabe. *Post-quantum key exchange: a new hope.* Proceedings of the 25th USENIX Security Symposium (2016), 327–343.

[2] M. H. Alsuwaiyel. *Algorithms: Design Techniques and Analysis.* World Scientific, (1999).

[3] S. Arora, R. Ge. *New algorithms for learning in presence of errors.* In Automata, Languages and Programming, Springer, (2011) 403–415.

[4] A.S. Bang: *Om ligningen $\Phi_m(X) = 0$.* Nyt tidsskrift for Matematik, Afdeling B (1895), 6–12.

[5] P.T. Bateman: *On the size of the coefficients of the cyclotomic polynomial.* Seminaire de Théorie des Nombres de Bordeaux, 11 (28) (1982) 1–18.

[6] I. Blanco-Chacón. *On the RLWE/PLWE equivalence for cyclotomic number fields.* To appear in Applicable Algebra in Engineering, Communications and Computing, 2020 (available in arxiv: `https://arxiv.org/abs/2001.10891`)

Category	Number of proposals
Code-based (Hamming)	5
Code-based (rank metric)	2
Lattice-based (LWE)	1
Lattice-based (RLWE)	6
Lattice-based (PLWE)	1
Lattice-based (Other)	4
Multivariate-based	4
Hash-based	1
Supersingular isogeny-based	1
Other	1

TABLE 1. NIST proposals. Second Round.

[7] D. Boneh, V. Shoup. *A graduate course in applied cryptography*, 2020 https://crypto.stanford.edu/~dabo/cryptobook/BonehShoup_0_5.pdf

[8] D.J. Bernstein, C. Chuengsatiansup, T. Lange, C. van Vredendaal: *NTRU Prime* (2016). http://eprint.iacr.org/2016/461

[9] P. E. Boas. *Another NP-Complete Problem and the Complexity of Computing Short Vectors in a Lattice.* Tech. Report 81-04, Mathematische Instituut, University of Amsterdam, 1981.

[10] M. Braithwaite. *Experimenting with post-quantum cryptography.* Google Security Blog, 2016. https://security.googleblog.com/2016/07/experimenting-with-post-quantum.html

[11] Z. Brakersky, C. Gentry, V. Vaikuntanathan. (*Leveled) Fully Homomorphic Encryption without Bootstrapping.* https://people.csail.mit.edu/vinodv/6892-Fall2013/BGV.pdf

[12] I. Chillotti, N. Gama, M. Georgieva and M. Izabachéne. *An homomorphic LWE based e-voting scheme.* https://ilachill.github.io/papers/CGGI16a-An_homomorphic_LWE_based_E-voting_Scheme.pdf

[13] A. Chopra. GLYPH: *A New Instantiation of the GLP Digital Signature Scheme.* https://eprint.iacr.org/2017/766.pdf

[14] J. Ding, B.Y. Yang. *Multivariate public key cryptography.* https://link.springer.com/content/pdf/10.1007/978-3-540-88702-7_6.pdf

[15] J. Ding, X. Xiang, L. Xiaodong. *A Simple Provably Secure Key Exchange Scheme Based on the Learning with Errors Problem* (2012) https://eprint.iacr.org/2012/688.pdf

[16] L. Ducas, A. Durmus. *Ring-LWE in polynomial rings.* In PKC, 2012.

[17] N.C. Dwarakanath, S. D. Galbraith. *Sampling from discrete Gaussians for lattice-based cryptography on a constrained device.* Preprint: https://www.math.auckland.ac.nz/~sgal018/gen-gaussians.pdf

[18] Y. Elias, K. Lauter, E. Ozman, K. Stange. *Ring-LWE cryptography for the number theorist.* In: E. Eischen, L. Long, R. Pries, K. Stange (eds) Directions in Number Theory. Association for Women in Mathematics Series, vol 3. Springer 2016.

[19] L. de Feo: *Mathematics of isogeny based cryptography.* https://arxiv.org/pdf/1711.04062.pdf

[20] C. Gentry. *Fully Homomorphic Encryption Using Ideal Lattices. In the 41st ACM Symposium on Theory of Computing (STOC)*, 2009.

[21] T. Guneysu, V. Lyubashevsky and T. Poppelmann. *Practical lattice-based cryptography: A signature scheme for embedded systems.* https://www.iacr.org/archive/ches2012/74280529/74280529.pdf

[22] S. Halevi, V. Shoup. *Faster Homomorphic Linear Transformations in HElib.* https://eprint.iacr.org/2018/244.pdf

[23] D. Harvey. *Faster arithmetic for number-theoretic transforms.* J. Symb. Comput., 60, (2014), 113119.

[24] J. Hoffstein, J. Pipher, J. H. Silverman. *NTRU: A ring-based public key cryptosystem. ANTS-III*, (1998), 267-288.

[25] A. Joux A, R. Lercier. *Number Field Sieve for the DLP.* In: van H.C.A. Tilborg, S. Jajodia (eds) Encyclopedia of Cryptography and Security. Springer, Boston (2011).

[26] N. Kobliz. *P-adic numbers, p-adic analysis, and zeta-functions.* Graduate texts in Mathematics, n. 58. Springer 1984.

[27] R.Le Clercq, S. S. Roy, F. Vercauteren, I. Verbauwhede. *Efficient software implementation of RLWE encryption.* https://eprint.iacr.org/2014/725.pdf
[28] V. Lyubashevsky, C. Peikert, O. Regev. *On ideal lattices and learning with errors over rings.* In: Gilbert H. (eds) Advances in Cryptology EUROCRYPT 2010. Lecture Notes in Computer Science, 6110. Springer.
[29] A. Menezes, T. Okamoto and S. Vanstone. *Reducing elliptic curve logarithms to logarithms in a finite field. IEEE Transactions on Information Theory* 39(5), (1993) 1639–1646.
[30] D. Micciancio. *The shortest vector in a lattice is hard to approximate to within some constant.* In Proc.39th Annual IEEE Symposium on Foundations of Computer Science, 1998.
[31] R. Overbeck, N. Sendrier. *Code-based cryptography.* In: D.J. Bernstein, J. Buchmann, E. Dahmen (eds) Post-Quantum Cryptography (2009). Springer, Berlin, Heidelberg .
[32] C. Peikert. 4̂extitHow (not) to instantiate ring-RLWE. In Zikas, V.; de Prisco, R. (eds.) SCN 2016, LNCS vol 9841, pags. 411–430 (2016) Springer.
[33] C. Peikert. *Lattice Cryptography for the Internet* (2014): https://eprint.iacr.org/2014/070.pdf
[34] C. Peikert, O. Regev, N. Stephens-Davidowitz. *Pseudorandomness of Ring-LWE for any ring and modulus.* In STOC, 2017.
[35] O. Regev. *On lattices, learning with errors, random linear codes and cryptography.* J. ACM, 56 (6), 2009.
[36] R. Rivest, L. Adleman, and M. Dertouzos. *On data banks and privacy homomorphisms.* In Foundations of Secure Computation, (1978), 169180.
[37] M. Rosca, D. Stehlé, A. Wallet. *On the ring-LWE and polynomial-LWE problems.* In: Nielsen J., Rijmen V. (eds) Advances in Cryptology EUROCRYPT 2018. Lecture Notes in Computer Science, vol 10820. Springer.
[38] M. Scott. *A note on the implementation of the Number Field Transform.* IMACC 2017. https://eprint.iacr.org/2017/727.pdf
[39] P. Shor. *Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer.* SIAM Journal on Computing, 26 (5), (1997), 1484–1509.
[40] D. N. Stehle, R. Steinfeld, K. Tanaka, K. Xagawa. *Efficient public key encryption based on ideal lattices.* In Advances in Cryptology ASIACRYPT (2009), 617–635.
[41] I. Stewart. *Algebraic number theory and Fermat's last theorem.* AK Peters Ltd, 2002.
[42] L. Washington. *Introduction to Cyclotomic Fields*, Graduate Texts in Mathematics, 83 (2 nd ed.), Springer-Verlag (1997).

Iván Blanco-Chacón is Assistant Professor at University of Alcalá de Henares. He was formerly a postdoctoral researcher at University College Dublin.

Department of Mathematics, School of Science, University of Alcalá de Henares, Ctra. Madrid-Barcelona Km. 33,600, Alcalá de Henares, Spain.
E-mail address: ivan.blancoc@uah.es

Irish Math. Soc. Bulletin
Number 86, Winter 2020, 47–77
ISSN 0791-5578

Linear Dynamical Systems

CLIFFORD GILMORE

Abstract. This expository survey is dedicated to recent developments in the area of linear dynamics. Topics include frequent hypercyclicity, $\mathcal{U}$-frequent hypercyclicity, reiterative hypercyclicity, operators of C-type, Li-Yorke and distributional chaos, and hypercyclic algebras.

1. Introduction

Chaos theory has been described in lay terms as the 'science of surprises' and in everyday usage chaos typically depicts something wild or a state of disorder. While this is adequate in ordinary parlance, it is natural to ask: what mathematically precise definition captures the essential properties of a chaotic dynamical system?

By a *dynamical system* we mean a pair (X, T), where X is a metric space and T is a continuous map acting on X. The investigation of dynamical systems is primarily concerned with the long term evolution of iterates of the map T, where n-fold iteration is denoted by

$$T^n = T \circ T \circ \cdots \circ T, \quad n \geq 0.$$

Devaney [65] suggested that (X, T) is chaotic if it possesses the following three characteristics.

1. It cannot be simplified.
2. It has some regularity.
3. Long term prediction is difficult.

He proposed these characteristics are captured by the following three mathematical properties.

The first characteristic of chaos corresponds to the notion of topological transitivity. A dynamical system (X, T) is said to be *topologically transitive* if for any pair of nonempty, open subsets $U, V \subset X$, there exists some $n \in \mathbb{N}$ such that

$$T^n(U) \cap V \neq \varnothing.$$

As illustrated in Figure 1, under the action of T every non-trivial part of X will eventually visit the whole space. This captures how the system cannot be simplified or reduced into smaller and potentially more manageable components.

To satisfy regularity, Devaney defined the second characteristic to be when the map T possesses a dense set of periodic points. A vector $y \in X$ is a periodic point for T if there exists $n \geq 1$ such that $T^n(y) = y$.

2020 *Mathematics Subject Classification.* 47A16, 46B87, 47-02.

Key words and phrases. Linear dynamics, chaos, hypercyclic, frequently hypercyclic, $\mathcal{U}$-frequently hypercyclic, reiteratively hypercyclic, Li-Yorke chaos, irregular vectors, distributional chaos, distributionally irregular vectors, operators of C-type, hypercyclic subspaces, hypercyclic algebras.

Received on 1-7-2020; revised 18-9-2020.

Support from the Irish Research Council via a Government of Ireland Postdoctoral Fellowship is gratefully acknowledged.

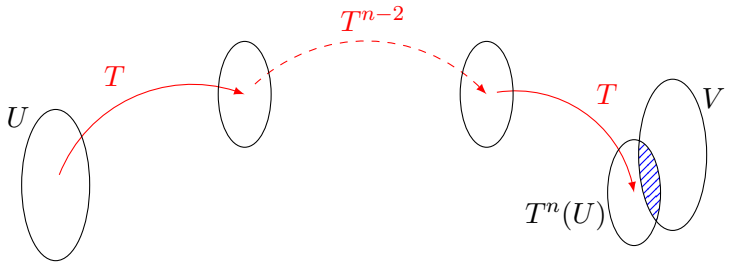


FIGURE 1. Topological transitivity.

The third characteristic of chaos corresponds to the notion of *sensitive dependence on initial conditions*, which is commonly referred to as the *butterfly effect*. It is considered the essence of chaos since it describes how small discrepancies in the initial state of the system may lead to vastly different outcomes. According to E. N. Lorenz, who is considered the father of chaos theory, it characterises 'when the present determines the future, but the approximate present does not approximately determine the future.' It explains, for instance, the difficulty in obtaining accurate long-term weather forecasts.

An elegant result by Banks et al. [8] demonstrated that sensitivity to initial conditions is redundant in Devaney's definition of chaos, since it follows automatically from the other two properties. So we define a dynamical system (X, T) to be *chaotic* if T is topologically transitive and T possesses a dense set of periodic points.

Chaos is typically viewed as a nonlinear phenomenon. Indeed, the field of classical dynamical systems investigates the mathematical rules governing the long-term evolution of nonlinear phenomena such as the weather, climate, turbulence and fluid dynamics. However, it is now well established that seemingly tractable linear systems may give rise to complex dynamical behaviour and linear chaos.

We say (X, T) is a *linear dynamical system* if X is a topological vector space and $T\colon X \to X$ is a continuous linear map. The central notion of linear dynamics is *hypercyclicity*, since when X is a separable, complete and metrizable topological vector space, the Birkhoff transitivity theorem gives that T is hypercyclic if and only if T is topologically transitive.

Linear dynamics began to receive systematic attention in the early 1990s following the pioneering work of Kitai [101], Gethner and Shapiro [74], and Godefroy and Shapiro [80]. It has since developed into a substantial branch of operator theory, which is evident from the monographs by Bayart and Matheron [22], and Grosse-Erdmann and Peris [98] that provide accessible and comprehensive introductions to the area.

This survey will primarily focus on advances that have occurred since publication of the books [22] and [98]. However, since this article is intended to be accessible to a wide mathematical audience, to ensure readability we begin by recalling the pertinent foundational concepts of linear dynamics. Thus, before we highlight recent progress we set the scene by mentioning some significant background (or dare we say *classical!*) results. Finally, it is not possible to attempt an exhaustive account of the field and the topics selected here are entirely influenced by the personal preferences of the author.

2. HYPERCYCLICITY

For clarity of the presentation we will mostly consider the setting of Banach or Hilbert spaces. Most of the definitions and results mentioned in the sequel can be appropriately extended to more general topological vector spaces such as Fréchet spaces. Where we consider it pertinent we will present results in this generality, so we remind the reader that a Fréchet space is a locally convex and completely metrizable topological vector

space. So unless otherwise stated, we let X be a separable Banach space and we denote by $\mathscr{L}(X)$ the space of continuous linear operators on X.

We say that $T \in \mathscr{L}(X)$ is *hypercyclic* if there exists $x \in X$ such that its T-orbit is dense in X, that is

$$\overline{\{T^n x : n \geq 0\}} = X.$$

Such an $x \in X$ is called a *hypercyclic vector* for T.

As briefly mentioned in the introduction, the Birkhoff transitivity theorem [45] states that an operator T is hypercyclic if and only if it is topologically transitive. This is a very useful result, and we note that in the course of the proof it employs a Baire category argument to show that the set of hypercyclic vectors for a hypercyclic operator forms a dense G_δ subset of X (cf. [22, Theorem 1.2]). We recall that a set is said to be G_δ if it is a countable intersection of open sets.

A prerequisite for hypercyclicity is that the space X is separable and furthermore hypercyclicity is a purely infinite-dimensional phenomenon, since linear operators cannot have dense orbits in the finite-dimensional setting. So we make a standing assumption that the spaces considered here are separable and infinite-dimensional.

The first examples of hypercyclic operators in the Banach and Hilbert space settings were identified by Rolewicz in 1969. For the convenience of the reader we recall, for $1 \leq p < \infty$, that the space ℓ^p of p-summable sequences is a separable Banach space when endowed with the norm $\|x\|_p = (\sum_{n=0}^{\infty} |x_n|^p)^{1/p}$, for the sequence $x = (x_n)$. The space c_0 is defined as the space of sequences with limit equal to zero, which is a separable Banach space when endowed with the sup-norm $\|x\| = \sup_{n\in\mathbb{N}} |x_n|$, for $x = (x_n)$. Rolewicz [124] proved in the setting $X = c_0$ or ℓ^p, $1 \leq p < \infty$, that scalar multiples of the backward shift $cB \in \mathscr{L}(X)$ are hypercyclic when $|c| > 1$. The *backward shift* $B \in \mathscr{L}(X)$ is defined as

$$B(x_1, x_2, x_3, \dots) = (x_2, x_3, x_4, \dots)$$

for $(x_n) \in X$. More generally, the *weighted backward shift* $B_w \in \mathscr{L}(X)$ is defined as

$$B_w(x_1, x_2, x_3, \dots) = (w_2 x_2, w_3 x_3, w_4 x_4, \dots)$$

where $w = (w_n)$ is a bounded sequence of nonzero scalars. For brevity we will simply refer to B_w as a weighted shift.

A complete characterisation of the hypercyclic weighted shifts was identified by Salas [125], who proved that B_w is hypercyclic on X if and only if

$$\sup_{n\geq 1} \prod_{j=1}^{n} |w_j| = \infty. \tag{2.1}$$

In [125] it was also shown that any perturbation $I + B_w$ of the identity operator I by a weighted shift B_w is hypercyclic on c_0 or ℓ^p, $1 \leq p < \infty$.

The notion of hypercyclicity also makes sense in the setting of more general topological vector spaces. In fact, the space $H(\mathbb{C})$ of entire functions that are holomorphic on the complex plane provided the first examples of functions that admit dense orbits under linear operators. We recall that $H(\mathbb{C})$ is a Fréchet space when endowed with the topology of local uniform convergence. Birkhoff [46] demonstrated in 1929 the existence of an entire function $f \in H(\mathbb{C})$ such that the sequence of translates $(f(\cdot + na))_{n\geq 1}$, for $a \neq 0$, forms a dense set in $H(\mathbb{C})$. MacLane [103] subsequently constructed in 1952 an entire function $f \in H(\mathbb{C})$ such that the sequence of derivatives $(f, f', f'', \dots)$ is dense in $H(\mathbb{C})$. We remark that the results from [46] and [103] were proven for the more general property of universality, which is briefly discussed in Section 2.1. In the language of linear dynamics these results give that translation operators $T_a \colon f(z) \mapsto f(z+a)$, for $a \neq 0$, and the differentiation operator $D \colon f \mapsto f'$ are hypercyclic on the space $H(\mathbb{C})$.

Some prevalent classes of operators that do not contain hypercyclic operators include contractions, finite-rank, nuclear, compact, quasinilpotent, strictly singular and Riesz operators. In the Hilbert space setting operators that are never hypercyclic include unitary, self-adjoint, normal, hyponormal, trace-class and Hilbert-Schmidt operators. An account of families of non-hypercyclic operators can be found in [98, Chapter 5].

Hypercyclicity is not, however, an anomalous phenomenon. It was independently demonstrated by Ansari [3] and Bernal [27] that every separable, infinite-dimensional Banach space supports a hypercyclic operator. This was generalised to the Fréchet space setting by Bonet and Peris [51], and Grivaux [84] subsequently proved that the result holds for the stronger property of mixing.

We say $T \in \mathscr{L}(X)$ is *mixing* if for any pair U, V of nonempty open subsets of X, there exists $N \in \mathbb{N}$ such that $T^n U \cap V \neq \varnothing$ for all $n \geq N$. Mixing is a strengthening of topological transitivity, so if T is mixing the Birkhoff transitivity theorem gives that T is hypercyclic.

We gather the existence results into the following theorem.

Theorem 2.1 (Ansari [3], Bernal [27], Bonet and Peris [51], Grivaux [84])**.** *Every separable, infinite-dimensional Fréchet space supports a mixing, and hence hypercyclic, operator.*

Since every separable, infinite-dimensional Banach space supports a hypercyclic operator, it is necessary that there exist hypercyclic operators that are compact perturbations of the identity, i.e. of the form

$$I + K,$$

where K is a compact (or even nuclear) operator. Such examples follow from results in [125], and they are quite remarkable since individually neither compact operators nor the identity can be hypercyclic. Another curious family of hypercyclic operators are the rank one perturbations of unitary operators acting on the Hilbert space ℓ^2 that were constructed by Grivaux [86]. This was a strengthening of a result by Shkarin [128], who constructed a rank two perturbation of a unitary operator acting on a Hilbert space.

Important classes of maps that contain hypercyclic operators include composition operators acting on function spaces such as the Hardy, Bergman and Dirichlet spaces. Composition and weighted composition operators are defined, respectively, as

$$f \mapsto C_\varphi f = f \circ \varphi, \qquad f \mapsto W_{\psi,\varphi} f = \psi \cdot f \circ \varphi$$

for fixed analytic maps φ and ψ. There exists a rich literature on the class of hypercyclic composition operators and an account of the fundamental results can be found in [98, Chapter 4]. To illustrate the theory we briefly mention the elegant characterisation of hypercyclic composition operators acting on the Hardy space $H^2(\mathbb{D})$. It was proven by Bourdon and Shapiro [56, 57] that C_φ is hypercyclic on $H^2(\mathbb{D})$ if and only if φ is an automorphism of the unit disc $\mathbb{D}$ with no fixed point in $\mathbb{D}$.

More recently Bayart [10], and Bayart and Charpentier [13] characterised the linear dynamical properties of C_φ acting on the Hardy space $H^2(\mathbb{B}^d)$, where φ a linear fractional map on the unit Euclidean ball $\mathbb{B}^d \subset \mathbb{C}^d$. Bonet and Domański [48] gave the following characterisation of the hypercyclic composition operators acting on the space $\mathscr{A}(\Omega)$ of real analytic functions on an open subset $\Omega \subset \mathbb{R}^d$. For φ a real analytic self-map of Ω, they proved that C_φ is hypercyclic on $\mathscr{A}(\Omega)$ if and only if φ is injective, φ' is never singular and φ is a runaway sequence on Ω. A map $\varphi\colon \Omega \to \Omega$ is said to be *runaway* if for every compact subset $K \subset \Omega$, there exists $n \in \mathbb{N}$ such that $\varphi^n(K) \cap K = \varnothing$.

In contrast, it was shown in [58] and [72] that the Fock and Schwartz spaces do not even support, respectively, supercyclic weighted and unweighted composition operators.

We say the operator $T \in \mathscr{L}(X)$ is *supercyclic* if there exists $x \in X$ such that its projective T-orbit is dense in X, that is

$$\overline{\{\lambda T^n x : n \geq 0,\ \lambda \in \mathbb{C}\}} = X.$$

Further significant classes of hypercyclic operators include adjoints of multipliers on spaces of holomorphic functions, generalisations of backward shifts acting on the Hardy and Bergman spaces (cf. [98, Chapter 4]), and Toeplitz operators acting on the Hardy space [9]. In the setting of $\mathscr{L}(X)$ and its separable ideals, hypercyclic properties of the class of elementary operators were investigated in [60] and [50]. As noted in [77, 75], some interesting questions remain open regarding the hypercyclicity of commutator maps and generalised derivations acting on separable Banach ideals of $\mathscr{L}(X)$.

An introduction to linear dynamics would be incomplete without mentioning the Hypercyclicity Criterion. It is a sufficient condition for hypercyclicity that has emerged as a powerful tool, since for a given operator it is not always straightforward to explicitly identify a hypercyclic vector. It was one of the principal results from Kitai [101], which was independently rediscovered by Gethner and Shapiro [74].

We say $T \in \mathscr{L}(X)$ satisfies the Hypercyclicity Criterion if there exist dense subsets X_0, $Y_0 \subset X$, an increasing sequence (n_k) of positive integers and maps $S_{n_k} : Y_0 \to X$, for $k \geq 1$, such that for any $x \in X_0$, $y \in Y_0$ the following hold as $k \to \infty$

(i) $T^{n_k} x \to 0$,

(ii) $S_{n_k}(y) \to 0$,

(iii) $T^{n_k} S_{n_k}(y) \to y$.

Note that the maps of the sequence S_{n_k} are not assumed to be self-maps of Y_0, linear or even continuous. If T satisfies the Hypercyclicity Criterion then T is hypercyclic (cf. [21, Theorem 1.6]). An elegant argument to prove this result shows that under the assumptions of the Hypercyclicity Criterion, the operator T is topologically transitive.

If T satisfies the Hypercyclicity Criterion for the full sequence $(n_k) = (k)$ of natural numbers, then T is mixing (cf. [98, Remark 3.13]). Moreover, Bès and Peris [44] proved that $T \in \mathscr{L}(X)$ satisfies the Hypercyclicity Criterion if and only if T is weakly mixing. We say $T \in \mathscr{L}(X)$ is *weakly mixing* if the direct sum $T \oplus T$ is hypercyclic on $X \oplus X$.

A long-standing open problem, originally posed in 1991 by Herrero [100], asked if T is hypercyclic does it follow that $T \oplus T$ is hypercyclic? (Equivalently, does T satisfy the Hypercyclicity Criterion?) The question was resolved in the negative in 2006 by de la Rosa and Read [64], who constructed a Banach space and a hypercyclic operator T such that T does not satisfy the (so-called!) Hypercyclicity Criterion. Bayart and Matheron [21] subsequently identified a family of hypercyclic, non-weakly mixing operators in the setting of the classical Banach spaces ℓ^p, for $1 \leq p < \infty$, which we note includes examples in the Hilbert space setting. A simplification of the counterexample from [21] can be found in [22, Section 4.2].

2.1. **Motivation.** While linear dynamics has developed into a substantial research area in its own right, we briefly mention here something about its origins.

One motivation for investigating hypercyclic operators grew from the *invariant subspace problem* and the study of cyclic operators. We say $T \in \mathscr{L}(X)$ is *cyclic* if there exists $x \in X$ (said to be a *cyclic vector* for T) such that the closed linear span of its T-orbit is dense in X, that is

$$\overline{\operatorname{span}}\{T^n x : n \geq 0\} = X.$$

The invariant subspace problem asks, given $T \in \mathscr{L}(X)$, does there always exist a non-trivial, closed T-invariant subspace $W \subset X$? The subspace W is T-invariant if $T(W) \subset W$ and it is said to be non-trivial if $W \neq \{0\}$ and $W \neq X$. Clearly T does not

possess a non-trivial closed invariant subspace if and only if every nonzero $x \in X$ is a cyclic vector for T.

A counterexample to the invariant subspace problem was constructed in 1976 by Enflo [67]. Read [121] subsequently identified an operator T, acting on the classical Banach space ℓ^1, such that every nonzero $x \in \ell^1$ is cyclic for T. However, the invariant subspace problem remains an open question in the Hilbert space and reflexive Banach space settings. We refer the interested reader to the monographs [120] and [59] for in-depth studies of this famous problem.

The invariant subspace problem naturally led research activity to the analogous *invariant subset problem* and the study of hypercyclic operators. For $T \in \mathscr{L}(X)$, the closure of the T-orbit of $x \in X$ is the smallest closed T-invariant subset that contains x. Thus T does not admit a non-trivial closed invariant subset if and only if every nonzero $x \in X$ is a hypercyclic vector for T. Read [122] identified such an example by constructing an operator $T\colon \ell^1 \to \ell^1$ such that every nonzero $x \in \ell^1$ is a hypercyclic vector for T. By taking the closed linear span of the orbits, it follows that we have a counterexample to the invariant subspace problem. For recent contributions to this topic we refer the curious reader to [92] and [93].

On the other hand, motivation to investigate hypercyclicity also stems from the more general notion of universality. For topological spaces X and Y, the countable family $(T_n)_{n\in\mathbb{N}}$ of continuous maps $T_n\colon X \to Y$ is *universal* if there exists $x \in X$ such that

$$\overline{\{T_n(x) : n \in \mathbb{N}\}} = Y.$$

Such an $x \in X$ is called a *universal element* for (T_n). If we let $X = Y$ be a topological vector space and we take the sequence (T_n) to be the iterates of a single linear operator, then it follows that hypercyclicity is a particular instance of universality.

The discovery of universal power series was credited in 1914 to Fekete [119]. He showed there exists a formal real power series $\sum_{j=1}^{\infty} a_j x^j$ on $[-1, 1]$ with the property that for any continuous function $g\colon [-1, 1] \to \mathbb{R}$ with $g(0) = 0$, there exists an increasing sequence of positive integers (n_k) such that

$$\sum_{j=1}^{n_k} a_j x^j \to g(x)$$

uniformly as $k \to \infty$. The observation of Fekete can be further extended to a universal Taylor series on all of $\mathbb{R}$ (cf. [94, Section 3a]).

Many of the statements for hypercyclicity have analogues for the more general notion of universality. In fact, the hypercyclicity results for the classical translation [46] and differentiation [103] operators acting on the space $H(\mathbb{C})$ were originally proven for universality. However, some of the powerful tools used to investigate hypercyclic operators, for instance the spectral techniques, are not available for universality. To learn more about this intriguing topic we refer the interested reader to the survey by Grosse-Erdmann [94] and the article by Bayart et al. [20].

2.2. **Linear Chaos.** Following the seminal paper of Godefroy and Shapiro [80], the definition proposed by Devaney became the accepted definition of chaos in linear dynamics. Alternative definitions of chaos also appear in the literature and we discuss some of them in Section 4.

We recall that the Birkhoff transitivity theorem gives that an operator is hypercyclic if and only if it is topologically transitive, which leads to the following definition. We say that $T \in \mathscr{L}(X)$ is *chaotic* if the following hold:

(i) T is hypercyclic,

(ii) T possesses a set of periodic points that is dense in X.

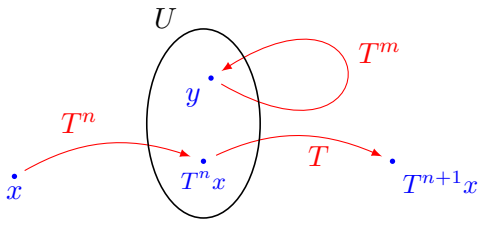


FIGURE 2. Chaos: each nonempty open subset contains a periodic point and a hypercyclic vector.

The behaviour of a periodic point is in stark contrast to that of a hypercyclic vector. However, as illustrated in Figure 2, for an operator T to be chaotic each nonempty open subset $U \subset X$ must contain a hypercyclic vector and a periodic point. We also remark that for a linear dynamical system (X, T), if T is hypercyclic then it follows directly that T has sensitive dependence on initial conditions [80].

The classical hypercyclic operators previously mentioned (non-trivial translations, differentiation operators and scalar multiples of the backward shift) all turn out to be chaotic (cf. [98, Section 2.3]). Further examples of chaotic operators include adjoint multipliers and (weighted) composition operators acting on function spaces such as the Hardy and Bergman spaces [80, 123, 36]. In particular, the chaotic composition operators acting on the Hardy space $H^2(\mathbb{D})$ were characterised by Taniguchi [131], who proved that C_φ is chaotic on $H^2(\mathbb{D})$ if and only if φ is an automorphism of the unit disc $\mathbb{D}$ with no fixed point in $\mathbb{D}$.

The chaotic weighted shifts B_w acting on ℓ^p, $1 \leq p < \infty$, were characterised by Grosse-Erdmann [95], who proved that B_w is chaotic if and only if

$$\sum_{n=1}^{\infty} \frac{1}{|w_1 \cdots w_n|^p} < \infty \tag{2.2}$$

and if and only if B_w admits a nonzero periodic point. The weighted shift B_w is chaotic on c_0 if and only if $\prod_{j=1}^{n} |w_j| \to \infty$, as $n \to \infty$.

A significant difference between hypercyclicity and chaos was identified by Bonet et al. [49], who demonstrated that there exist spaces that admit no chaotic operator.

Theorem 2.2 (Bonet, Martínez-Giménez and Peris [49]). *There exist separable infinite-dimensional Banach spaces that do not support a chaotic operator.*

To prove Theorem 2.2, they demonstrated that the hereditarily indecomposable Banach spaces constructed by Gowers and Maurey [83] do not support chaotic operators. Thus operators of the form $I + K$ were shown to be non-chaotic, where K is strictly singular and I is the identity. We note that their argument also holds for operators of the form $I + K$, where K is compact, acting on the hereditarily indecomposable Banach spaces that were subsequently constructed by Argyros and Haydon [4]. A Banach space X is said to be hereditarily indecomposable if no closed subspace of X is decomposable as a direct sum of infinite-dimensional subspaces.

On the other hand, de la Rosa et al. [63] constructed chaotic operators that are compact (or even nuclear) perturbations of diagonal operators that have complex diagonal coefficients of modulus 1. This gives, for instance, that there exist chaotic operators on any complex Banach space with an unconditional basis.

Theorem 2.3 (de la Rosa, Leonhard, Grivaux and Peris [63]). *Let X be a complex separable Banach space having an unconditional Schauder decomposition. Then X supports an operator which is chaotic.*

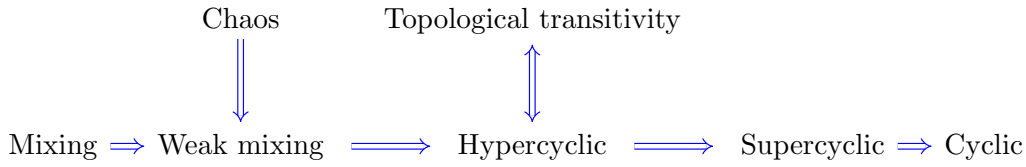


FIGURE 3. Relations between the dynamical properties from Section 2.

Chaotic operators satisfy the Hypercyclicity Criterion and hence chaos implies weak mixing (cf. [21, Proposition 6.11]). A summary of the relations between the dynamical properties introduced thus far can be found in Figure 3.

3. Recurrence in Linear Dynamics

For $T \in \mathscr{L}(X)$ to satisfy the definition of hypercyclicity, we require the existence of a vector $x \in X$ such that for every nonempty, open subset $U \subset X$, the *return set*

$$\mathcal{N}_T(x, U) \coloneqq \{n \geq 0 : T^n x \in U\}$$

is nonempty, as illustrated in Figure 4(a). It turns out if T is hypercyclic then $\mathcal{N}_T(x, U)$ is in fact an infinite set. It is thus natural to ask, are some orbits more recurrent than others?

One approach to resolve this question is to consider quantitative differences in hypercyclic behaviour by calculating an appropriate density of the return sets. The *lower* and *upper densities* of a set $A \subset \mathbb{N}$ are defined, respectively, as

$$\underline{\operatorname{dens}}(A) \coloneqq \liminf_{n\to\infty} \frac{|A \cap \{1, 2, \ldots, n\}|}{n},$$
$$\overline{\operatorname{dens}}(A) \coloneqq \limsup_{n\to\infty} \frac{|A \cap \{1, 2, \ldots, n\}|}{n},$$

where $|\cdot|$ denotes the cardinality of the set. The *upper Banach density* of $A \subset \mathbb{N}$ is defined as

$$\overline{\operatorname{Bd}}(A) \coloneqq \lim_{N\to\infty} \frac{b_N}{N}$$

where

$$b_N \coloneqq \limsup_{k\to\infty} |A \cap [k+1,\, k+N]|\,.$$

These densities are related as follows

$$\underline{\operatorname{dens}}(A) \leq \overline{\operatorname{dens}}(A) \leq \overline{\operatorname{Bd}}(A).$$

Investigation of the lower density of return sets was initiated in 2004 by Bayart and Grivaux [16, 18] when they introduced the notion of frequent hypercyclicity. Since then the study of recurrent orbits has developed into one of the most important branches of linear dynamics.

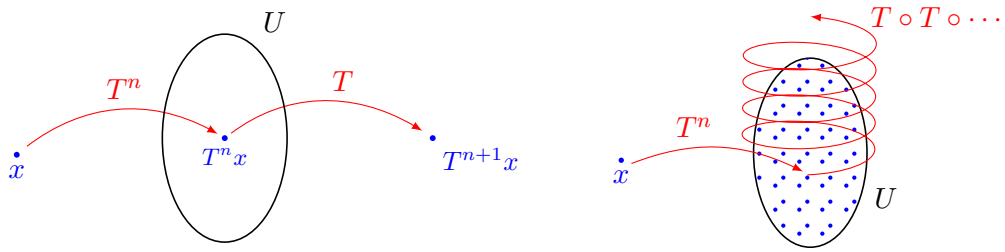
3.1. Frequent Hypercyclicity.

We say $T \in \mathscr{L}(X)$ is *frequently hypercyclic* if there exists $x \in X$ such that for any nonempty open subset $U \subset X$, the return set $\mathcal{N}_T(x, U)$ has positive lower density, that is

$$\underline{\operatorname{dens}}(\mathcal{N}_T(x, U)) > 0.$$

Such an $x \in X$ is a *frequently hypercyclic vector* for T.

Frequent hypercyclicity gives a quantitative description of how frequently an orbit visits each neighbourhood. As illustrated in 4(b), for T to be frequently hypercyclic, each time the T-orbit visits a particular U it must actually visit U quite often before it moves away.



(a) T-orbit of x visits U.

(b) Recurrent T-orbit of x in U.

FIGURE 4

The classical hypercyclic operators mentioned in Section 2 (non-trivial translations, differentiation and scalar multiples of the backward shift) turn out to possess the stronger property of frequent hypercyclicity. Weighted shifts also provide a rich source of examples to illustrate the nature of frequent hypercyclicity.

Frequently hypercyclic weighted shifts were characterised by Bayart and Ruzsa [24] with the following theorem.

Theorem 3.1 (Bayart and Ruzsa [24]). *Let $1 \leq p < \infty$. The weighted shift $B_w \colon \ell^p \to \ell^p$ is frequently hypercyclic if and only if*

$$\sum_{n=1}^{\infty} \frac{1}{|w_1 \cdots w_n|^p} < \infty. \tag{3.1}$$

We remark that a comparison with (2.2) reveals that a weighted shift acting on ℓ^p, for $1 \leq p < \infty$, is frequently hypercyclic if and only if it is chaotic.

Weighted shifts also provide examples of hypercyclic operators that are not frequently hypercyclic. For instance, in [22, Example 6.17] they show that $B_w \colon \ell^2 \to \ell^2$ defined by

$$w_n = \sqrt{\frac{n+1}{n}}$$

satisfies (2.1) but not (3.1), and hence B_w is hypercyclic and non-frequently hypercyclic.

The behaviour of weighted shifts acting on the sequence space c_0 is not so straightforward. Bayart and Grivaux [19] identified weighted shifts B_w acting on c_0 that are frequently hypercyclic but not chaotic nor mixing. However, it was shown by Bonilla and Grosse-Erdmann [52] that every chaotic weighted shift on c_0 is frequently hypercyclic. The following, somewhat technical, characterisation of frequently hypercyclic weighted shifts acting on the space c_0 was given in [24].

Theorem 3.2 (Bayart and Ruzsa [24]). *Let $w = (w_n)_{n \in \mathbb{N}_0}$ be a bounded sequence of positive integers. Then B_w is frequently hypercyclic on c_0 if and only if there exists a sequence $(M(p))$ of positive real numbers tending to $+\infty$ and a sequence (E_p) of subsets of $\mathbb{N}_0$ such that*

(i) for any $p \geq 1$, $\underline{\mathrm{dens}}(E_p) > 0$,

(ii) for any $p, q \geq 1$, $p \neq q$, $(E_p + [0,p]) \cap (E_p + [0,q]) = \varnothing$,

(iii) $\lim\limits_{\substack{n \to +\infty \\ n \in E_p + [0,p]}} w_1 \cdots w_n = +\infty$,

(iv) for any $p, q \geq 1$, for any $n \in E_p$ and any $m \in E_q$ with $m > n$, for any $t \in \{0, \ldots, q\}$,

$$w_1 \cdots w_{m-n+t} \geq M(p) M(q).$$

We note that in [24] versions of Theorems 3.1 and 3.2 are also proven for the sequence spaces $\ell^p(\mathbb{Z})$ and $c_0(\mathbb{Z})$ indexed over the integers.

Recently Charpentier et al. [61] extended Theorem 3.1 to general classes of Fréchet sequence spaces. In particular, they identified Köthe sequence spaces such that frequent hypercyclicity of B_w is equivalent to chaoticity, and examples of Köthe sequence spaces where B_w is frequently hypercyclic but not chaotic.

Examples of frequently hypercyclic operators can also be found among the classes of composition operators acting on function spaces. It turns out that the composition operator C_φ acting on the classical Hardy space $H^2(\mathbb{D})$ is frequently hypercyclic if and only if C_φ is hypercyclic [18, 19]. Furthermore, the ever curious family of rank 1 perturbations of unitary operators constructed by Grivaux [86] are even frequently hypercyclic and chaotic!

Many results for hypercyclicity have analogues in the frequently hypercyclic case. For instance, there exists a sufficient condition known as the Frequent Hypercyclicity Criterion. If an operator T satisfies this criterion then T is frequently hypercyclic, chaotic and mixing (cf. [98, Theorem 9.9, Proposition 9.11]). However, it was shown in [19] that there exist frequently hypercyclic weighted shifts on the space c_0 that do not satisfy the Frequent Hypercyclicity Criterion.

The following theorem contrasts further with the hypercyclic case.

Theorem 3.3 (Shkarin [127])**.** *There exist separable infinite-dimensional Banach spaces that do not support frequently hypercyclic operators.*

Analogous to the chaotic case, it was shown in [127] that operators of the form $I + K$, where K is compact or even strictly singular, cannot be frequently hypercyclic. Thus the hereditarily indecomposable Banach spaces constructed in [83] and [4] do not support frequently hypercyclic operators.

However, it was shown by de la Rosa et al. [63] that the chaotic operator from Theorem 2.3 is also frequently hypercyclic, which gives that any complex Banach space with an unconditional basis supports a frequently hypercyclic operator.

Another significant difference to the hypercyclic case is that the set of frequently hypercyclic vectors is of first category.

Theorem 3.4 (Moothathu [116], Bayart and Ruzsa [24], Grivaux and Matheron [90])**.** *Let T be frequently hypercyclic. Then the set of frequently hypercyclic vectors for T is a meagre set.*

As a consequence of Theorem 3.4, the powerful Baire category theorem is not available in the study of frequent hypercyclicity. Measure-theoretic techniques have emerged as an effective alternative approach and we discuss this topic in Section 3.3.

Recently Grivaux [89] considered frequently hypercyclic vectors with irregular behaviour. A frequently hypercyclic vector $x \in X$ is said to have an *irregularly visiting orbit* if there exists a nonempty open $U_0 \subset X$ such that the lower density of its return set $\mathcal{N}_T(x, U_0)$ is strictly less than its upper density, i.e.

$$\underline{\operatorname{dens}}\left(\mathcal{N}_T(x, U_0)\right) < \overline{\operatorname{dens}}\left(\mathcal{N}_T(x, U_0)\right),$$

or in other words, the return set $\mathcal{N}_T(x, U_0)$ has no density. It turns out that every operator satisfying a strong form of the Frequent Hypercyclicity Criterion possesses a frequently hypercyclic vector with an irregularly visiting orbit [89]. Such examples can be found in the article by Grivaux [87], who investigated a particular family of hypercyclic operators introduced by Glasner and Weiss [79]. However, it remains an open question whether all frequently hypercyclic operators admit a frequently hypercyclic vector with an irregularly visiting orbit [89, Question 3.2].

Finally we mention that two challenging problems in linear dynamics asked whether every chaotic operator is frequently hypercyclic [19, Question 6.4], and whether the inverse of a frequently hypercyclic operator is still frequently hypercyclic [18, Question 4.3], [99, Problem 44]. These questions were recently resolved in the negative by Menet [109, 112] with the introduction of *operators of C-type*. We postpone discussion of operators of C-type and these results until Section 5.

3.2. **Upper Frequent and Reiterative Hypercyclicity.** Two classes of operators that have recently attracted much interest are the upper frequently and reiteratively hypercyclic operators. They provide a fine-grained picture of the quantitative differences in the dynamical behaviours that lie between hypercyclicity and frequent hypercyclicity.

The notion of upper, or $\mathcal{U}$-frequent hypercyclicity was introduced by Shkarin [127]. We say $T \in \mathscr{L}(X)$ is *$\mathcal{U}$-frequently hypercyclic* if there exists $x \in X$ such that for any nonempty open subset $U \subset X$, the return set $\mathcal{N}_T(x, U)$ has positive upper density, i.e.

$$\overline{\operatorname{dens}}(\mathcal{N}_T(x, U)) > 0.$$

Such an $x \in X$ is called a *$\mathcal{U}$-frequently hypercyclic vector* for T.

$\mathcal{U}$-frequent hypercyclicity is by definition weaker than frequent hypercyclicity, as illustrated by the example from [24] of a weighted shift on the space c_0 that is $\mathcal{U}$-frequently hypercyclic but not frequently hypercyclic.

In further contrast to the frequently hypercyclic case, it was shown in [24] that the set of $\mathcal{U}$-frequently hypercyclic vectors for T is comeagre.

Theorem 3.5 (Bayart and Ruzsa [24])**.** *Let T be $\mathcal{U}$-frequently hypercyclic. Then the set of $\mathcal{U}$-frequently hypercyclic vectors for T is comeagre.*

However, analogous to the frequently hypercyclic case, the hereditarily indecomposable Banach spaces constructed in [83] and [4] do not support $\mathcal{U}$-frequently hypercyclic operators [127]. Thus it follows that the set of $\mathcal{U}$-frequently hypercyclic vectors is either empty or comeagre. An open question arising from this fact, and stated in [54], is whether the set of $\mathcal{U}$-frequently hypercyclic vectors (when it exists) is a G_δ-set.

A general criterion that can be used to demonstrate $\mathcal{U}$-frequent hypercyclicity was introduced in [41], and Bonilla and Grosse-Erdmann [54] subsequently introduced a simplification with the following $\mathcal{U}$-Frequent Hypercyclicity Criterion.

Theorem 3.6 (Bonilla and Grosse-Erdmann [54])**.** *Let $T \in \mathscr{L}(X)$. Suppose that there exist dense subsets $X_0, Y_0 \subset X$ and mappings $S_n \colon Y_0 \to X$, $n \geq 0$. If for any $y \in Y_0$ and $\varepsilon > 0$ there exists $A \subset \mathbb{N}$ with $\overline{\operatorname{dens}}(A) > 0$ and $\delta > 0$ such that the following hold,*

(i) for any $x \in X_0$ there is some $B \subset A$ with $\overline{\operatorname{dens}}(B) > \delta$ such that for any $n \in B$

$$\|T^n x\| < \varepsilon,$$

(ii) $\displaystyle\sum_{n \in A} S_n y$ converges,

(iii) for any $m \in A$

$$\left\| T^m \sum_{n \in A} S_n y - y \right\| < \varepsilon,$$

then T is $\mathcal{U}$-frequently hypercyclic.

It was shown in [24] that weighted shifts B_w acting on the spaces ℓ^p, $1 \leq p < \infty$, are $\mathcal{U}$-frequently hypercyclic if and only if they are frequently hypercyclic, i.e. they satisfy (3.1). They also show in [24] that replacing the lower density in Theorem 3.2 (i) by the condition $\overline{\operatorname{dens}}(E_p) > 0$ gives a characterisation of the $\mathcal{U}$-frequently hypercyclic weighted shifts on c_0.

The following interesting property of invertible frequently hypercyclic operators was identified in [24].

Theorem 3.7 (Bayart and Ruzsa [24]). *If T is invertible and frequently hypercyclic then its inverse T^{-1} is $\mathcal{U}$-frequently hypercyclic.*

The notion of reiterative hypercyclicity was introduced by Bès et al. [41] when they considered the upper Banach density of return sets. We say $T \in \mathscr{L}(X)$ is *reiteratively hypercyclic* if there exists $x \in X$ such that for every nonempty open $U \subset X$, the return set $\mathcal{N}_T(x, U)$ has positive upper Banach density, i.e.

$$\overline{\mathrm{Bd}}\,(\mathcal{N}_T(x, U)) > 0.$$

It was proven in [41] that there exists a reiteratively hypercyclic weighted shift on c_0 that is not $\mathcal{U}$-frequently hypercyclic. They also prove that there exists a mixing (and hence hypercyclic) weighted shift on ℓ^p that is not reiteratively hypercyclic [41]. On the other hand, it has been shown that chaos implies reiterative hypercyclicity [109] and reiterative hypercyclicity implies weak mixing [41].

Theorem 3.8 (Bès, Menet, Peris and Puig [41]). *Let X be a separable and infinite-dimensional Banach space. If $T \in \mathscr{L}(X)$ is reiteratively hypercyclic then T is weakly mixing.*

Theorem 3.9 (Menet [109]). *Let X be a separable infinite-dimensional Banach space. If $T \in \mathscr{L}(X)$ is chaotic then T is reiteratively hypercyclic.*

If T is reiteratively hypercyclic then it turns out that its set of reiteratively hypercyclic vectors coincides with the set of T-hypercyclic vectors [41]. Some further nice properties of reiterative hypercyclicity are contained in the following theorems, including a positive answer to the $\mathcal{U}$-frequently and reiteratively hypercyclic analogues of Herrero's problem.

Theorem 3.10 (Bonilla and Grosse-Erdmann [54]). *Let $T \in \mathscr{L}(X)$ be invertible. If T is reiteratively hypercyclic then so is its inverse.*

Theorem 3.11 (Ernst, Esser and Menet [68]). *If $T \in \mathscr{L}(X)$ is $\mathcal{U}$-frequently hypercyclic (resp. reiteratively hypercyclic), then $T \oplus T$ is $\mathcal{U}$-frequently hypercyclic (resp. reiteratively hypercyclic).*

It was shown in [24] that the weighted shift B_w acting on ℓ^p is $\mathcal{U}$-frequently hypercyclic if and only if it is frequently hypercyclic. This result was subsequently extended in [41], where it was shown that every reiteratively hypercyclic weighted shift on $\ell^p(\mathbb{N})$ and $\ell^p(\mathbb{Z})$ is frequently hypercyclic. It was observed in [54] that replacing upper density by upper Banach density in Theorem 3.6 gives a Reiterative Hypercyclicity Criterion.

We remark that the studies in [54] and [68] employed the general framework of $\mathcal{A}$-hypercyclicity which was introduced in [41], where $\mathcal{A}$ is a Furstenberg family. A nonempty family $\mathcal{A}$ of subsets of $\mathbb{N}_0$ is a *Furstenberg family* if it is hereditary upward, that is if $A \in \mathcal{A}$ and $A \subset B$, then $B \in \mathcal{A}$. We say $T \in \mathscr{L}(X)$ is *$\mathcal{A}$-hypercyclic* if there exists $x \in X$ such that for any nonempty open $U \subset X$ it holds that

$$\mathcal{N}_T(x, U) \in \mathcal{A}.$$

For instance, if $\mathcal{A}$ is the family of nonempty subsets of $\mathbb{N}_0$, then $\mathcal{A}$-hypercyclicity corresponds to hypercyclicity, and if $\mathcal{A}$ is the family of sets with positive lower density then $\mathcal{A}$-hypercyclicity corresponds to frequent hypercyclicity.

With the general machinery of $\mathcal{A}$-hypercyclicity, the results in [41], [54] and [68] for $\mathcal{U}$-frequent and reiterative hypercyclicity follow as special cases. This approach was also employed by Grosse-Erdmann [97] to prove the following theorem.

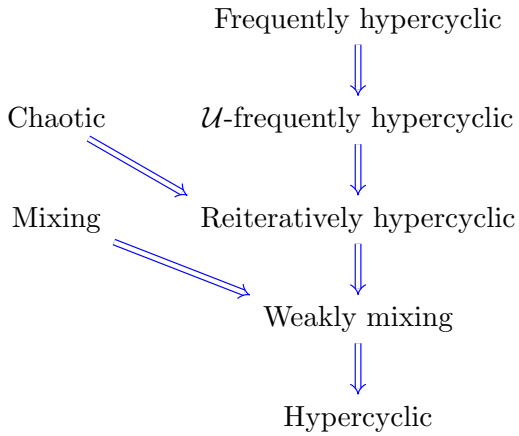


FIGURE 5. Relations between various linear dynamical properties.

Theorem 3.12 (Grosse-Erdmann [97]). *Let B_w be an invertible weighted shift on $c_0(\mathbb{Z})$. If B_w is $\mathcal{U}$-frequently hypercyclic, then so is its inverse B_w^{-1}.*

We also note that a study using the framework of Furstenberg families with respect to topological transitivity was conducted by Bès et al. [42].

Finally we mention that weighted upper and lower densities were studied in Ernst and Mouze [69] and Menet [113] to identify a fine-grained picture of the dynamical notions that lie between $\mathcal{U}$-frequent and frequent hypercyclicity. In [68] weighted densities were also studied to illustrate the dynamical behaviours lying between reiterative hypercyclicity and $\mathcal{U}$-frequent hypercyclicity.

3.3. **Ergodic Theory and Frequent Hypercyclicity.** In the absence of Baire category techniques, probabilistic methods inspired by ergodic theory have proven a fruitful strategy in the study of frequent hypercyclicity. This approach is originally due to Flytzanis [73], and [22, Chapter 5] contains a comprehensive introduction to this topic.

Unless otherwise stated, in this subsection X denotes a separable complex Banach space with Borel σ-algebra $\mathcal{B}$. We let μ be a finite Borel measure and we let $\mathbb{T} = \{\lambda \in \mathbb{C} : |\lambda| = 1\}$ denote the unit circle. The measure μ is said to have *full support* if $\mu(A) > 0$ for every nonempty open $A \in \mathcal{B}$.

For a probability space $(X, \mathcal{B}, \mu)$, the measurable map $T\colon (X, \mathcal{B}, \mu) \to (X, \mathcal{B}, \mu)$ is said to be *ergodic* if μ is T-invariant, and if $A \in \mathcal{B}$ satisfies $T^{-1}(A) = A$ up to a set of measure zero then $\mu(A) = 0$ or 1. We recall that the measure μ is said to be T-invariant if $\mu\left(T^{-1}(A)\right) = \mu(A)$ for all $A \in \mathcal{B}$.

The cornerstone of probabilistic methods in linear dynamics is the following observation. For $T \in \mathscr{L}(X)$, if there exists a T-invariant Borel probability measure μ on X, with full support, such that T is an ergodic transformation with respect to μ, then T is frequently hypercyclic (cf. [22, Proposition 6.23]). This can be seen as a consequence of Birkhoff's ergodic theorem, which states if $T\colon (X, \mathcal{B}, \mu) \to (X, \mathcal{B}, \mu)$ is ergodic with respect to μ, then for any μ-integrable function f on X

$$\frac{1}{N}\sum_{n=0}^{N-1} f(T^n x) \xrightarrow{N\to\infty} \int_X f\, d\mu \tag{3.2}$$

for μ-almost every $x \in X$ (this is interpreted as meaning that the time average of f with respect to T coincides with its space average). The separability of X gives a countable base (V_j) of open sets of X, so when we apply (3.2) to the indicator function $\mathbb{1}_{V_j}$, $j \geq 1$

and using the fact that μ has full support, we get

$$\frac{1}{N}\sum_{n=0}^{N-1} \mathbb{1}_{V_j}(T^n x) = \frac{|\{n < N \,:\, T^n x \in V_j\}|}{N} \longrightarrow \int_X \mathbb{1}_{V_j}\, d\mu = \mu(V_j) > 0.$$

Thus there exist subsets $A_j \subset X$, $j \geq 1$, of full measure, such that for any $x \in A_j$

$$\lim_{N\to\infty} \frac{|\{n < N \,:\, T^n x \in V_j\}|}{N} \longrightarrow \mu(V_j) > 0.$$

Since every nonempty open set contains some V_j and since $\bigcap_{j\geq 1} A_j$ has full measure, it follows for μ-almost every $x \in X$ and every nonempty open $U \subset X$ that

$$\liminf_{N\to\infty} \frac{|\{n < N \,:\, T^n x \in U\}|}{N} > 0,$$

and thus T is frequently hypercyclic.

A practical application of this observation utilises the following fact: if T possesses an abundant supply of unimodular eigenvalues, then T admits an invariant Gaussian measure with respect to which it is ergodic. An eigenvector for $T \in \mathscr{L}(X)$ is said to be *unimodular* if the associated eigenvalue has modulus 1. We say that $T \in \mathscr{L}(X)$ has a *perfectly spanning set of unimodular eigenvectors* if, for every countable $D \subset \mathbb{T}$, we have

$$\overline{\text{span}}\{\ker(T - \lambda I) \,:\, \lambda \in \mathbb{T} \setminus D\} = X.$$

Bayart and Grivaux [17] proved for a separable Banach space X, that if $T \in \mathscr{L}(X)$ has a perfectly spanning set of unimodular eigenvalues then T is hypercyclic. They subsequently proved in [18] that under these conditions in the Hilbert space setting T is frequently hypercyclic. This result was then proven in the Banach space setting by Grivaux [85].

Theorem 3.13 (Grivaux [85])**.** *For a complex Banach space X, if $T \in \mathscr{L}(X)$ has a perfectly spanning set of eigenvectors associated to unimodular eigenvalues, then T is frequently hypercyclic.*

Research on this topic initially focused on Gaussian measures, since they are a natural choice in the infinite-dimensional setting. Conditions under which $T \in \mathscr{L}(X)$ admits a Gaussian ergodic measure with full support were studied in Bayart and Grivaux [19] and Bayart and Matheron [23]. However, more recently non-Gaussian measures have been studied by Grivaux [85], Murillo-Arcila and Peris [117, 118], and Grivaux and Matheron [90]. We also remark that Theorem 3.13 was proven in [85] for a non-Gaussian measure.

Some of the main results from [90] are the following. A measure μ on X is said to be *continuous* if $\mu(\{x\}) = 0$ for every $x \in X$.

Theorem 3.14 (Grivaux and Matheron [90])**.** *Let X be a reflexive Banach space. Any frequently hypercyclic operator $T \in \mathscr{L}(X)$ admits a continuous invariant probability measure with full support.*

Theorem 3.15 (Grivaux and Matheron [90])**.** *If X is a reflexive Banach space and if $V \subset X$ is a nonempty open set, then any frequently hypercyclic operator $T \in \mathscr{L}(X)$ admits a continuous ergodic probability measure μ such that $\mu(V) > 0$.*

The next theorem concerns the sequence space $c_0(\mathbb{Z})$ indexed over the integers.

Theorem 3.16 (Grivaux and Matheron [90])**.** *There exists a frequently hypercyclic operator on the space $c_0(\mathbb{Z})$ that does not admit an ergodic measure with full support.*

A key technique employed in [90] was the introduction of the parameter $c(T) \in [0, 1]$ associated with any hypercyclic $T \in \mathscr{L}(X)$. It is defined for $r > 0$ as

$$c(T) = \sup_{x \in HC(T)} \overline{\text{dens}}\left(\mathcal{N}_T(x, B(0, r))\right), \tag{3.3}$$

where $HC(T)$ is the set of hypercyclic vectors for T and $B(0, r)$ is the ball centred at the origin of radius $r > 0$. It describes the maximal frequency with which the orbit of a hypercyclic vector x visits a ball centred at the origin. Its usefulness can be seen in the following theorem.

Theorem 3.17 (Grivaux and Matheron [90]). *Let $T \in \mathscr{L}(X)$. If T admits an ergodic measure with full support then $c(T) = 1$.*

In [90] they show that $\overline{\text{dens}}\left(\mathcal{N}_T(x, B(0, r))\right) = c(T)$ for a comeagre set of hypercyclic vectors and so it follows that

$$c(T) = \sup\left\{c \geq 0 : \overline{\text{dens}}\left(\mathcal{N}_T(x, B(0, r))\right) \geq c \text{ for a comeagre set of } x \in HC(T)\right\}.$$

Menet [109] recently proved with the following theorem that there exists a chaotic operator that admits only countably many unimodular eigenvalues. Hence the unimodular eigenvectors cannot be perfectly spanning. This answered a long-standing question by Flytzanis [73] that asked whether every hypercyclic operator with unimodular eigenvectors that span a dense subspace necessarily possesses uncountably many unimodular eigenvectors.

Theorem 3.18 (Menet [109]). *Let X be the complex Banach space c_0 or ℓ^p, for $1 \leq p < \infty$. There exists a chaotic operator $T \in \mathscr{L}(X)$ that possesses only countably many unimodular eigenvalues.*

The operator from Theorem 3.18 was an operator of C-type and further discussion of this family of operators appears in Section 5.

Another motivation for looking beyond Gaussian measures is that it was recently shown by Grivaux et al. [91, Section 2.5] that a *typical* hypercyclic operator T acting on a Hilbert space H does not possess eigenvalues. We will not elaborate here on what is meant in [91] by typical, but we remark that an immediate consequence is that a *typical* hypercyclic operator is not chaotic.

4. Li-Yorke and Distributional Chaos

The term *chaos* first appeared in mathematical literature in an article by Li and Yorke [102], where they studied the dynamical behaviour of interval maps with period three. Schweizer and Smítal [126] subsequently introduced the stronger notion of *distributional chaos* for self-maps of a compact interval. The study of distributional chaos in the linear dynamical setting was initiated by Martínez-Giménez et al. [104].

The operator $T \in \mathscr{L}(X)$ is said to be *Li-Yorke chaotic* if there exists an uncountable set $\Gamma \subset X$ such that for each distinct pair $(x, y) \in \Gamma \times \Gamma$ we have

$$\liminf_{n\to\infty} \| T^n x - T^n y \| = 0 \qquad \text{and} \qquad \limsup_{n\to\infty} \| T^n x - T^n y \| > 0.$$

This definition captures local aspects of the dynamical behaviour of pairs of vectors by describing orbits that are proximal without being asymptotic.

The connection between Li-Yorke chaos and the property of irregularity was identified by Bermúdez et al. [26]. We say that $x \in X$ is an *irregular vector* for T if there exist increasing sequences (j_k) and (n_k) of positive integers such that

$$\lim_{k\to\infty} T^{j_k} x = 0 \quad \text{and} \quad \lim_{k\to\infty} \|T^{n_k} x\| = \infty.$$

This notion was introduced by Beauzamy [25] for Banach spaces and it was generalised to the Fréchet space setting by Bernardes et al. [34].

It was shown in [26] that T is Li-Yorke chaotic if and only if T admits an irregular vector. It is also well known that hypercyclic vectors are irregular. On the other hand, families of operators that do not admit an irregular vector include compact and normal operators.

Li-Yorke chaotic weighted shifts were characterised in [26] with the following theorem.

Theorem 4.1 (Bermúdez, Bonilla, Martínez-Giménez and Peris [26]). *Let $X = c_0$ or ℓ^p, $1 \leq p < \infty$. The weighted shift $B_w \colon X \to X$ is Li-Yorke chaotic if and only if*

$$\sup_{\substack{n\in\mathbb{N}\\ m>n}} \prod_{j=n}^{m} |w_j| = \infty.$$

Comparing Theorem 4.1 to (2.1), we see that it is possible to define a weight sequence such that B_w is Li-Yorke chaotic but not hypercyclic.

The Li-Yorke chaotic composition operators and adjoint multipliers were characterised in [34]. In particular, they show for an automorphism φ of a domain $\Omega \subset \mathbb{C}$, that the composition operator C_φ acting on the space $H(\Omega)$ of holomorphic functions on Ω is Li-Yorke chaotic if and only if it is hypercyclic.

A strengthening of Li-Yorke chaos was introduced in [126] with the notion of distributional chaos. Before we give the definition of distributional chaos we introduce the following functions. Given $\delta > 0$, we define the *lower* and *upper distributional functions* of $x, y \in X$ associated to $T \in \mathscr{L}(X)$ as, respectively,

$$F_{x,y}(\delta) \coloneqq \underline{\operatorname{dens}}\left(\left\{j \in \mathbb{N} \,:\, \left\|T^j x - T^j y\right\| < \delta\right\}\right) \tag{4.1}$$

and

$$F^*_{x,y}(\delta) \coloneqq \overline{\operatorname{dens}}\left(\left\{j \in \mathbb{N} \,:\, \left\|T^j x - T^j y\right\| < \delta\right\}\right). \tag{4.2}$$

Note that $F_{x,y}$ and $F^*_{x,y}$ are nondecreasing maps on $(0, \infty)$ with $0 \leq F_{x,y} \leq F^*_{x,y} \leq 1$.

If the pair (x, y) satisfy $F^*_{x,y} \equiv 1$ and $F_{x,y}(\varepsilon) = 0$ for some $\varepsilon > 0$, then (x, y) is called a *distributionally chaotic pair*. The operator T is said to be *distributionally chaotic* if there exists an uncountable set $\Gamma \subset Y$ such that every distinct pair $(x, y) \in \Gamma \times \Gamma$ is a distributionally chaotic pair for T. The set Γ is known as a *distributionally scrambled set* for T. We say that T is *densely distributionally chaotic* if the set Γ may be chosen to be dense in X.

It follows from results in [26] and Bernardes et al. [33] that in the linear setting distributional chaos is equivalent to the more tractable notion of distributional irregularity. We say $x \in X$ is a *distributionally irregular vector* for T if there exists $A, B \subset \mathbb{N}$ with

$$\overline{\operatorname{dens}}(A) = 1 = \overline{\operatorname{dens}}(B)$$

such that

$$\lim_{\substack{n\to\infty\\ n\in A}} T^n x = 0 \quad \text{and} \quad \lim_{\substack{n\to\infty\\ n\in B}} \|T^n x\| = \infty.$$

This strengthening of irregularity, introduced in [26], describes a more complicated statistical dependence between orbits.

Examples of distributionally chaotic operators include the differentiation operator D acting on the space $H(\mathbb{C})$ of entire functions (this follows from [33, Corollary 17]), and weighted shifts acting on the sequence spaces ℓ^p [104].

We have that every infinite-dimensional separable Banach space supports a distributionally chaotic operator.

Theorem 4.2 (Bermúdez, Bonilla, Martínez-Giménez and Peris [26]). *Every infinite-dimensional separable Banach space supports a distributionally chaotic operator.*

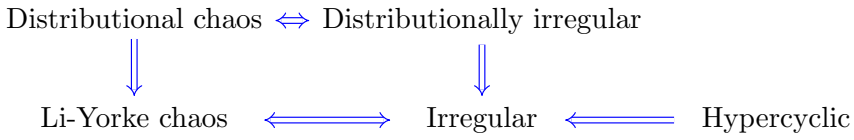


FIGURE 6. Relations between dynamical properties introduced in Section 4.

On the other hand, in [104, Example 13] they gave an example of a backward shift acting on a weighted ℓ^p space that is distributionally chaotic but not hypercyclic. Backward shifts acting on weighted ℓ^p spaces are also a source of examples of operators that are mixing but not distributionally chaotic [105, Theorem 2.1]. In [104] they also give an example of a hypercyclic and distributionally chaotic operator that is not chaotic in the sense of Devaney.

In [24] they identify, as stated in the theorem below, the existence of frequently hypercyclic operators that are not distributionally chaotic.

Theorem 4.3 (Bayart and Ruzsa [24]). *There exists a frequently hypercyclic weighted shift acting on $c_0(\mathbb{Z})$ that is not distributionally chaotic.*

However, for unilateral weighted shifts (i.e. indexed over $\mathbb{N}$), the properties of frequent hypercyclicity and distributional chaos are equivalent.

Theorem 4.4 (Bayart and Ruzsa [24]). *A frequently hypercyclic weighted shift acting on c_0 or ℓ^p, $1 \leq p < \infty$ is distributionally chaotic.*

For a Banach space X, if the set $\{x \in X : T^n x \to 0\}$ is dense in X, then it follows that Devaney chaos implies distributional chaos, and $\mathcal{U}$-frequent hypercyclicity implies distributional chaos [35].

It was also shown in [35] if there exists a set $S \subset \mathbb{N}$ with $\overline{\text{dens}}(S) > 0$ such that

$$\sum_{n \in S} \frac{1}{|w_1 \cdots w_n|^p} < \infty$$

then the weighted shift B_w acting on ℓ^p, $1 \leq p < \infty$, is densely distributionally chaotic.

We note Bernardes et al. [35] conducted an in-depth study of the differing strengths of distributional chaos. To do this they modified the definition by varying the values of the distributional functions (4.1) and (4.2). Other interesting directions of research include the notion of mean Li-Yorke chaos that has been investigated by Bernardes et al. [32].

The following theorems highlight that the probabilistic techniques described in Section 3.3 may also shed some light on the nature of distributional chaos.

Theorem 4.5 (Bayart and Ruzsa [24]). *Let $T \in \mathscr{L}(X)$ be such that the $\mathbb{T}$-eigenvectors are perfectly spanning with respect to Lebesgue measure. Then T is distributionally chaotic.*

It was also shown in [91, Section 2.7] that typical hypercyclic operator is densely distributionally chaotic.

Theorem 4.6 (Grivaux and Matheron [90]). *Let (X, T) be a linear dynamical system, and assume that T admits an ergodic measure with full support. Then T admits a comeagre set of distributionally irregular vectors. This holds in particular if X is a complex Banach space and T has a perfectly spanning set of unimodular eigenvectors.*

5. Operators of C-Type

Operators of C-type have emerged as a rich source of chaotic operators that can be fine-tuned to possess very specific properties. They were introduced by Menet [109] and they provide many important (counter) examples in linear dynamics. An in-depth study of operators of C-type was conducted by Grivaux et al. [91, Section 6] and they have been further developed by Menet [112, 114]. In this section, unless otherwise specified, *chaos* means chaos in the sense of Devaney.

The class of operators of C-type originated in response to the question, first posed in [19], that asked whether chaotic operators are frequently hypercyclic. We recall in the setting of the sequence spaces ℓ^p, $1 \leq p < \infty$, that the weighted shift B_w is chaotic if and only if it is frequently hypercyclic [95], [24]. On the other hand, the sequence space c_0 had hitherto been a fruitful source of counterexamples, indeed it was shown in [19] that there exists a frequently hypercyclic weighted shift on c_0 that is not chaotic. However, in [52] it was proven if B_w is chaotic on c_0 then it follows that it is frequently hypercyclic. There were thus insurmountable obstacles to solving the problem by utilising established approaches.

The question was finally resolved in [109] with the construction of chaotic operators of C-type that are not frequently hypercyclic. An analogous question on whether chaotic operators are distributionally chaotic, posed in [33], was also settled in [109].

Theorem 5.1 (Menet [109])**.** *Let X be the real or complex Banach space c_0 or ℓ^p, for $1 \leq p < \infty$. There exists a chaotic operator $T \in \mathscr{L}(X)$ that is not distributionally chaotic nor $\mathcal{U}$-frequently hypercyclic, and hence not frequently hypercyclic.*

Before we give the definition of operators of C-type, we introduce some notation. Let $\mathbb{N}_0$ denote the set of non-negative integers and we let $\ell^p(\mathbb{N}_0)$ be the space of p-summable sequences indexed over $\mathbb{N}_0$, for $1 \leq p < \infty$. The canonical basis of $\ell^p(\mathbb{N}_0)$ is denoted by $(e_k)_{k\geq 0}$. The parameters ρ, w, φ, b are defined as follows,

- $\rho = (\rho_n)_{n\geq 1}$ is a sequence of nonzero complex numbers with $\sum_{n\geq 1} |\rho_n| < \infty$,
- $w = (w_j)_{j\geq 1}$ is a sequence of complex numbers which is both bounded and bounded below, that is
$$0 < \inf_{k\geq 1} |w_k| \leq \sup_{k\geq 1} |w_k| < \infty,$$
- the map $\varphi\colon \mathbb{N}_0 \to \mathbb{N}_0$ is defined such that $\varphi(0) = 0$, $\varphi(n) < n$ for every $n \geq 1$, and the preimage $\varphi^{-1}(l) = \{n \geq 0 : \varphi(n) = l\}$ is an infinite set for every $l \geq 0$,
- $b = (b_n)_{n\geq 0}$ is a strictly increasing sequence of positive integers such that $b_0 = 0$ and $b_{n+1} - b_n$ is a multiple of $2\left(b_{\varphi(n)+1} - b_{\varphi(n)}\right)$ for every $n \geq 1$.

An *operator of C-type* $T_{\rho,w,\varphi,b}\colon \ell^p(\mathbb{N}_0) \to \ell^p(\mathbb{N}_0)$ is defined as

$$T_{\rho,w,\varphi,b}\, e_k = \begin{cases} w_{k+1} e_{k+1}, & \text{if } k \in [b_n,\, b_{n+1} - 1),\ n \geq 0, \\ \rho_n e_{b_{\varphi(n)}} - \left(\prod_{j=b_n+1}^{b_{n+1}-1} w_j\right)^{-1} e_{b_n}, & \text{if } k = b_{n+1} - 1,\ n \geq 1, \\ -\left(\prod_{j=b_0+1}^{b_1-1} w_j\right)^{-1} e_0, & \text{if } k = b_1 - 1. \end{cases}$$

A crucial property of operators of C-type is that every basis vector e_k is periodic for $T_{\rho,w,\varphi,b}$. It is shown in [91, Fact 6.4] that

$$T_{\rho,w,\varphi,b}^{2(b_{n+1}-b_n)} e_k = e_k, \quad \text{if } k \in [b_n,\, b_{n+1}),\ n \geq 0.$$

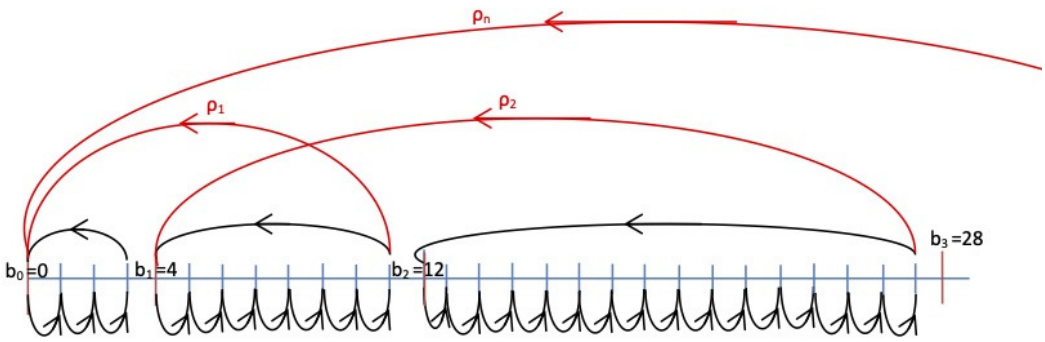


FIGURE 7. Periodicity of each vector e_k. (Figure courtesy of Q. Menet)

Consequently every finitely supported sequence is periodic for $T_{\rho,w,\varphi,b}$ and thus $T_{\rho,w,\varphi,b}$ possesses a dense set of periodic points. The periodicity of each e_k is illustrated in Figure 7 for a particular sequence (b_n).

It was also shown in [91, Proposition 6.5] that $T_{\rho,w,\varphi,b}$ is chaotic if

$$\limsup_{\substack{N\to\infty \\ N\in\varphi^{-1}(n)}} |\rho_N| \prod_{j=b_N+1}^{b_{N+1}-1} |w_j| = \infty, \quad \text{for every } n \geq 0.$$

The term *operator of C-type* was coined in [91], where the choice of the letter 'C' was motivated by their innate connection to *cyclic* and *chaotic* operators.

An inherent characteristic of operators of C-type is an abundant supply of periodic points. We recall that it is well known for a complex Banach space X, that the set of periodic points of $T \in \mathscr{L}(X)$ is given by

$$\operatorname{span}\{x \in X \,:\, Tx = \lambda x, \text{ for some root of unity } \lambda \in \mathbb{C}\}\,.$$

This is an interesting contrast with the results quoted at the end of Section 3.3, which state that a typical hypercyclic operator does not possess any eigenvalues and is not chaotic [91, Section 2.5]. So it is reasonable to ask whether it is possible to find *natural* classes of $\mathcal{U}$-frequently hypercyclic operators in the Hilbert and Banach space settings that are not frequently hypercyclic.

Another long-standing open problem in linear dynamics, stated in [18] and [99, Problem 44], asked whether the inverse of an invertible frequently hypercyclic operator is also frequently hypercyclic. The answer in the hypercyclic case was already well known, since the inverse of a topologically transitive operator is also topologically transitive (cf. [98, Proposition 2.23]).

As a stepping stone to resolving this question, Menet [114] proved the following theorem by constructing a suitable operator of C-type. We note that the operators of C-type considered in [91] are not invertible, so a new tweak of the parameters of $T_{\rho,w,\varphi,b}$ was required.

Theorem 5.2 (Menet [114]). *There exist invertible $\mathcal{U}$-frequently hypercyclic operators on $\ell^p(\mathbb{N}_0)$, for $1 \leq p < \infty$, such that the inverse is not $\mathcal{U}$-frequently hypercyclic.*

On the other hand, if T is invertible and frequently hypercyclic, it was shown in [24] that its inverse T^{-1} is $\mathcal{U}$-frequently hypercyclic. So a counterexample necessarily requires that T^{-1} is $\mathcal{U}$-frequently hypercyclic but non-frequently hypercyclic. Such

operators were identified in [24] and [91], however they are not invertible. The suitable counterexample was constructed by Menet [112].

Theorem 5.3 (Menet [112])**.** *There exists an operator on $\ell^1(\mathbb{N})$ that is invertible and frequently hypercyclic, but with an inverse that is not frequently hypercyclic.*

Another outstanding open question in linear dynamics, originally posed in [18, Question 4.9], asks whether the direct sum $T \oplus T$ of a frequently hypercyclic operator T is itself frequently hypercyclic. We recall that there exist hypercyclic operators T such that $T \oplus T$ is not hypercyclic [64], [21]. On the other hand, we recall that it was shown in [68] that if T is $\mathcal{U}$-frequently hypercyclic (resp. reiteratively hypercyclic), then $T \oplus T$ is $\mathcal{U}$-frequently hypercyclic (resp. reiteratively hypercyclic).

If T is a frequently hypercyclic operator acting on a Banach space X, then it is known T is weakly mixing (cf. [98, Theorem 9.8]), and thus $T \oplus T$ is hypercyclic on $X \oplus X$. This problem is discussed in [91, Section 6.6], where they identify a class of operators of C-type that give the following related result.

Theorem 5.4 (Grivaux, Matheron and Menet [91])**.** *Let $p > 1$. There exists a sequence $(T_n)_{n\geq 1}$ of frequently hypercyclic operators on $\ell^p(\mathbb{N}_0)$ such that the ℓ^p-sum operator*

$$\bigoplus_{n\geq 1} T_n \colon \bigoplus_{n\geq 1} \ell^p(\mathbb{N}_0) \to \bigoplus_{n\geq 1} \ell^p(\mathbb{N}_0)$$

is not $\mathcal{U}$-frequently hypercyclic.

5.1. **Relations Between Dynamical Properties.** We briefly revisit Figure 5 to augment it with some of the new examples that emerged following the systematic investigation of operators of C-type conducted in the monster study [91].

Most of the implications in Figure 5 follow by definition, apart from the following: chaos implies reiterative hypercyclicity [109], and reiterative hypercyclicity implies weak mixing [41]. Furthermore, the implications in Figure 5 are strict and in general no further relations hold since there exist examples of operators that are:

- chaotic but not $\mathcal{U}$-frequently hypercyclic: operators of C-type on ℓ^p [109] and [91, Theorem 6.18],
- chaotic and mixing but not $\mathcal{U}$-frequently hypercyclic: [91, Example 6.35],
- chaotic and frequently hypercyclic but not mixing: shift acting on a Hilbert space [7],
- chaotic and frequently hypercyclic but not mixing, nor ergodic with respect to a probability measure with full support: [91, Example 6.23],
- frequently hypercyclic but not chaotic nor mixing: weighted shift on c_0 [19],
- $\mathcal{U}$-frequently hypercyclic but not frequently hypercyclic: weighted shift on c_0 [24] and [91, Example 6.30],
- mixing but not reiteratively hypercyclic: weighted shift on ℓ^p [41],
- reiteratively hypercyclic but not $\mathcal{U}$-frequently hypercyclic: weighted shift on c_0 [41],
- weakly mixing but not mixing: weighted shift on ℓ^p [62],
- hypercyclic but non-weakly mixing: shift acting on a specific Banach space [64], shift acting on ℓ^p [21].

We remark that the results from [91, Section 6] provide in many instances the first such examples in the Hilbert space setting.

6. Hypercyclic Vectors

A recurring question asked of the author is, 'what does a hypercyclic vector look like?' Our primary focus thus far has been on properties of operators, however the vectors that enable complex linear dynamical behaviour also give rise to deep and interesting questions. In this section we highlight some properties of hypercyclic vectors and we explore the rich algebraic structures contained in the set of hypercyclic vectors.

We start with the important question of the permissible growth rates of entire functions $f \in H(\mathbb{C})$ that are hypercyclic with respect to the differentiation operator $D\colon f \mapsto f'$. If $\varphi\colon \mathbb{R}_+ \to \mathbb{R}_+$ is a function with $\varphi(r) \to \infty$ as $r \to \infty$, then there exists a D-hypercyclic entire function $f \in H(\mathbb{C})$ such that

$$|f(z)| \leq \varphi(r)\frac{e^r}{\sqrt{r}}, \quad \text{for } |z| = r \text{ sufficiently large.}$$

This growth is optimal, since for the critical rate of $e^r/\sqrt{r}$, there does not exist a D-hypercyclic entire function $f \in H(\mathbb{C})$ such that

$$|f(z)| \leq c\frac{e^r}{\sqrt{r}}, \quad \text{for } |z| = r > 0,$$

where $c > 0$ is a constant (cf. [98, Theorem 4.22]).

As we might expect, the frequently hypercyclic entire functions must grow faster than in the hypercyclic case. The question of optimal growth in the frequently hypercyclic case was settled by Drasin and Saksman [66] with the careful construction of an entire function with the following growth.

Theorem 6.1 (Drasin and Saksman [66])**.** *For any constant $C > 0$, there exists a D-frequently hypercyclic entire function $f \in H(\mathbb{C})$ such that*

$$\sup_{|z|=r} |f(z)| \leq C\frac{e^r}{r^{1/4}}, \qquad \text{for all } r > 0.$$

This estimate is optimal, every such function satisfies

$$\limsup_{r\to\infty} r^{1/4}e^{-r} \sup_{|z|=r} |f(z)| > 0.$$

Analogous questions on the permissible growth rates of D-distributionally chaotic entire functions was subsequently investigated in [28] and [76].

On the other hand, entire functions $f \in H(\mathbb{C})$ that are hypercyclic with respect to the translation operators $T_a\colon f(z) \mapsto f(z + a)$, for $a \neq 0$, may have arbitrarily slow transcendental growth (cf. [98, Theorem 4.23]). For a function $\varphi\colon (0, \infty) \to [1, \infty)$, with $\varphi(r)/r^N \to \infty$ as $r \to \infty$ for any $N \geq 1$, there exists $f \in H(\mathbb{C})$ that is hypercyclic with respect to T_a such that

$$|f(z)| \leq C\varphi(r)$$

for $|z| = r > 0$ and where $C > 0$ is a constant.

In the frequently hypercyclic case, Blasco et al. [47] identified the following sharp result.

Theorem 6.2 (Blasco, Bonilla and Grosse-Erdmann [47])**.** *Let the function $\varphi\colon \mathbb{R}_+ \to \mathbb{R}_+$ be arbitrary. Then there exists a T_a-frequently hypercyclic $f \in H(\mathbb{C})$ with*

$$\sup_{|z|=r} |f(z)| \leq C\varphi(r)$$

for $r > 0$ sufficiently large and for some constant $C > 0$ if and only if

$$\liminf_{r\to\infty} \frac{\log \varphi(r)}{r} > 0.$$

Permissible growth rates of hypercyclic, frequently hypercyclic and distributionally chaotic operators acting on the space of harmonic functions on $\mathbb{R}^N$, for $N \geq 2$, have also been studied. With respect to the partial differentiation operators, the growth of harmonic functions was investigated in [1], [47], [78], [28] and [76]. For translation operators the permissible growth of hypercyclic and frequently hypercyclic harmonic functions was studied in [81] and [47].

6.1. **Structural Properties.** We let $HC(T)$ denote the set of hypercyclic vectors for the hypercyclic operator $T \in \mathscr{L}(X)$. Structural properties of the set $HC(T)$ have been extensively studied and this has led to some beautiful results.

For instance, Ansari [2] proved for a hypercyclic operator T and any $p \in \mathbb{N}$, that the powers T^p are also hypercyclic and that their sets of hypercyclic vectors coincide, i.e. $HC(T) = HC(T^p)$. This turns out to be a special case of an elegant result by Bourdon and Feldman [55], who showed that the T-orbit of any $x \in X$ is either everywhere dense or nowhere dense in X. The analogous result for frequent hypercyclicity was proven in [18], i.e. for frequently hypercyclic T and any $p \in \mathbb{N}$, it follows that T^p is frequently hypercyclic and their sets of frequently hypercyclic vectors coincide.

For hypercyclic $T \in \mathscr{L}(X)$, it is known that the set $HC(T)$ is a dense G_δ subset in X (cf. [22, Theorem 1.2]), so $HC(T)$ is large in a topological sense. As a consequence we have for any hypercyclic $T \in \mathscr{L}(X)$, that every vector $x \in X$ can be written as the sum of two hypercyclic vectors, i.e. $X = HC(T) + HC(T)$ (cf. [22, Proposition 1.29]).

An important result on the algebraic structure of the set $HC(T)$, due to Herrero and Bourdon, gives that every hypercyclic operator admits a dense invariant subspace in which every nonzero vector is hypercyclic. It then follows that the set $HC(T)$ is a connected subset of X (cf. [98, Theorem 2.55, Corollary 2.65]).

6.2. **Hypercyclic Subspaces.** For a hypercyclic operator $T \in \mathscr{L}(X)$, a *hypercyclic subspace* is defined as a closed infinite-dimensional subspace $M \subset X$ such that every nonzero vector in M is hypercyclic for T. Hypercyclic subspaces have amassed a vast literature since the early work of Bernal González and Montes-Rodríguez [30], and introductions to this subject can be found in [30, Chapter 8] and [98, Chapter 10].

We briefly remark that this topic fits into the broader area that seeks to identify (inside particular sets) large algebraic structures such as infinite-dimensional vector spaces, closed infinite-dimensional subspaces, and infinitely generated algebras. These properties are known as lineability, spaceability and algebrability, and we refer the curious reader to [5] and [31] to learn more about this interesting area.

In contrast to the generic property that $HC(T) \cup \{0\}$ always contains a dense subspace of hypercyclic vectors, it turns out that there exist hypercyclic operators that do not admit a hypercyclic subspace. On the other hand, examples of operators for which every nonzero vector is hypercyclic are uncommon, for instance the construction of Read [122].

Examples of operators that support hypercyclic subspaces include the differentiation and translation operators acting on $H(\mathbb{C})$ (cf. [98, Examples 10.12 and 10.13]). For $X = c_0$ or ℓ^p, $1 \leq p < \infty$, [98, Example 10.10] recalls that a weighted shift $B_w \in \mathscr{L}(X)$ that satisfies the Hypercyclicity Criterion admits a hypercyclic subspace if

$$\sup_{n \geq 1} \limsup_{k \to \infty} \prod_{j=1}^{n} |w_{j+k}| < \infty.$$

However, in [98, Examples 10.26] it is shown that scalar multiples of the backward shift $cB \in \mathscr{L}(X)$, for $|c| > 1$, do not possess hypercyclic subspaces.

The following characterisation of operators that satisfy the Hypercyclicity Criterion and admit a hypercyclic subspace was identified by González et al. [82].

Theorem 6.3 (González, León-Saavedra and Montes-Rodríguez [82]). *Let X be a separable complex Banach space and suppose that $T \in \mathscr{L}(X)$ satisfies the Hypercyclicity Criterion. The following are equivalent.*

(i) T possesses a hypercyclic subspace.

(ii) There exists some closed infinite-dimensional subspace $M_0 \subset X$ and an increasing sequence of integers (n_k) such that $T^{n_k}x \to 0$ for all $x \in M_0$.

(iii) There exists some closed infinite-dimensional subspace $M_0 \subset X$ and an increasing sequence of integers (n_k) such that $\sup_k \|T^{n_k}_{|M_0}\| < \infty$.

(iv) The essential spectrum of T intersects the closed unit disk.

An interesting question arising from Theorem 6.3 is whether there exists a characterisation of hypercyclic operators that admit a hypercyclic subspace that does not assume the Hypercyclicity Criterion.

We note in the Fréchet space setting that the existence of hypercyclic subspaces has recently been investigated by Menet [106, 108, 110].

For a family $(T_\lambda)_{\lambda\in\Lambda}$ of hypercyclic operators acting on the space X, we say $x \in X$ is a *common hypercyclic vector* if it is hypercyclic for each T_λ, $\lambda \in \Lambda$. Thus the common hypercyclic vectors are the elements of

$$\bigcap_{\lambda\in\Lambda} HC\,(T_\lambda)$$

and it immediately follows from the Baire category theorem if Λ is countable then the set of common hypercyclic vectors for $(T_\lambda)_{\lambda\in\Lambda}$ is a dense G_δ-set (cf. [98, Proposition 11.2]).

When the family $(T_\lambda)_{\lambda\in\Lambda}$ is uncountable, it is recalled in [22, Chapter 7] and [98, Chapter 11] that common hypercyclic vectors exist for the family of differentiation operators $(\lambda D)_{\lambda\neq 0}$ for $\lambda \in \mathbb{C}$, and for the family translation operators $(T_{e^{i\theta}})_\theta$ for $\theta \in [0,\, 2\pi)$ acting on the space $H(\mathbb{C})$. The multiples $(\lambda B)_\lambda$, for $|\lambda| > 1$, of the backward shift B on the sequence spaces c_0 or ℓ^p, $1 \leq p < \infty$, also possess common hypercyclic vectors (cf. [98, Example 11.11]). In each of these cases the families of operators in fact admit a dense G_δ set of common hypercyclic vectors. On the other hand, in [22, Example 7.1] they demonstrate that the hypercyclic weighted shifts B_w on ℓ^2 do not admit a common hypercyclic vector.

Hitherto, the results concerning common hypercyclic vectors were primarily for families indexed by a subset of $\mathbb{R}$. Notable examples in the two-dimensional case were by Shkarin [130] and Tsirivas [132]. Bayart [11] subsequently identified common hypercyclic vectors for higher-dimensional families $(T_\lambda)_{\lambda\in\mathbb{R}^d}$, for $d \geq 1$.

A natural question arising from this notion asks whether a family of operators can admit a common hypercyclic subspace. It turns out that even finitely many hypercyclic operators that possess hypercyclic subspaces need not share a common hypercyclic subspace. For instance, [98, Example 11.22] demonstrates that the operators $B_w \oplus B_v$ and $B_v \oplus B_w$ acting on the direct sum $\ell^2 \oplus \ell^2$ with

$$w_n = \frac{n+1}{n},\ v_n = 2,\ n \geq 1$$

both have hypercyclic subspaces but do not admit a common hypercyclic subspace.

On the other hand, [98, Example 11.28] gives for $X = c_0$ or ℓ^p, $1 \leq p < \infty$, that for $T \in \mathscr{L}(X)$ defined by

$$T(x_1,\, x_2,\, x_3, \dots) = (x_2,\, x_4,\, x_6, \dots),$$

the operators λT, $|\lambda| > 1$, have a common hypercyclic subspace.

Positive examples also include the countable family of composition operators C_{φ_j}, for a sequence $(\varphi_j)_{j\geq 1}$ of automorphisms of a domain $\Omega \subset \mathbb{C}$ (cf. [98, p. 328]). An interesting result from Menet [111] has shown that nonzero multiples of the differentiation operator $D\colon H(\mathbb{C}) \to H(\mathbb{C})$ and nonzero multiples of translation operators $T_a\colon H(\mathbb{C}) \to H(\mathbb{C})$, for $a \neq 0$, even share a common hypercyclic subspace!

Further research directions that have been pursued include the study of common $\mathcal{A}$-hypercyclic and common $\mathcal{U}$-frequently hypercyclic vectors, where sufficient conditions for their existence were identified by Mestiri [115]. Common and $\mathcal{U}$-frequently hypercyclic subspaces were also studied by Bès and Menet [40].

Frequently hypercyclic subspaces are defined as expected. They were originally investigated by Grosse-Erdmann and Bonilla [53], who provided the following sufficient condition for their existence.

Theorem 6.4 (Grosse-Erdmann and Bonilla [53])**.** *Let X be a separable Banach space and suppose that $T \in \mathscr{L}(X)$ satisfies the Frequent Hypercyclicity Criterion. If there exists a closed infinite-dimensional subspace $M_0 \subset X$ such that for all $x \in X_0$*

$$T^n x \to 0$$

then T possesses a frequently hypercyclic subspace.

It was demonstrated in [53] that the operator $\varphi(D)\colon H(\mathbb{C}) \to H(\mathbb{C})$ induced by the differentiation operator D supports a frequently hypercyclic subspace, where φ is an entire function of exponential type that is not a polynomial.

In contrast, it was proven by Bayart et al. [15] that the operator $P(D)$ acting on the space $H(\mathbb{C})$, where P is a nonconstant polynomial, is frequently hypercyclic but does not admit a frequently hypercyclic subspace. The result from [15] in fact identified a family a frequently hypercyclic operators that admits a hypercyclic subspace but does not support a frequently hypercyclic subspace. They even remark in [15] that it follows from a result of [40] that $P(D)$ even admits a $\mathcal{U}$-frequently hypercyclic subspace. Thus operators of the type $P(D)$ are frequently hypercyclic and support a $\mathcal{U}$-frequently hypercyclic but not a frequently hypercyclic subspace.

The first instance of a frequently hypercyclic operator that supports a hypercyclic but not a frequently hypercyclic subspace was identified by Menet [107] in answer to a question posed in [53]. The example from [107] was a weighted shift $B_w\colon \ell^p \to \ell^p$, for $1 \leq p < \infty$, with weights given by $w_k = 2$ if $k \in [a_{2n}, a_{2n+1})$ for some $n \geq 0$, and $w_k = 1$ otherwise. Here $(a_n)_{n\geq 0}$ is an appropriately chosen, strictly increasing sequence of integers.

6.3. **Hypercyclic Algebras.** When the space X supports an algebra structure, a question that has recently attracted much research activity is whether the set of hypercyclic vectors $HC(T)$ admits, apart from zero, a subalgebra of X. An up-to-date overview of this topic can be found in Bayart et al. [14].

We recall that the space $H(\mathbb{C})$ of entire functions is a Fréchet algebra when endowed with pointwise multiplication. It was shown by Aron et al. [6] that non-trivial translation operators $T_a\colon H(\mathbb{C}) \to H(\mathbb{C})$ do not support a hypercyclic algebras.

On the other hand, it was independently demonstrated (via different approaches) by Bayart and Matheron [22, Section 8.5], and Shkarin [129] that the differentiation operator $D\colon H(\mathbb{C}) \to H(\mathbb{C})$ admits a hypercyclic algebra. Bès et al. [37] subsequently extended this for convolution operators $\Phi(D)$ induced by the differentiation operator.

Theorem 6.5 (Bès, Conejero and Papathanasiou [37])**.** *Let $\Omega \subset \mathbb{C}$ be a simply connected domain and $H(\Omega)$ the space of holomorphic functions on Ω endowed with the compact open topology. Let Φ be a nonconstant polynomial with $\Phi(0) = 0$. Then the*

set of functions $f \in H(\Omega)$ that generate a hypercyclic algebra for $\Phi(D)$ is comeagre in $H(\Omega)$.

Bayart [12] identified the following characterisation for convolution operators in the case $|\Phi(0)| < 1$.

Theorem 6.6 (Bayart [12])**.** *Let Φ be a nonconstant entire function of exponential type. Assume that $|\Phi(0)| < 1$. The following are equivalent.*

(i) $\Phi(D)$ supports a hypercyclic algebra.

(ii) Φ is not a scalar multiple of an exponential function.

Sufficient conditions for convolution operators in the case $|\Phi(0)| = 1$ were also given in [12], and this was extended by Bès et al. [39] with the following theorem.

Theorem 6.7 (Bès, Ernst and Prieto [39])**.** *Let Φ be a nonconstant entire function of exponential type with $\Phi(0) = 1$. If Φ is of subexponential growth, then $\Phi(D)$ has a hypercyclic algebra.*

In [39] they augment Theorem 6.7 by giving sufficient conditions for convolution operators to admit a hypercyclic algebra in the case when Φ is not of subexponential growth.

The picture is not so clear for convolution operators with $|\Phi(0)| > 1$. An example in [12] demonstrates for $\Phi(z) = 2\exp(-z) + \sin z$, that $\Phi(D)$ supports a hypercyclic algebra. The following special case was also given in [14].

Theorem 6.8 (Bayart, Costa Júnior and Papathanasiou [14])**.** *Let Φ be a nonconstant entire function of exponential type that is not a multiple of an exponential function. Assume that $|\Phi(0)| > 1$ and that there exists some $w \in \mathbb{C}$ such that $|\Phi(tw)| \to 0$ as $t \to +\infty$. Then $\Phi(D)$ supports a hypercyclic algebra.*

The question of whether the operator D and convolution operators admit dense and infinitely generated hypercyclic algebras was recently investigated and answered in the affirmative by Bayart [12], Bernal-González and Calderón-Moreno [29], Falcó and Grosse-Erdmann [70], and Bès and Papathanasiou [43].

For a domain $\Omega \subset \mathbb{C}$, Bès et al. [38] proved that weighted composition operators $W_{\psi,\varphi}\colon H(\Omega) \to H(\Omega)$ cannot even support a supercyclic algebra, where a supercyclic algebra is defined as expected. However, the following theorem demonstrates that the situation is different if we consider the operator $P(C_\varphi)$ given by the nonconstant polynomial P.

Theorem 6.9 (Bayart [12])**.** *Let $\Omega \subset \mathbb{C}$ be a simply connected domain and let φ be a univalent holomorphic self-map of Ω which has no fixed point in Ω. Assume P is a nonconstant polynomial that is not a multiple of z and satisfies $|P(1)| < 1$. Then $P(C_\varphi)$ supports a hypercyclic algebra.*

The sequence space ℓ^1 is a Banach algebra when endowed with the convolution product $(u * v)(k) = \sum_{j=0}^{k} u_j v_{k-j}$, for $u, v \in \ell^1$. It was shown in [22, p. 217] that twice the backward shift $2B\colon \ell^1 \to \ell^1$ admits a hypercyclic algebra. This was subsequently extended in [12] with the following theorem.

Theorem 6.10 (Bayart [12])**.** *We consider the backward shift $B\colon \ell^1 \to \ell^1$ and let P be a nonconstant polynomial with complex coefficients. If $P(\mathbb{D}) \cap \mathbb{T} \neq \varnothing$, then the operator $P(B)$ admits a hypercyclic algebra.*

We note that an interesting example from [14, Example 4.12] identifies an invertible operator T acting on a Banach algebra, such that T supports a hypercyclic algebra while its inverse T^{-1} doe not admit a hypercyclic algebra.

The topic of hypercyclic algebras is rapidly evolving and research is expanding into different directions such as the investigation of frequently hypercyclic algebras [71], [14].

7. Some Open Questions

We finish by listing some interesting questions in linear dynamics that remain open. Most of the questions already appear in the literature and questions 1-3 were kindly suggested by Sophie Grivaux. Further open questions can also be found in [88] and [96].

Question 1. Find *natural* classes of $\mathcal{U}$-frequently hypercyclic operators on Hilbert and Banach spaces that are not frequently hypercyclic. Operators of C-type satisfying this description were identified in [91], but do examples exist among more *classical* operators?

Question 2. Characterise the operators $T_{\lambda,\omega} = D_\lambda + B_\omega$ of the form diagonal plus weighted backward shift, acting on a complex separable infinite-dimensional Hilbert space $\mathcal{H}$, which are hypercyclic, frequently hypercyclic or $\mathcal{U}$-frequently hypercyclic. Here, with respect to a fixed orthonormal basis of $\mathcal{H}$, the diagonal coefficients of D_λ are given by $\lambda = (\lambda_k)$, pairwise distinct unimodular complex numbers such that λ_k tends to 1 as $k \to \infty$, and for all $M > 0$ the weights $\omega = (\omega_k)$ satisfy $0 < \omega_k \leq M$ for every $k \geq 1$. (cf. [91, Section 4.3])

Question 3. On the classical Hardy space $H^2(\mathbb{D})$, characterise the hypercyclic Toeplitz operators, i.e. operators whose matrices with respect to the standard basis of $H^2(\mathbb{D})$ have constant diagonals (cf. [9]).

Question 4. Do examples of invertible frequently hypercyclic operators with non-frequently hypercyclic inverse exist on Hilbert or reflexive Banach spaces? (cf. [112])

Question 5. When the operator T is frequently hypercyclic, does it follow that the direct sum $T \oplus T$ is frequently hypercyclic? (cf. [19])

Question 6. Does every frequently hypercyclic operator admit a frequently hypercyclic vector with an irregularly visiting orbit? (cf. [89, Question 3.2])

Question 7. Does there exist a characterisation of operators that admit a hypercyclic subspace that does not assume the operator satisfies the Hypercyclicity Criterion?

Acknowledgements

The author is grateful to Frédéric Bayart, Sophie Grivaux, Karl Grosse-Erdmann, Quentin Menet and Alfred Peris for helpful suggestions during the initial stages of writing this survey. He wishes to thank Tom Carroll and Quentin Menet for reading this text and for valuable comments that have improved the article. He is also grateful to the anonymous referee for helpful remarks that improved the text. Permission from Quentin Menet for the use of Figure 7 is gratefully acknowledged. The author would also like to thank the editor Tony O'Farrell for the invitation to write this survey.

References

[1] M. P. Aldred and D. H. Armitage. Harmonic analogues of G. R. MacLane's universal functions. *J. London Math. Soc. (2)*, 57(1):148–156, 1998.
[2] S. I. Ansari. Hypercyclic and cyclic vectors. *J. Funct. Anal.*, 128(2):374–383, 1995.
[3] S. I. Ansari. Existence of hypercyclic operators on topological vector spaces. *J. Funct. Anal.*, 148(2):384–390, 1997.
[4] S. A. Argyros and R. G. Haydon. A hereditarily indecomposable $\mathcal{L}_\infty$-space that solves the scalar-plus-compact problem. *Acta Math.*, 206(1):1–54, 2011.

[5] R. M. Aron, L. Bernal González, D. M. Pellegrino, and J. B. Seoane Sepúlveda. *Lineability: the search for linearity in mathematics*. Monographs and Research Notes in Mathematics. CRC Press, Boca Raton, FL, 2016.
[6] R. M. Aron, J. A. Conejero, A. Peris, and J. B. Seoane-Sepúlveda. Powers of hypercyclic functions for some classical hypercyclic operators. *Integr. Equ. Oper. Theory*, 58(4):591–596, 2007.
[7] C. Badea and S. Grivaux. Unimodular eigenvalues, uniformly distributed sequences and linear dynamics. *Adv. Math.*, 211(2):766–793, 2007.
[8] J. Banks, J. Brooks, G. Cairns, G. Davis, and P. Stacey. On Devaney's definition of chaos. *Amer. Math. Monthly*, 99(4):332–334, 1992.
[9] A. Baranov and A. Lishanskii. Hypercyclic Toeplitz operators. *Results Math.*, 70(3-4):337–347, 2016.
[10] F. Bayart. Parabolic composition operators on the ball. *Adv. Math.*, 223(5):1666–1705, 2010.
[11] F. Bayart. Common hypercyclic vectors for high-dimensional families of operators. *Int. Math. Res. Not. IMRN*, (21):6512–6552, 2016.
[12] F. Bayart. Hypercyclic algebras. *J. Funct. Anal.*, 276(11):3441–3467, 2019.
[13] F. Bayart and S. Charpentier. Hyperbolic composition operators on the ball. *Trans. Amer. Math. Soc.*, 365(2):911–938, 2013.
[14] F. Bayart, F. Costa Júnior, and D. Papathanasiou. Baire theorem and hypercyclic algebras. arXiv:1910.05000, 2019.
[15] F. Bayart, R. Ernst, and Q. Menet. Non-existence of frequently hypercyclic subspaces for $P(D)$. *Israel J. Math.*, 214(1):149–166, 2016.
[16] F. Bayart and S. Grivaux. Hypercyclicité: le rôle du spectre ponctuel unimodulaire. *C. R. Math. Acad. Sci. Paris*, 338(9):703–708, 2004.
[17] F. Bayart and S. Grivaux. Hypercyclicity and unimodular point spectrum. *J. Funct. Anal.*, 226(2):281–300, 2005.
[18] F. Bayart and S. Grivaux. Frequently hypercyclic operators. *Trans. Amer. Math. Soc.*, 358(11):5083–5117, 2006.
[19] F. Bayart and S. Grivaux. Invariant Gaussian measures for operators on Banach spaces and linear dynamics. *Proc. Lond. Math. Soc. (3)*, 94(1):181–210, 2007.
[20] F. Bayart, K.-G. Grosse-Erdmann, V. Nestoridis, and C. Papadimitropoulos. Abstract theory of universal series and applications. *Proc. Lond. Math. Soc. (3)*, 96(2):417–463, 2008.
[21] F. Bayart and É. Matheron. Hypercyclic operators failing the hypercyclicity criterion on classical Banach spaces. *J. Funct. Anal.*, 250(2):426–441, 2007.
[22] F. Bayart and É. Matheron. *Dynamics of linear operators*, vol. 179 of *Cambridge Tracts in Mathematics*. Cambridge University Press, Cambridge, 2009.
[23] F. Bayart and E. Matheron. Mixing operators and small subsets of the circle. *J. Reine Angew. Math.*, 715:75–123, 2016.
[24] F. Bayart and I. Z. Ruzsa. Difference sets and frequently hypercyclic weighted shifts. *Ergodic Theory Dynam. Systems*, 35(3):691–709, 2015.
[25] B. Beauzamy. *Introduction to operator theory and invariant subspaces*, vol. 42 of *North-Holland Mathematical Library*. North-Holland Publishing Co., Amsterdam, 1988.
[26] T. Bermúdez, A. Bonilla, F. Martínez-Giménez, and A. Peris. Li-Yorke and distributionally chaotic operators. *J. Math. Anal. Appl.*, 373(1):83–93, 2011.
[27] L. Bernal-González. On hypercyclic operators on Banach spaces. *Proc. Amer. Math. Soc.*, 127(4):1003–1010, 1999.
[28] L. Bernal-González and A. Bonilla. Order of growth of distributionally irregular entire functions for the differentiation operator. *Complex Var. Elliptic Equ.*, 61(8):1176–1186, 2016.
[29] L. Bernal-González and M. d. C. Calderón-Moreno. Hypercyclic algebras for D-multiples of convolution operators. *Proc. Amer. Math. Soc.*, 147(2):647–653, 2019.
[30] L. Bernal González and A. Montes-Rodríguez. Universal functions for composition operators. *Complex Variables Theory Appl.*, 27(1):47–56, 1995.
[31] L. Bernal-González, D. Pellegrino, and J. B. Seoane-Sepúlveda. Linear subsets of nonlinear sets in topological vector spaces. *Bull. Amer. Math. Soc. (N.S.)*, 51(1):71–130, 2014.
[32] N. C. Bernardes, A. Bonilla, and A. Peris. Mean Li-Yorke chaos in Banach spaces. *J. Funct. Anal.*, 278(3):108343, 31, 2020.
[33] N. C. Bernardes, Jr., A. Bonilla, V. Müller, and A. Peris. Distributional chaos for linear operators. *J. Funct. Anal.*, 265(9):2143–2163, 2013.
[34] N. C. Bernardes, Jr., A. Bonilla, V. Müller, and A. Peris. Li-Yorke chaos in linear dynamics. *Ergodic Theory Dynam. Systems*, 35(6):1723–1745, 2015.

[35] N. C. Bernardes, Jr., A. Bonilla, A. Peris, and X. Wu. Distributional chaos for operators on Banach spaces. *J. Math. Anal. Appl.*, 459(2):797–821, 2018.
[36] J. Bès. Dynamics of weighted composition operators. *Complex Anal. Oper. Theory*, 8(1):159–176, 2014.
[37] J. Bès, J. A. Conejero, and D. Papathanasiou. Convolution operators supporting hypercyclic algebras. *J. Math. Anal. Appl.*, 445(2):1232–1238, 2017.
[38] J. Bès, J. A. Conejero, and D. Papathanasiou. Hypercyclic algebras for convolution and composition operators. *J. Funct. Anal.*, 274(10):2884–2905, 2018.
[39] J. Bès, R. Ernst, and A. Prieto. Hypercyclic algebras for convolution operators of unimodular constant term. *J. Math. Anal. Appl.*, 483(1):123595, 25, 2020.
[40] J. Bès and Q. Menet. Existence of common and upper frequently hypercyclic subspaces. *J. Math. Anal. Appl.*, 432(1):10–37, 2015.
[41] J. Bès, Q. Menet, A. Peris, and Y. Puig. Recurrence properties of hypercyclic operators. *Math. Ann.*, 366(1-2):545–572, 2016.
[42] J. Bès, Q. Menet, A. Peris, and Y. Puig. Strong transitivity properties for operators. *J. Differential Equations*, 266(2-3):1313–1337, 2019.
[43] J. Bès and D. Papathanasiou. Algebrable sets of hypercyclic vectors for convolution operators. *Israel J. Math.*, 238(1):91–119, 2020.
[44] J. Bès and A. Peris. Hereditarily hypercyclic operators. *J. Funct. Anal.*, 167(1):94–112, 1999.
[45] G. D. Birkhoff. Surface transformations and their dynamical applications. *Acta Math.*, 43(1):1–119, 1922.
[46] G. D. Birkhoff. Démonstration d'un théoreme elementaire sur les fonctions entieres. *C. R. Acad. Sci. Paris*, 189:473–475, 1929.
[47] O. Blasco, A. Bonilla, and K.-G. Grosse-Erdmann. Rate of growth of frequently hypercyclic functions. *Proc. Edinb. Math. Soc. (2)*, 53(1):39–59, 2010.
[48] J. Bonet and P. Domański. Hypercyclic composition operators on spaces of real analytic functions. *Math. Proc. Cambridge Philos. Soc.*, 153(3):489–503, 2012.
[49] J. Bonet, F. Martínez-Giménez, and A. Peris. A Banach space which admits no chaotic operator. *Bull. London Math. Soc.*, 33(2):196–198, 2001.
[50] J. Bonet, F. Martínez-Giménez, and A. Peris. Universal and chaotic multipliers on spaces of operators. *J. Math. Anal. Appl.*, 297(2):599–611, 2004.
[51] J. Bonet and A. Peris. Hypercyclic operators on non-normable Fréchet spaces. *J. Funct. Anal.*, 159(2):587–595, 1998.
[52] A. Bonilla and K.-G. Grosse-Erdmann. Frequently hypercyclic operators and vectors. *Ergodic Theory Dynam. Systems*, 27(2):383–404, 2007.
[53] A. Bonilla and K.-G. Grosse-Erdmann. Frequently hypercyclic subspaces. *Monatsh. Math.*, 168(3-4):305–320, 2012.
[54] A. Bonilla and K.-G. Grosse-Erdmann. Upper frequent hypercyclicity and related notions. *Rev. Mat. Complut.*, 31(3):673–711, 2018.
[55] P. S. Bourdon and N. S. Feldman. Somewhere dense orbits are everywhere dense. *Indiana Univ. Math. J.*, 52(3):811–819, 2003.
[56] P. S. Bourdon and J. H. Shapiro. Cyclic composition operators on H^2. In *Operator theory: operator algebras and applications, Part 2 (Durham, NH, 1988)*, vol. 51 of *Proc. Sympos. Pure Math.*, pp. 43–53. Amer. Math. Soc., Providence, RI, 1990.
[57] P. S. Bourdon and J. H. Shapiro. Cyclic phenomena for composition operators. *Mem. Amer. Math. Soc.*, 125(596):x+105, 1997.
[58] T. Carroll and C. Gilmore. Weighted composition operators on the Fock space and their dynamics. arXiv:1911.07254, 2019.
[59] I. Chalendar and J. R. Partington. *Modern approaches to the invariant-subspace problem*, vol. 188 of *Cambridge Tracts in Mathematics*. Cambridge University Press, Cambridge, 2011.
[60] K. C. Chan. Hypercyclicity of the operator algebra for a separable Hilbert space. *J. Operator Theory*, 42(2):231–244, 1999.
[61] S. Charpentier, K. Grosse-Erdmann, and Q. Menet. Chaos and frequent hypercyclicity for weighted shifts. arXiv:1911.09186, 2019.
[62] G. Costakis and M. Sambarino. Topologically mixing hypercyclic operators. *Proc. Amer. Math. Soc.*, 132(2):385–389, 2004.
[63] M. de la Rosa, L. Frerick, S. Grivaux, and A. Peris. Frequent hypercyclicity, chaos, and unconditional Schauder decompositions. *Israel J. Math.*, 190:389–399, 2012.
[64] M. de la Rosa and C. Read. A hypercyclic operator whose direct sum $T \oplus T$ is not hypercyclic. *J. Operator Theory*, 61(2):369–380, 2009.

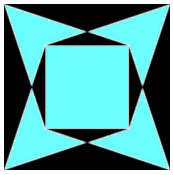
[65] R. L. Devaney. *An introduction to chaotic dynamical systems*. Addison-Wesley, Redwood City, CA, second edition, 1989.
[66] D. Drasin and E. Saksman. Optimal growth of entire functions frequently hypercyclic for the differentiation operator. *J. Funct. Anal.*, 263(11):3674–3688, 2012.
[67] P. Enflo. On the invariant subspace problem for Banach spaces. *Acta Math.*, 158(3-4):213–313, 1987.
[68] R. Ernst, C. Esser, and Q. Menet. $\mathcal{U}$-frequent hypercyclicity notions and related weighted densities. *Israel J. Math.*, to appear, 2019. arXiv:1907.05502.
[69] R. Ernst and A. Mouze. A quantitative interpretation of the frequent hypercyclicity criterion. *Ergodic Theory Dynam. Systems*, 39(4):898–924, 2019.
[70] J. Falcó and K.-G. Grosse-Erdmann. Algebrability of the set of hypercyclic vectors for backward shift operators. *Adv. Math.*, 366:107082, 2020.
[71] J. Falcó and K.-G. Grosse-Erdmann. Algebras of frequently hypercyclic vectors. *Math. Nachr.*, 293(6):1120–1135, 2020.
[72] C. Fernández, A. Galbis, and E. Jordá. Dynamics and spectra of composition operators on the Schwartz space. *J. Funct. Anal.*, 274(12):3503–3530, 2018.
[73] E. Flytzanis. Unimodular eigenvalues and linear chaos in Hilbert spaces. *Geom. Funct. Anal.*, 5(1):1–13, 1995.
[74] R. M. Gethner and J. H. Shapiro. Universal vectors for operators on spaces of holomorphic functions. *Proc. Amer. Math. Soc.*, 100(2):281–288, 1987.
[75] C. Gilmore. Dynamics of generalised derivations and elementary operators. *Complex Anal. Oper. Theory*, 13(1):257–274, 2019.
[76] C. Gilmore, F. Martínez-Giménez, and A. Peris. Rate of growth of distributionally chaotic functions. arXiv:1810.09266, 2018.
[77] C. Gilmore, E. Saksman, and H.-O. Tylli. Hypercyclicity properties of commutator maps. *Integr. Equ. Oper. Theory*, 87(1):139–155, 2017.
[78] C. Gilmore, E. Saksman, and H.-O. Tylli. Optimal growth of harmonic functions frequently hypercyclic for the partial differentiation operator. *Proc. Roy. Soc. Edinburgh Sect. A*, 149(6):1577–1594, 2019.
[79] E. Glasner and B. Weiss. A universal hypercyclic representation. *J. Funct. Anal.*, 268(11):3478–3491, 2015.
[80] G. Godefroy and J. H. Shapiro. Operators with dense, invariant, cyclic vector manifolds. *J. Funct. Anal.*, 98(2):229–269, 1991.
[81] M. C. Gómez-Collado, F. Martínez-Giménez, A. Peris, and F. Rodenas. Slow growth for universal harmonic functions. *J. Inequal. Appl.*, pp. 1–6, 2010.
[82] M. González, F. León-Saavedra, and A. Montes-Rodríguez. Semi-Fredholm theory: hypercyclic and supercyclic subspaces. *Proc. London Math. Soc. (3)*, 81(1):169–189, 2000.
[83] W. T. Gowers and B. Maurey. The unconditional basic sequence problem. *J. Amer. Math. Soc.*, 6(4):851–874, 1993.
[84] S. Grivaux. Hypercyclic operators, mixing operators, and the bounded steps problem. *J. Operator Theory*, 54(1):147–168, 2005.
[85] S. Grivaux. A new class of frequently hypercyclic operators. *Indiana Univ. Math. J.*, 60(4):1177–1201, 2011.
[86] S. Grivaux. A hypercyclic rank one perturbation of a unitary operator. *Math. Nachr.*, 285(5-6):533–544, 2012.
[87] S. Grivaux. Some new examples of universal hypercyclic operators in the sense of Glasner and Weiss. *Trans. Amer. Math. Soc.*, 369(11):7589–7629, 2017.
[88] S. Grivaux. Ten questions in linear dynamics. In *Études opératorielles*, vol. 112 of *Banach Center Publ.*, pp. 143–151. Polish Acad. Sci. Inst. Math., Warsaw, 2017.
[89] S. Grivaux. Frequently hypercyclic operators with irregularly visiting orbits. *J. Math. Anal. Appl.*, 462(1):542–553, 2018.
[90] S. Grivaux and É. Matheron. Invariant measures for frequently hypercyclic operators. *Adv. Math.*, 265:371–427, 2014.
[91] S. Grivaux, É. Matheron, and Q. Menet. Linear dynamical systems on Hilbert spaces: typical properties and explicit examples. *Mem. Amer. Math. Soc.*, to appear, 2017. arXiv:1703.01854.
[92] S. Grivaux and M. Roginskaya. On Read's type operators on Hilbert spaces. *Int. Math. Res. Not. IMRN* Art. ID rnn 083, 42, 2008.
[93] S. Grivaux and M. Roginskaya. A general approach to Read's type constructions of operators without non-trivial invariant closed subspaces. *Proc. Lond. Math. Soc. (3)*, 109(3):596–652, 2014.

[94] K.-G. Grosse-Erdmann. Universal families and hypercyclic operators. *Bull. Amer. Math. Soc. (N.S.)*, 36(3):345–381, 1999.
[95] K.-G. Grosse-Erdmann. Hypercyclic and chaotic weighted shifts. *Studia Math.*, 139(1):47–68, 2000.
[96] K.-G. Grosse-Erdmann. Frequently hypercyclic operators: recent advances and open problems. In *Advanced courses of mathematical analysis VI*, pp. 173–190. World Sci. Publ., Hackensack, NJ, 2017.
[97] K.-G. Grosse-Erdmann. Frequently hypercyclic bilateral shifts. *Glasg. Math. J.*, 61(2):271–286, 2019.
[98] K.-G. Grosse-Erdmann and A. Peris Manguillot. *Linear chaos*. Universitext. Springer, London, 2011.
[99] A. J. Guirao, V. Montesinos, and V. Zizler. *Open problems in the geometry and analysis of Banach spaces*. Springer, 2016.
[100] D. A. Herrero. Limits of hypercyclic and supercyclic operators. *J. Funct. Anal.*, 99(1):179–190, 1991.
[101] C. Kitai. *Invariant closed sets for linear operators*. PhD thesis, University of Toronto, 1982.
[102] T. Y. Li and J. A. Yorke. Period three implies chaos. *Amer. Math. Monthly*, 82(10):985–992, 1975.
[103] G. R. MacLane. Sequences of derivatives and normal families. *J. Analyse Math.*, 2:72–87, 1952.
[104] F. Martínez-Giménez, P. Oprocha, and A. Peris. Distributional chaos for backward shifts. *J. Math. Anal. Appl.*, 351(2):607–615, 2009.
[105] F. Martínez-Giménez, P. Oprocha, and A. Peris. Distributional chaos for operators with full scrambled sets. *Math. Z.*, 274(1-2):603–612, 2013.
[106] Q. Menet. Hypercyclic subspaces and weighted shifts. *Adv. Math.*, 255:305–337, 2014.
[107] Q. Menet. Existence and non-existence of frequently hypercyclic subspaces for weighted shifts. *Proc. Amer. Math. Soc.*, 143(6):2469–2477, 2015.
[108] Q. Menet. Hereditarily hypercyclic subspaces. *J. Operator Theory*, 73(2):385–405, 2015.
[109] Q. Menet. Linear chaos and frequent hypercyclicity. *Trans. Amer. Math. Soc.*, 369(7):4977–4994, 2017.
[110] Q. Menet. Invariant subspaces for non-normable Fréchet spaces. *Adv. Math.*, 339:495–539, 2018.
[111] Q. Menet. Existence of common hypercyclic subspaces for the derivative operator and the translation operators. *Rev. R. Acad. Cienc. Exactas Fís. Nat. Ser. A Mat. RACSAM*, 113(2):487–505, 2019.
[112] Q. Menet. Inverse of frequently hypercyclic operators. arXiv:1910.04452, 2019.
[113] Q. Menet. A bridge between $\mathcal{U}$-frequent hypercyclicity and frequent hypercyclicity. *J. Math. Anal. Appl.*, 482(2):123569, 15, 2020.
[114] Q. Menet. Inverse of $\mathcal{U}$-frequently hypercyclic operators. *J. Funct. Anal.*, 279(4):108543, 2020.
[115] M. Mestiri. Common upper frequent hypercyclicity. *Studia Math.*, 250(1):1–18, 2020.
[116] T. K. S. Moothathu. Two remarks on frequent hypercyclicity. *J. Math. Anal. Appl.*, 408(2):843–845, 2013.
[117] M. Murillo-Arcila and A. Peris. Strong mixing measures for linear operators and frequent hypercyclicity. *J. Math. Anal. Appl.*, 398(2):462–465, 2013.
[118] M. Murillo-Arcila and A. Peris. Strong mixing measures for C_0-semigroups. *Rev. R. Acad. Cienc. Exactas Fís. Nat. Ser. A Mat. RACSAM*, 109(1):101–115, 2015.
[119] J. Pal. Zwei kleine bemerkungen. *Tohoku Math. J.*, 6(6):42–43, 1914.
[120] H. Radjavi and P. Rosenthal. *Invariant subspaces*. Dover Publications, Inc., Mineola, NY, second edition, 2003.
[121] C. J. Read. A solution to the invariant subspace problem on the space l_1. *Bull. London Math. Soc.*, 17(4):305–317, 1985.
[122] C. J. Read. The invariant subspace problem for a class of Banach spaces. II. Hypercyclic operators. *Israel J. Math.*, 63(1):1–40, 1988.
[123] H. Rezaei. Chaotic property of weighted composition operators. *Bull. Korean Math. Soc.*, 48(6):1119–1124, 2011.
[124] S. Rolewicz. On orbits of elements. *Studia Math.*, 32:17–22, 1969.
[125] H. N. Salas. Hypercyclic weighted shifts. *Trans. Amer. Math. Soc.*, 347(3):993–1004, 1995.
[126] B. Schweizer and J. Smítal. Measures of chaos and a spectral decomposition of dynamical systems on the interval. *Trans. Amer. Math. Soc.*, 344(2):737–754, 1994.
[127] S. Shkarin. On the spectrum of frequently hypercyclic operators. *Proc. Amer. Math. Soc.*, 137(1):123–134, 2009.
[128] S. Shkarin. A hypercyclic finite rank perturbation of a unitary operator. *Math. Ann.*, 348(2):379–393, 2010.

[129] S. Shkarin. On the set of hypercyclic vectors for the differentiation operator. *Israel J. Math.*, 180:271–283, 2010.
[130] S. Shkarin. Remarks on common hypercyclic vectors. *J. Funct. Anal.*, 258(1):132–160, 2010.
[131] M. Taniguchi. Chaotic composition operators on the classical holomorphic spaces. *Complex Var. Theory Appl.*, 49(7-9):529–538, 2004.
[132] N. Tsirivas. Existence of common hypercyclic vectors for translation operators. *J. Operator Theory*, 80(2):257–294, 2018.

Cliff Gilmore is an IRC funded Government of Ireland Postdoctoral Fellow at UCC. His main research interests are currently in linear dynamics and quantum chaos. He completed his BSc(Hons) and MSc at NUI Galway, and he subsequently earned Licentiate and PhD degrees from the University of Helsinki.

School of Mathematical Sciences, University College Cork, Ireland.
E-mail address: clifford.gilmore@ucc.ie



Irish Math. Soc. Bulletin
Number 86, Winter 2020, 79–101
ISSN 0791-5578

The integral double Burnside ring of the symmetric group S_3

NORA KRAUSS

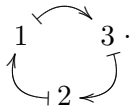
ABSTRACT. The double Burnside R-algebra $\mathrm{B}_R(G,G)$ of a finite group G with coefficients in a commutative ring R has been introduced by S. Bouc. It is R-linearly generated by finite (G,G)-bisets, modulo a relation identifying disjoint union and sum. Its multiplication is induced by the tensor product. In his thesis at NUI Galway, B. Masterson described $\mathrm{B}_{\mathbf{Q}}(\mathrm{S}_3,\mathrm{S}_3)$ as a subalgebra of $\mathbf{Q}^{8\times 8}$. We give a variant of this description and continue to describe $\mathrm{B}_R(\mathrm{S}_3,\mathrm{S}_3)$ for $R \in \{\mathbf{Z}, \mathbf{Z}_{(2)}, \mathbf{F}_2, \mathbf{Z}_{(3)}, \mathbf{F}_3\}$ via congruences as suborders of certain R-orders respectively via path algebras over R.

1. Introduction

1.1. **Groups.** Groups describe symmetries of objects. That is to say, any mathematical object X has a symmetry group, called automorphism group $\mathrm{Aut}(X)$, consisting of isomorphisms from X to X. For instance, for a natural number n, the set $\{1,2,\ldots,n\}$ has as automorphism group the symmetric group $\mathrm{Aut}(\{1,2,\ldots,n\}) = \mathrm{S}_n$. This group consists of all bijections from $\{1,2,\ldots,n\}$ to itself. For example, we obtain

$$\begin{aligned}\mathrm{S}_3 &= \left\{\begin{pmatrix}1&2&3\\1&2&3\end{pmatrix},\begin{pmatrix}1&2&3\\2&1&3\end{pmatrix},\begin{pmatrix}1&2&3\\3&2&1\end{pmatrix},\begin{pmatrix}1&2&3\\1&3&2\end{pmatrix},\begin{pmatrix}1&2&3\\2&3&1\end{pmatrix},\begin{pmatrix}1&2&3\\3&1&2\end{pmatrix}\right\}\\ &= \{\mathrm{id},(1,2),(1,3),(2,3),(1,2,3),(1,3,2)\}\ .\end{aligned}$$

In the first row, $\begin{pmatrix}1&2&3\\a&b&c\end{pmatrix}$ is the map sending $1\mapsto a$, $2\mapsto b$, $3\mapsto c$.

In the second row, we have used the cycle notation, e.g. $\begin{pmatrix}1&2&3\\3&1&2\end{pmatrix} = (1,3,2)$, the latter meaning 

.

We multiply by composition, e.g. $(1,2)\bullet(1,3) = (1,2,3)$.
By a theorem of Cayley, any finite group is isomorphic to a subgroup of S_n for some n.

1.2. **The Biset category and biset functors.** Suppose given finite groups H and G. An (H,G)-*biset* X is a finite set X together with a multiplication with elements of H on the left and a multiplication with elements of G on the right that commute with each other, i.e.

$$(h\cdot x)\cdot g = h\cdot(x\cdot g) =: h\cdot x\cdot g$$

for $h\in H$, $g\in G$ and $x\in X$.

As a first example, $M_1 := \mathrm{S}_3$ is a $(\mathrm{S}_2,\mathrm{S}_3)$-biset via multiplication in S_3. So for $h\in\mathrm{S}_2 = \{\mathrm{id},(1,2)\}$, $g\in\mathrm{S}_3$ and $x\in M_1$ we let $h\cdot x\cdot g := h\bullet x\bullet g$.

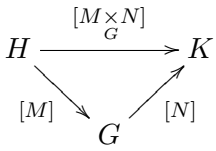
As a second example, consider the cyclic group $\mathrm{C}_3 = \{\mathrm{id},(1,2,3),(1,3,2)\}$ and the group isomorphism $\alpha:\mathrm{C}_3\to\mathrm{C}_3$, $x\mapsto x^2$. Then the set $M_2 := \mathrm{C}_3$ is a $(\mathrm{C}_3,\mathrm{C}_3)$-biset,

2020 *Mathematics Subject Classification.* 19A22.
Key words and phrases. double Burnside ring, symmetric group, path algebra.
Received on 3-9-2020; revised 15-10-2020.

on the left via multiplication, on the right via application of α and then multiplication. E.g.

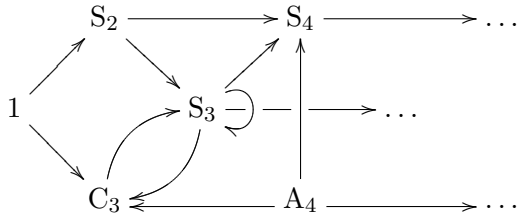
$$\begin{array}{rcll}(1,2,3)\cdot(1,3,2)\cdot(1,3,2) & = & (1,2,3)\bullet(1,3,2)\bullet\alpha((1,3,2)) & \\ & = & (1,2,3)\bullet(1,3,2)\bullet(1,2,3) & = \quad (1,2,3)\ .\end{array}$$

Suppose given a commutative ring R. S. Bouc introduced the *biset category* Biset_R, see [5, §3.1], see also the historical comments in [5, §1.4]. As objects, the category Biset_R has finite groups. The R-module of morphisms between two finite groups H and G is given by the double Burnside R-module $\mathrm{Biset}_R(H,G) = \mathrm{B}_R(H,G)$, which is R-linearly generated by finite (H,G)-bisets, modulo a relation identifying disjoint union and sum. In particular, each (H,G)-biset M yields a morphism $H \xrightarrow{[M]} G$ in Biset_R. Composition of morphisms in Biset_R is given by a tensor product operation on bisets that is similar to the tensor product of bimodules. Given an (H,G)-biset M and an (G,K)-biset N, we write $M \underset{G}{\times} N$ for their tensor product, which is an (H,K)-biset. So in Biset_R, we have the commutative triangle



.

The category Biset_R may roughly be imagined by a picture like this.



Here, A_4 is the alternating group on 4 elements. Each biset yields an arrow, and so does each R-linear combination of bisets. Of course, there are many more objects in Biset_R – each finite group is an object there – and many more arrows between them that are not in our picture.

1.3. **Biset functors.** Let $\mathcal{X}$ and $\mathcal{Y}$ be classes of finite groups closed under forming subgroups, factor groups and extensions. Following Bouc [3, §3.4.1], we say that an (H,G)-biset M is $(\mathcal{X},\mathcal{Y})$-*free* if for each $m \in M$ the left stabilizer of m in H is in $\mathcal{X}$ and the right stabilizer of m in G is in $\mathcal{Y}$. We have the subcategory $\mathrm{Biset}_R^{\mathcal{X},\mathcal{Y}}$ of Biset_R: As objects, it has finite groups. The R-module of morphisms in $\mathrm{Biset}_R^{\mathcal{X},\mathcal{Y}}$ between two finite groups H and G is given by the submodule of $\mathrm{B}_R(H,G)$ generated by the images of $(\mathcal{X},\mathcal{Y})$-free (H,G)-bisets, cf. [3, Lemme 4].

Certain classical theories may now be formulated as contravariant functors from $\mathrm{Biset}_R^{\mathcal{X},\mathcal{Y}}$ to the category of R-modules, called *biset functors* over R.

Consider a prime number p. Let $\mathcal{X}$ be the class of all finite groups. Let $\mathcal{Y}$ be the class of finite groups whose orders are not divisible by p. Then e.g. the $(\mathrm{S}_2,\mathrm{S}_3)$-biset M_1 and the $(\mathrm{C}_3,\mathrm{C}_3)$-biset M_2 from §1.2 yield morphisms in $\mathrm{Biset}_{\mathbf{Z}}^{\mathcal{X},\mathcal{Y}}$.

Suppose given an object of $\mathrm{Biset}_{\mathbf{Z}}^{\mathcal{X},\mathcal{Y}}$, i.e. a finite group G. Let

$$\mathbf{F}_p = \mathbf{Z}/p\mathbf{Z} = \{0,\ldots,p-1\}\ ,$$

where we agree to calculate modulo p. An $\mathbf{F}_p$-representation of G is a finite dimensional $\mathbf{F}_p$-vectorspace V, together with a left multiplication with elements of G. Such a representation is called simple if it does not have a nontrivial subrepresentation. Each

representation has a sequence of subrepresentations with simple steps, called composition factors.

Let $\mathrm{Rep}_{\mathbf{F}_p}(G)$ be the free abelian group on the set of isoclasses of simple representations. Each $\mathbf{F}_p$-representation V of G yields an element $[V]$ in $\mathrm{Rep}_{\mathbf{F}_p}(G)$, namely the formal sum of its composition factors. Given finite groups H and G and an (H,G)-biset M, we obtain the map

$$\begin{array}{ccc} \mathrm{Rep}_{\mathbf{F}_p}(G) & \xrightarrow{\mathrm{Rep}_{\mathbf{F}_p}([M])} & \mathrm{Rep}_{\mathbf{F}_p}(H) \\ [V] & \mapsto & [\mathbf{F}_pM \underset{\mathbf{F}_pG}{\otimes} V] \ , \end{array}$$

using the usual tensor product over rings.

These constructions furnish a contravariant $\mathbf{Z}$-linear functor $\mathrm{Rep}_{\mathbf{F}_p}$ from $\mathrm{Biset}_{\mathbf{Z}}^{\mathcal{X},\mathcal{Y}}$ to the category of $\mathbf{Z}$-modules, i.e. to the category of abelian groups. In particular, using the bisets M_1 and M_2 from §1.2, we obtain the maps

$$\begin{array}{ccc} \mathrm{Rep}_{\mathbf{F}_p}(\mathrm{S}_3) & \xrightarrow{\mathrm{Rep}_{\mathbf{F}_p}([M_1])} & \mathrm{Rep}_{\mathbf{F}_p}(\mathrm{S}_2) \\ [V] & \mapsto & [\text{restriction of } V \text{ to } \mathrm{S}_2] \end{array}$$

and

$$\begin{array}{ccc} \mathrm{Rep}_{\mathbf{F}_p}(\mathrm{C}_3) & \xrightarrow{\mathrm{Rep}_{\mathbf{F}_p}([M_2])} & \mathrm{Rep}_{\mathbf{F}_p}(\mathrm{C}_3) \\ [V] & \mapsto & [\text{twist of } V \text{ with } \alpha] \ . \end{array}$$

Note that, if $p \leq n$, even the simple $\mathbf{F}_p$-representations of S_n are not entirely known: One knows a construction, due to James [9], but one does not know their $\mathbf{F}_p$-dimensions. Biset functors do not directly aim to solve this problem, but at any rate they are a tool to work with these representations.

1.4. **Globally-defined Mackey functors.** There is an equivalence of categories between the category of biset functors over R and the category of *globally-defined Mackey functors* $\mathrm{Mack}_R^{\mathcal{X},\mathcal{Y}}$ [6, §8]. Here, a globally-defined Mackey functor, with respect to $\mathcal{X}$ and $\mathcal{Y}$, maps groups to R-modules and each group morphism α covariantly to an R-module morphism $\alpha_\star$, provided $\mathrm{kern}(\alpha) \in \mathcal{Y}$, and contravariantly to $\alpha^\star$, provided $\mathrm{kern}(\alpha) \in \mathcal{X}$. It is required that these morphisms satisfy a list of compatibilities, amongst which a Mackey formula, see e.g. [6, §8]. By that equivalence, these requirements on a Mackey functor can now be viewed as properties that result from being a contravariant functor from $\mathrm{Biset}_R^{\mathcal{X},\mathcal{Y}}$ to R-Mod.

1.5. **Further examples.** We list two examples of biset functors, [6, §8].

- Let $\mathcal{X} = \{1\}$ and let $\mathcal{Y}$ consist of all finite groups. Let $n \geq 0$. Consider the biset functor $\mathrm{Biset}_{\mathbf{Z}}^{\mathcal{X},\mathcal{Y}} \to \mathbf{Z}$-Mod that maps a finite group G to the algebraic K-theory $\mathrm{K}_n(\mathbf{Z}G)$ of $\mathbf{Z}G$.
- Let $\mathcal{X}$ consist of all finite groups and let $\mathcal{Y} = \{1\}$. Let $n \geq 0$. Consider the biset functor $\mathrm{Biset}_R^{\mathcal{X},\mathcal{Y}} \to R$-Mod that maps a finite group G to the cohomology $\mathrm{H}^n(G,R)$ of G with trivial coefficients.

For some more examples, see [6, §8]. The example of the classical Burnside ring, depending on a group G, is also explained in [4, §6.1].

1.6. **The double Burnside algebra.** Suppose given a finite group G, i.e an object of Biset_R. Its endomorphism ring $\mathrm{B}_R(G,G)$ in the category Biset_R is called *double Burnside algebra* of G.

The isomorphism classes of finite transitive (G,G)-bisets form an R-linear basis of $\mathrm{B}_R(G,G)$. In particular, if we choose a system $\mathcal{L}_{G\times G}$ of representatives for the conjugacy classes of subgroups of $G \times G$, we have the R-linear basis $([(G \times G)/U] : U \in \mathcal{L}_{G\times G})$.

If G is cyclic and if R is a field in which $|G|$ and $\varphi(|G|)$ are invertible, where φ denotes Euler's totient function, then the double Burnside algebra $\mathrm{B}_R(G,G)$ is semisimple. This is shown in [7, Theorem 8.11, Remark 8.12(a)].

In case of $G = \mathrm{S}_3$, we have 22 conjugacy classes of subgroups of $\mathrm{S}_3 \times \mathrm{S}_3$ and thus $\mathrm{rk}_R(\mathrm{B}_R(\mathrm{S}_3,\mathrm{S}_3)) = 22$. The double Burnside $\mathbf{Q}$-algebra $\mathrm{B}_{\mathbf{Q}}(\mathrm{S}_3,\mathrm{S}_3)$ has been described by B. Masterson [1, §8] and then by B. Masterson and G. Pfeiffer [2, §7]. We describe $\mathrm{B}_{\mathbf{Q}}(\mathrm{S}_3,\mathrm{S}_3)$ independently, using a direct Magma-supported calculation [10], with the aim of being able to pass from $\mathrm{B}_{\mathbf{Q}}(\mathrm{S}_3,\mathrm{S}_3)$ to $\mathrm{B}_{\mathbf{Z}}(\mathrm{S}_3,\mathrm{S}_3)$ in the sequel.

In order to do that, we first restate some preliminaries on bisets and the double Burnside ring in §2 and construct a $\mathbf{Z}$-linear basis of $\mathrm{B}_{\mathbf{Z}}(\mathrm{S}_3,\mathrm{S}_3)$ in §3.

In §4 we tackle the problem that the double Burnside $\mathbf{Q}$-algebra $\mathrm{B}_{\mathbf{Q}}(\mathrm{S}_3,\mathrm{S}_3)$ is not semisimple [5, Proposition 6.1.5], thus not isomorphic to a direct product of matrix rings. As a substitute, we use a suitable isomorphic copy A of $\mathrm{B}_{\mathbf{Q}}(\mathrm{S}_3,\mathrm{S}_3)$. We obtain this copy using a Peirce decomposition of $\mathrm{B}_{\mathbf{Q}}(\mathrm{S}_3,\mathrm{S}_3)$. In addition, we give a description of $\mathrm{B}_{\mathbf{Q}}(\mathrm{S}_3,\mathrm{S}_3)$ as path algebra modulo relations.

The next step, in §5, is to pass from $\mathrm{B}_{\mathbf{Q}}(\mathrm{S}_3,\mathrm{S}_3)$ to $\mathrm{B}_{\mathbf{Z}}(\mathrm{S}_3,\mathrm{S}_3)$. We find a $\mathbf{Z}$-order $A_{\mathbf{Z}}$ inside A such that $A_{\mathbf{Z}}$ contains an isomorphic copy of $\mathrm{B}_{\mathbf{Z}}(\mathrm{S}_3,\mathrm{S}_3)$, which we describe via congruences, cf. Proposition 5, Theorem 8.

$$\begin{array}{ccc} \mathrm{B}_{\mathbf{Q}}(\mathrm{S}_3,\mathrm{S}_3) & \xrightarrow{\ \sim\ } & A \\ \uparrow & & \uparrow \\ \mathrm{B}_{\mathbf{Z}}(\mathrm{S}_3,\mathrm{S}_3) & \xrightarrow{\text{injective}} & A_{\mathbf{Z}} \end{array}$$

We calculate a path algebra for $\mathrm{B}_{\mathbf{Z}_{(2)}}(\mathrm{S}_3,\mathrm{S}_3)$, cf. Proposition 11. We deduce that $\mathrm{B}_{\mathbf{F}_2}(\mathrm{S}_3,\mathrm{S}_3)$ is Morita equivalent to the path algebra

$$\mathbf{F}_2\left[\ \tilde{\mathrm{e}}_3 \underset{\tilde\tau_1}{\overset{\tilde\tau_2}{\rightleftarrows}} \tilde{\mathrm{e}}_5 \overset{\tilde\tau_4}{\underset{\tilde\tau_3}{\rightleftarrows}} \tilde{\mathrm{e}}_4 \ \circlearrowright \tilde\tau_7\ \right] \Big/ \begin{pmatrix} \tilde\tau_2\tilde\tau_1 & , & \tilde\tau_2\tilde\tau_3 & , & \tilde\tau_2\tilde\tau_7, \\ \tilde\tau_4\tilde\tau_1 & , & \tilde\tau_4\tilde\tau_3 & , & \tilde\tau_4\tilde\tau_7, \\ \tilde\tau_7\tilde\tau_1 & , & \tilde\tau_7\tilde\tau_3 & , & \tilde\tau_7^2 - \tilde\tau_1\tilde\tau_2 \end{pmatrix},$$

cf. Corollary 12.

We calculate a path algebra for $\mathrm{B}_{\mathbf{Z}_{(3)}}(\mathrm{S}_3,\mathrm{S}_3)$, cf. Proposition 15. We deduce that $\mathrm{B}_{\mathbf{F}_3}(\mathrm{S}_3,\mathrm{S}_3)$ is Morita equivalent to the path algebra

$$\mathbf{F}_3\left[\ \tilde{\mathrm{e}}_5 \qquad \tilde{\mathrm{e}}_3 \underset{\tilde\tau_1}{\overset{\tilde\tau_2}{\rightleftarrows}} \tilde{\mathrm{e}}_6 \underset{\tilde\tau_3}{\overset{\tilde\tau_4}{\rightleftarrows}} \tilde{\mathrm{e}}_4\ \right] \Big/ (\tilde\tau_4\tilde\tau_3,\ \tilde\tau_4\tilde\tau_1,\ \tilde\tau_2\tilde\tau_1,\ \tilde\tau_2\tilde\tau_3)\ ,$$

cf. Corollary 16.

2. Preliminaries on bisets and the double Burnside algebra

Bisets. Recall that an (G,G)-*biset* X is a finite set X together with a left G and a right G-action that commute with each other, i.e. $(h\cdot x)\cdot g = h\cdot(x\cdot g) =: h\cdot x\cdot g$ for $h,g\in G$ and $x\in X$.

Every (G,G)-biset X can be regarded as a left $(G\times G)$-set by setting $(h,g)x := hxg^{-1}$ for $(h,g)\in G\times G$ and $x\in X$. Likewise, every left $(G\times G)$-set Y can be regarded as an (G,G)-biset by setting $h\cdot y\cdot g := (h,g^{-1})y$ for $h,g\in G$ and $y\in Y$. We freely use this identification.

Tensor product. Let M be an (G,G)-biset and let N be a (G,G)-biset. The cartesian product $M \times N$ is a (G,G)-biset via $h(m,n)p = (hm, np)$ for $h,p \in G$ and $(m,n) \in M \times N$. It becomes a left G-set via $g(m,n) = (mg^{-1}, gn)$ for $g \in G$ and $(m,n) \in M \times N$. We call the set of G-orbits on $M \times N$ the *tensor product* $M \underset{G}{\times} N$ of M and N. This also is an (G,G)-biset. The G-orbit of the element $(m,n) \in M \times N$ is denoted by $m \underset{G}{\times} n \in M \underset{G}{\times} N$. Moreover, let L be a (G,G)-biset. Then $M \underset{G}{\times} (N \underset{G}{\times} L) \xrightarrow{\sim} (M \underset{G}{\times} N) \underset{G}{\times} L$, $m \underset{G}{\times} (n \underset{G}{\times} \ell) \mapsto (m \underset{G}{\times} n) \underset{G}{\times} \ell$ as (G,G)-bisets.

Double Burnside R-algebra. We denote by $\mathrm{B}_R(G,G)$ the double Burnside R-algebra of G. Recall that $\mathrm{B}_R(G,G)$ is the R-module freely generated by the isomorphism classes of finite (G,G)-bisets, modulo the relations $[M \sqcup N] = [M] + [N]$ for (G,G)-bisets M, N. Multiplication is defined by $[M] \underset{G}{\cdot} [N] = [M \underset{G}{\times} N]$ for (G,G)-bisets M, N. An R-linear basis of $\mathrm{B}_R(G,G)$ is given by $([(G \times G)/U] : U \in \mathcal{L}_{G\times G})$, where we choose a system $\mathcal{L}_{G\times G}$ of representatives for the conjugacy classes of subgroups of $G \times G$. Moreover, $1_{\mathrm{B}_{\mathbf{Z}}(G,G)} = [G]$.

Abbreviation. In case of $G = \mathrm{S}_3$, we often abbreviate $\mathrm{B}_R := \mathrm{B}_R(\mathrm{S}_3, \mathrm{S}_3)$.

3. $\mathbf{Z}$-linear basis of $\mathrm{B}_{\mathbf{Z}}(\mathrm{S}_3, \mathrm{S}_3)$

The following calculations were done using the computer algebra system Magma [10].

The group S_3 has the subgroups

$$V_0 := \{\mathrm{id}\},\ V_1 := \langle (1,2) \rangle,\ V_2 := \langle (1,3) \rangle,\ V_3 := \langle (2,3) \rangle,\ V_4 := \langle (1,2,3) \rangle,\ V_5 := \mathrm{S}_3\ .$$

The set $\{V_0,\ V_1,\ V_4,\ V_5\}$ is a system of representatives for the conjugacy classes of subgroups of S_3. In S_3, we write $a := (1,2)$, $b := (1,2,3)$ and $1 := \mathrm{id}$. So $V_1 = \langle a \rangle$, $V_4 = \langle b \rangle$ and $V_5 = \langle a, b \rangle$.

A system of representatives for the conjugacy classes of subgroups of $\mathrm{S}_3 \times \mathrm{S}_3$ is given by

$$\begin{array}{llll}
U_{0,0} := V_0 \times V_0 = \{(1,1)\}, & U_{4,1} := V_4 \times V_1 = \langle (b,1), (1,a) \rangle, \\
U_{1,0} := V_1 \times V_0 = \langle (a,1) \rangle, & U_{1,4} := V_1 \times V_4 = \langle (a,1), (1,b) \rangle, \\
U_{0,1} := V_0 \times V_1 = \langle (1,a) \rangle, & U_7 := \langle (a,a), (b,1) \rangle, \\
\Delta(V_1) = \langle (a,a) \rangle, & \Delta(V_5) = \langle (a,a), (b,b) \rangle, \\
U_{4,0} := V_4 \times V_0 = \langle (b,1) \rangle, & U_{4,4} := V_4 \times V_4 = \langle (b,1), (1,b) \rangle, \\
U_{0,4} := V_0 \times V_4 = \langle (1,b) \rangle, & U_{1,5} := V_1 \times V_5 = \langle (a,1), (1,a), (1,b) \rangle, \\
\Delta(V_4) = \langle (b,b) \rangle, & U_{5,1} := V_5 \times V_1 = \langle (a,1), (b,1), (1,a) \rangle, \\
U_{1,1} := V_1 \times V_1 = \langle (a,1), (1,a) \rangle, & U_{4,5} := V_4 \times V_5 = \langle (b,1), (1,a), (1,b) \rangle, \\
U_{5,0} := V_5 \times V_0 = \langle (a,1), (b,1) \rangle, & U_{5,4} := V_5 \times V_4 = \langle (a,1), (b,1), (1,b) \rangle, \\
U_{0,5} := V_0 \times V_5 = \langle (1,a), (1,b) \rangle, & U_8 := \langle (a,a), (b,1), (1,b) \rangle, \\
U_6 := \langle (a,a), (1,b) \rangle, & U_{5,5} := V_5 \times V_5 = \langle (a,1), (1,a), (b,1), (1,b) \rangle.
\end{array}$$

Let $H_{i,j} := [(\mathrm{S}_3 \times \mathrm{S}_3)/U_{i,j}]$ for $i,j \in \{0,1,4,5\}$, $H_s := [(\mathrm{S}_3 \times \mathrm{S}_3)/U_s]$ for $s \in [6,8]$ and $H_t^{\Delta} := [(\mathrm{S}_3 \times \mathrm{S}_3)/\Delta(V_t)]$ for $t \in \{1,4,5\}$.

So we obtain the $\mathbf{Z}$-linear basis

$$\begin{array}{ll}
\mathcal{H} := & (H_{0,0}, H_{1,0}, H_{0,1}, H_1^{\Delta}, H_{4,0}, H_{0,4}, H_4^{\Delta}, H_{1,1}, H_{5,0}, H_{0,5}, H_6, \\
& H_{4,1}, H_{1,4}, H_7, H_5^{\Delta}, H_{4,4}, H_{1,5}, H_{5,1}, H_{4,5}, H_{5,4}, H_8, H_{5,5})
\end{array}$$

of $\mathrm{B}_{\mathbf{Z}}(\mathrm{S}_3, \mathrm{S}_3)$. Of course, $\mathcal{H}$ is also a $\mathbf{Q}$-linear basis of $\mathrm{B}_{\mathbf{Q}}(\mathrm{S}_3, \mathrm{S}_3)$.

4. $\mathrm{B}_{\mathbf{Q}}(\mathrm{S}_3, \mathrm{S}_3)$

4.1. **Peirce decomposition of $\mathrm{B}_{\mathbf{Q}}(\mathrm{S}_3, \mathrm{S}_3)$.** Using Magma [10] we obtain an orthogonal decomposition of $1_{\mathrm{B}_{\mathbf{Q}}}$ into the following idempotents of $\mathrm{B}_{\mathbf{Q}} = \mathrm{B}_{\mathbf{Q}}(\mathrm{S}_3, \mathrm{S}_3)$.

$$\begin{array}{rcl}
e & := & -\frac{1}{2}H_{0,0} + H_{1,0} + \frac{1}{2}H_{4,0} \\
g & := & \frac{4}{3}H_{0,0} - 2H_{1,0} - \frac{4}{3}H_{0,1} - H_{4,0} + 2H_{1,1} + H_{4,1} \\
h & := & -\frac{1}{12}H_{0,0} + \frac{1}{3}H_{0,1} + \frac{1}{4}H_{4,0} - \frac{1}{4}H_{0,4} + \frac{3}{4}H_{4,4} - H_{4,1} \\
\varepsilon_2 & := & -H_{0,0} + H_{1,0} + H_{0,1} + H_1^{\Delta} - 2H_{1,1} \\
\varepsilon_3 & := & -\frac{1}{4}H_{0,0} + \frac{1}{4}H_{4,0} + \frac{1}{4}H_{0,4} + \frac{1}{2}H_4^{\Delta} - \frac{3}{4}H_{4,4} \\
\varepsilon_4 & := & \frac{1}{2}H_{0,0} - H_1^{\Delta} - \frac{1}{2}H_4^{\Delta} + H_5^{\Delta}
\end{array}$$

Write $\varepsilon_1 := e + g + h$. In Remark 1 and Remark 3, we shall see that these idempotents are primitive. In a next step, we fix $\mathbf{Q}$-linear bases of the Peirce components.

Peirce component	$\mathbf{Q}$-linear basis
$e\,\mathrm{B}_{\mathbf{Q}}\,e$	$e = -\frac{1}{2}H_{0,0} + H_{1,0} + \frac{1}{2}H_{4,0}$
$e\,\mathrm{B}_{\mathbf{Q}}\,g$	$b_{e,g} := \frac{1}{2}H_{0,0} - H_{1,0} - \frac{1}{2}H_{0,1} - \frac{1}{2}H_{4,0} + H_{1,1} + \frac{1}{2}H_{4,1}$
$e\,\mathrm{B}_{\mathbf{Q}}\,h$	$b_{e,h} := -\frac{1}{8}H_{0,0} + \frac{1}{4}H_{1,0} + \frac{1}{2}H_{0,1} + \frac{1}{8}H_{4,0} - \frac{3}{8}H_{0,4} - H_{1,1} - \frac{1}{2}H_{4,1} + \frac{3}{4}H_{1,4} + \frac{3}{8}H_{4,4}$
$g\,\mathrm{B}_{\mathbf{Q}}\,e$	$b_{g,e} := -\frac{4}{3}H_{0,0} + 2H_{1,0} + H_{4,0}$
$g\,\mathrm{B}_{\mathbf{Q}}\,g$	$g = \frac{4}{3}H_{0,0} - 2H_{1,0} - \frac{4}{3}H_{0,1} - H_{4,0} + 2H_{1,1} + H_{4,1}$
$g\,\mathrm{B}_{\mathbf{Q}}\,h$	$b_{g,h} := -\frac{1}{3}H_{0,0} + \frac{1}{2}H_{1,0} + \frac{4}{3}H_{0,1} + \frac{1}{4}H_{4,0} - H_{0,4} - 2H_{1,1} - H_{4,1} + \frac{3}{2}H_{1,4} + \frac{3}{4}H_{4,4}$
$h\,\mathrm{B}_{\mathbf{Q}}\,e$	$b_{h,e} := -\frac{1}{3}H_{0,0} + H_{4,0}$
$h\,\mathrm{B}_{\mathbf{Q}}\,g$	$b_{h,g} := \frac{1}{3}H_{0,0} - \frac{1}{3}H_{0,1} - H_{4,0} + H_{4,1}$
$h\,\mathrm{B}_{\mathbf{Q}}\,h$	$h = -\frac{1}{12}H_{0,0} + \frac{1}{3}H_{0,1} + \frac{1}{4}H_{4,0} - \frac{1}{4}H_{0,4} + \frac{3}{4}H_{4,4} - H_{4,1}$
$e\,\mathrm{B}_{\mathbf{Q}}\,\varepsilon_4$	$b_{e,\varepsilon_4} := -\frac{1}{8}H_{0,0} + \frac{1}{4}H_{1,0} + \frac{1}{4}H_{0,1} + \frac{1}{8}H_{4,0} + \frac{1}{8}H_{0,4} - \frac{1}{2}H_{1,1} - \frac{1}{4}H_{0,5} - \frac{1}{4}H_{4,1} - \frac{1}{4}H_{1,4} - \frac{1}{8}H_{4,4} + \frac{1}{2}H_{1,5} + \frac{1}{4}H_{4,5}$
$g\,\mathrm{B}_{\mathbf{Q}}\,\varepsilon_4$	$b_{g,\varepsilon_4} := -\frac{1}{3}H_{0,0} + \frac{1}{2}H_{1,0} + \frac{2}{3}H_{0,1} + \frac{1}{4}H_{4,0} + \frac{1}{3}H_{0,4} - H_{1,1} - \frac{2}{3}H_{0,5} - \frac{1}{2}H_{4,1} - \frac{1}{2}H_{1,4} - \frac{1}{4}H_{4,4} + H_{1,5} + \frac{1}{2}H_{4,5}$
$h\,\mathrm{B}_{\mathbf{Q}}\,\varepsilon_4$	$b_{h,\varepsilon_4} := -\frac{1}{12}H_{0,0} + \frac{1}{6}H_{0,1} + \frac{1}{4}H_{4,0} + \frac{1}{12}H_{0,4} - \frac{1}{6}H_{0,5} - \frac{1}{2}H_{4,1} - \frac{1}{4}H_{4,4} + \frac{1}{2}H_{4,5}$
$\varepsilon_2\,\mathrm{B}_{\mathbf{Q}}\,\varepsilon_2$	$\varepsilon_2 = -H_{0,0} + H_{1,0} + H_{0,1} + H_1^{\Delta} - 2H_{1,1}$
$\varepsilon_2\,\mathrm{B}_{\mathbf{Q}}\,\varepsilon_4$	$b_{\varepsilon_2,\varepsilon_4} := -\frac{1}{2}H_{0,0} + \frac{1}{2}H_{1,0} + \frac{1}{2}H_{0,1} + \frac{1}{2}H_1^{\Delta} + \frac{1}{2}H_{0,4} - H_{1,1} - \frac{1}{2}H_{0,5} - \frac{1}{2}H_6 - \frac{1}{2}H_{1,4} + H_{1,5}$
$\varepsilon_3\,\mathrm{B}_{\mathbf{Q}}\,\varepsilon_3$	$\varepsilon_3 = -\frac{1}{4}H_{0,0} + \frac{1}{4}H_{4,0} + \frac{1}{4}H_{0,4} + \frac{1}{2}H_4^{\Delta} - \frac{3}{4}H_{4,4}$
$\varepsilon_4\,\mathrm{B}_{\mathbf{Q}}\,e$	$b_{\varepsilon_4,e} := \frac{1}{6}H_{0,0} - \frac{1}{3}H_{1,0} - \frac{1}{6}H_{4,0} + \frac{1}{3}H_{5,0}$
$\varepsilon_4\,\mathrm{B}_{\mathbf{Q}}\,g$	$b_{\varepsilon_4,g} := -\frac{1}{6}H_{0,0} + \frac{1}{3}H_{1,0} + \frac{1}{6}H_{0,1} + \frac{1}{6}H_{4,0} - \frac{1}{3}H_{1,1} - \frac{1}{3}H_{5,0} - \frac{1}{6}H_{4,1} + \frac{1}{3}H_{5,1}$
$\varepsilon_4\,\mathrm{B}_{\mathbf{Q}}\,h$	$b_{\varepsilon_4,h} := \frac{1}{24}H_{0,0} - \frac{1}{12}H_{1,0} - \frac{1}{6}H_{0,1} - \frac{1}{24}H_{4,0} + \frac{1}{8}H_{0,4} + \frac{1}{3}H_{1,1} + \frac{1}{12}H_{5,0} + \frac{1}{6}H_{4,1} - \frac{1}{4}H_{1,4} - \frac{1}{8}H_{4,4} - \frac{1}{3}H_{5,1} + \frac{1}{4}H_{5,4}$
$\varepsilon_4\,\mathrm{B}_{\mathbf{Q}}\,\varepsilon_2$	$b_{\varepsilon_4,\varepsilon_2} := -\frac{1}{2}H_{0,0} + \frac{1}{2}H_{1,0} + \frac{1}{2}H_{0,1} + \frac{1}{2}H_1^{\Delta} + \frac{1}{2}H_{4,0} - H_{1,1} - \frac{1}{2}H_{5,0} - \frac{1}{2}H_{4,1} - \frac{1}{2}H_7 + H_{5,1}$
$\varepsilon_4\,\mathrm{B}_{\mathbf{Q}}\,\varepsilon_4$	$\varepsilon_4 = \frac{1}{2}H_{0,0} - H_1^{\Delta} - \frac{1}{2}H_4^{\Delta} + H_5^{\Delta}$, $b'_{\varepsilon_4,\varepsilon_4} := \frac{1}{24}H_{0,0} - \frac{1}{12}H_{1,0} - \frac{1}{12}H_{0,1} - \frac{1}{24}H_{4,0} - \frac{1}{24}H_{0,4} + \frac{1}{6}H_{1,1} + \frac{1}{12}H_{5,0} + \frac{1}{12}H_{0,5} + \frac{1}{12}H_{4,1} + \frac{1}{12}H_{1,4} + \frac{1}{24}H_{4,4} - \frac{1}{6}H_{1,5} - \frac{1}{6}H_{5,1} - \frac{1}{12}H_{4,5} - \frac{1}{12}H_{5,4} + \frac{1}{6}H_{5,5}$, $b''_{\varepsilon_4,\varepsilon_4} := \frac{1}{4}H_{0,0} - \frac{3}{4}H_{1,0} - \frac{3}{4}H_{0,1} + \frac{1}{4}H_1^{\Delta} - \frac{1}{4}H_{4,0} - \frac{1}{4}H_{0,4} + \frac{3}{2}H_{1,1} + \frac{3}{4}H_{5,0} + \frac{3}{4}H_{0,5} - \frac{1}{4}H_6 + \frac{3}{4}H_{4,1} + \frac{3}{4}H_{1,4} - \frac{1}{4}H_7 + \frac{1}{4}H_{4,4} - \frac{3}{2}H_{1,5} - \frac{3}{2}H_{5,1} - \frac{3}{4}H_{4,5} - \frac{3}{4}H_{5,4} + \frac{1}{4}H_8 + \frac{3}{2}H_{5,5}$

Remark 1. The idempotents $e, g, h, \varepsilon_2, \varepsilon_3$ are primitive, as $e\,\mathrm{B}_{\mathbf{Q}}\,e \cong \mathbf{Q}$, $g\,\mathrm{B}_{\mathbf{Q}}\,g \cong \mathbf{Q}$, $h\,\mathrm{B}_{\mathbf{Q}}\,h \cong \mathbf{Q}$, $\varepsilon_2\,\mathrm{B}_{\mathbf{Q}}\,\varepsilon_2 \cong \mathbf{Q}$ and $\varepsilon_3\,\mathrm{B}_{\mathbf{Q}}\,\varepsilon_3 \cong \mathbf{Q}$.

We have the following multiplication table for the basis elements of $\mathrm{B}_{\mathbf{Q}} = \mathrm{B}_{\mathbf{Q}}(\mathrm{S}_3, \mathrm{S}_3)$.

$(\cdot)$	e	$b_{e,g}$	$b_{e,h}$	$b_{g,e}$	g	$b_{g,h}$	$b_{h,e}$	$b_{h,g}$	h	b_{e,ε_4}	b_{g,ε_4}	b_{h,ε_4}	ε_2	$b_{\varepsilon_2,\varepsilon_4}$	ε_3	$b_{\varepsilon_4,e}$	$b_{\varepsilon_4,g}$	$b_{\varepsilon_4,h}$	$b_{\varepsilon_4,\varepsilon_2}$	ε_4	$b'_{\varepsilon_4,\varepsilon_4}$	$b''_{\varepsilon_4,\varepsilon_4}$
e	e	$b_{e,g}$	$b_{e,h}$	0	0	0	0	0	0	b_{e,ε_4}	0	0	0	0	0	0	0	0	0	0	0	0
$b_{e,g}$	0	0	0	e	$b_{e,g}$	$b_{e,h}$	0	0	0	0	b_{e,ε_4}	0	0	0	0	0	0	0	0	0	0	0
$b_{e,h}$	0	0	0	0	0	0	e	$b_{e,g}$	$b_{e,h}$	0	0	b_{e,ε_4}	0	0	0	0	0	0	0	0	0	0
$b_{g,e}$	$b_{g,e}$	g	$b_{g,h}$	0	0	0	0	0	0	b_{g,ε_4}	0	0	0	0	0	0	0	0	0	0	0	0
g	0	0	0	$b_{g,e}$	g	$b_{g,h}$	0	0	0	0	b_{g,ε_4}	0	0	0	0	0	0	0	0	0	0	0
$b_{g,h}$	0	0	0	0	0	0	$b_{g,e}$	g	$b_{g,h}$	0	0	b_{g,ε_4}	0	0	0	0	0	0	0	0	0	0
$b_{h,e}$	$b_{h,e}$	$b_{h,g}$	h	0	0	0	0	0	0	b_{h,ε_4}	0	0	0	0	0	0	0	0	0	0	0	0
$b_{h,g}$	0	0	0	$b_{h,e}$	$b_{h,g}$	h	0	0	0	0	b_{h,ε_4}	0	0	0	0	0	0	0	0	0	0	0
h	0	0	0	0	0	0	$b_{h,e}$	$b_{h,g}$	h	0	0	b_{h,ε_4}	0	0	0	0	0	0	0	0	0	0
b_{e,ε_4}	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	b_{e,ε_4}	0	0
b_{g,ε_4}	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	b_{g,ε_4}	0	0
b_{h,ε_4}	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	b_{h,ε_4}	0	0
ε_2	0	0	0	0	0	0	0	0	0	0	0	0	ε_2	$b_{\varepsilon_2,\varepsilon_4}$	0	0	0	0	0	0	0	0
$b_{\varepsilon_2,\varepsilon_4}$	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	$b_{\varepsilon_2,\varepsilon_4}$	0	0
ε_3	0	0	0	0	0	0	0	0	0	0	0	0	0	0	ε_3	0	0	0	0	0	0	0
$b_{\varepsilon_4,e}$	$b_{\varepsilon_4,e}$	$b_{\varepsilon_4,g}$	$b_{\varepsilon_4,h}$	0	0	0	0	0	0	$b'_{\varepsilon_4,\varepsilon_4}$	0	0	0	0	0	0	0	0	0	0	0	0
$b_{\varepsilon_4,g}$	0	0	0	$b_{\varepsilon_4,e}$	$b_{\varepsilon_4,g}$	$b_{\varepsilon_4,h}$	0	0	0	0	$b'_{\varepsilon_4,\varepsilon_4}$	0	0	0	0	0	0	0	0	0	0	0
$b_{\varepsilon_4,h}$	0	0	0	0	0	0	$b_{\varepsilon_4,e}$	$b_{\varepsilon_4,g}$	$b_{\varepsilon_4,h}$	0	0	$b'_{\varepsilon_4,\varepsilon_4}$	0	0	0	0	0	0	0	0	0	0
$b_{\varepsilon_4,\varepsilon_2}$	0	0	0	0	0	0	0	0	0	0	0	0	$b_{\varepsilon_4,\varepsilon_2}$	$b''_{\varepsilon_4,\varepsilon_4} - 12b'_{\varepsilon_4,\varepsilon_4}$	0	0	0	0	0	0	0	0
ε_4	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	$b_{\varepsilon_4,e}$	$b_{\varepsilon_4,g}$	$b_{\varepsilon_4,h}$	$b_{\varepsilon_4,\varepsilon_2}$	ε_4	$b'_{\varepsilon_4,\varepsilon_4}$	$b''_{\varepsilon_4,\varepsilon_4}$
$b'_{\varepsilon_4,\varepsilon_4}$	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	$b'_{\varepsilon_4,\varepsilon_4}$	0	0
$b''_{\varepsilon_4,\varepsilon_4}$	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	$b''_{\varepsilon_4,\varepsilon_4}$	0	0

We see that ε_3 is even a central element.

Lemma 2. *Consider* $\mathbf{Q}[\eta,\xi]/(\eta^2, \eta\xi, \xi^2) = \mathbf{Q}[\overline{\eta}, \overline{\xi}]$, *where* $\overline{\xi} := \xi + (\eta^2, \eta\xi, \xi^2)$ *and* $\overline{\eta} := \eta + (\eta^2, \eta\xi, \xi^2)$.

We have the $\mathbf{Q}$*-algebra isomorphism*

$$\begin{array}{rccc} \mu: & \mathbf{Q}[\overline{\eta}, \overline{\xi}] & \to & \varepsilon_4\,\mathrm{B}_{\mathbf{Q}}\,\varepsilon_4 \\ & \overline{\eta} & \mapsto & b'_{\varepsilon_4,\varepsilon_4} \\ & \overline{\xi} & \mapsto & b''_{\varepsilon_4,\varepsilon_4}\ . \end{array}$$

Proof. Since $\varepsilon_4\,\mathrm{B}_{\mathbf{Q}}\,\varepsilon_4 = {}_{\mathbf{Q}}\langle \varepsilon_4, b'_{\varepsilon_4,\varepsilon_4}, b''_{\varepsilon_4,\varepsilon_4}\rangle$ is commutative and $(b'_{\varepsilon_4,\varepsilon_4})^2 = 0$, $(b''_{\varepsilon_4,\varepsilon_4})^2 = 0$ and $b'_{\varepsilon_4,\varepsilon_4} b''_{\varepsilon_4,\varepsilon_4} = 0$, the map μ is a well-defined $\mathbf{Q}$-algebra morphism.

As the $\mathbf{Q}$-linear basis $(1, \overline{\eta}, \overline{\xi})$ is mapped to the $\mathbf{Q}$-linear basis $(\varepsilon_4, b'_{\varepsilon_4,\varepsilon_4}, b''_{\varepsilon_4,\varepsilon_4})$, it is bijective. □

Remark 3. *The ring* $\mathbf{Q}[\overline{\eta}, \overline{\xi}]$ *is local. In particular,* ε_4 *is a primitive idempotent of* $\mathrm{B}_{\mathbf{Q}}$.

Proof. We have $\mathrm{U}(\mathbf{Q}[\overline{\eta}, \overline{\xi}]) = \mathbf{Q}[\overline{\eta}, \overline{\xi}] \setminus (\overline{\eta}, \overline{\xi})$, as for $u := a + b\overline{\eta} + c\overline{\xi}$ the inverse is given by $u^{-1} = a^{-1} - a^{-2}b\overline{\eta} - a^{-2}c\overline{\xi}$ for $a, b, c \in \mathbf{Q}$, with $a \neq 0$. Thus the nonunits of $\mathbf{Q}[\overline{\eta}, \overline{\xi}]$ form an ideal and so $\mathbf{Q}[\overline{\eta}, \overline{\xi}]$ is a local ring. □

To standardize notation, we aim to construct a $\mathbf{Q}$-algebra $A := \bigoplus_{i,j} A_{i,j}$ such that $A \cong \mathrm{B}_{\mathbf{Q}}(\mathrm{S}_3, \mathrm{S}_3)$.

In a first step to do so, we choose $\mathbf{Q}$-vector spaces $A_{i,j}$ and $\mathbf{Q}$-linear isomorphisms $\gamma_{i,j} : A_{i,j} \xrightarrow{\sim} \varepsilon_i \, \mathrm{B}_{\mathbf{Q}} \, \varepsilon_j$ for $i, j \in [1,4]$. We define the tuple of $\mathbf{Q}$-vector spaces

$$\begin{array}{llll} (A_{1,1}\,, & A_{1,2}\,, & A_{1,3}\,, & A_{1,4}\,, \\ A_{2,1}\,, & A_{2,2}\,, & A_{2,3}\,, & A_{2,4}\,, \\ A_{3,1}\,, & A_{3,2}\,, & A_{3,3}\,, & A_{3,4}\,, \\ A_{4,1}\,, & A_{4,2}\,, & A_{4,3}\,, & A_{4,4}) \end{array} := \begin{array}{llll} (\mathbf{Q}^{3\times 3}\,, & 0\,, & 0\,, & \mathbf{Q}^{3\times 1}\,, \\ 0\,, & \mathbf{Q}\,, & 0\,, & \mathbf{Q}\,, \\ 0\,, & 0\,, & \mathbf{Q}\,, & 0\,, \\ \mathbf{Q}^{1\times 3}\,, & \mathbf{Q}\,, & 0\,, & \mathbf{Q}[\overline{\eta}, \overline{\xi}])\,, \end{array}$$

cf. Lemma 2.

We have $\gamma_{s,t} = 0$ for $(s,t) \in \{(1,2),(1,3),(2,1),(2,3),(3,1),(3,2),(3,4),(4,3)\}$.

Let

$$\begin{array}{rcl} \gamma_{1,1} : A_{1,1} & \xrightarrow{\sim} & \varepsilon_1 \, \mathrm{B}_{\mathbf{Q}} \, \varepsilon_1 \\ \begin{pmatrix} r_{1,1} & r_{1,2} & r_{1,3} \\ r_{2,1} & r_{2,2} & r_{2,3} \\ r_{3,1} & r_{3,2} & r_{3,3} \end{pmatrix} & \mapsto & \begin{array}{lllll} & r_{1,1}e & + r_{1,2}b_{e,g} & + r_{1,3}b_{e,h} \\ + & r_{2,1}b_{g,e} & + r_{2,2}g & + r_{2,3}b_{g,h} \\ & + r_{3,1}b_{h,e} & + r_{3,2}b_{h,g} & + r_{3,3}h \end{array} \end{array},$$

$$\begin{array}{rcl} \gamma_{1,4} : A_{1,4} & \xrightarrow{\sim} & \varepsilon_1 \, \mathrm{B}_{\mathbf{Q}} \, \varepsilon_4 \\ \begin{pmatrix} u_1 \\ u_2 \\ u_3 \end{pmatrix} & \mapsto & \begin{array}{l} u_1 b_{e,\varepsilon_4} \\ + u_2 b_{g,\varepsilon_4} \\ + u_3 b_{h,\varepsilon_4} \end{array} \end{array},$$

$$\begin{array}{rcl} \gamma_{2,2} : A_{2,2} & \xrightarrow{\sim} & \varepsilon_2 \, \mathrm{B}_{\mathbf{Q}} \, \varepsilon_2 \\ u & \mapsto & u\varepsilon_2 \end{array}, \qquad \begin{array}{rcl} \gamma_{2,4} : A_{2,4} & \xrightarrow{\sim} & \varepsilon_2 \, \mathrm{B}_{\mathbf{Q}} \, \varepsilon_4 \\ u & \mapsto & u b_{\varepsilon_2,\varepsilon_4} \end{array},$$

$$\begin{array}{rcl} \gamma_{3,3} : A_{3,3} & \xrightarrow{\sim} & \varepsilon_3 \, \mathrm{B}_{\mathbf{Q}} \, \varepsilon_3 \\ u & \mapsto & u\varepsilon_3 \end{array},$$

$$\begin{array}{rcl} \gamma_{4,1} : A_{4,1} & \xrightarrow{\sim} & \varepsilon_4 \, \mathrm{B}_{\mathbf{Q}} \, \varepsilon_1 \\ \begin{pmatrix} v_1 & v_2 & v_3 \end{pmatrix} & \mapsto & v_1 b_{\varepsilon_4,e} + v_2 b_{\varepsilon_4,g} + v_3 b_{\varepsilon_4,h} \end{array},$$

$$\begin{array}{rcl} \gamma_{4,2} : A_{4,2} & \xrightarrow{\sim} & \varepsilon_4 \, \mathrm{B}_{\mathbf{Q}} \, \varepsilon_2 \\ u & \mapsto & u b_{\varepsilon_4,\varepsilon_2} \end{array},$$

$$\begin{array}{rcl} \gamma_{4,4} \overset{\text{L.2}}{:=} \mu : A_{4,4} & \xrightarrow{\sim} & \varepsilon_4 \, \mathrm{B}_{\mathbf{Q}} \, \varepsilon_4 \\ a + b\overline{\eta} + c\overline{\xi} & \mapsto & a\varepsilon_4 + b b'_{\varepsilon_4,\varepsilon_4} + c b''_{\varepsilon_4,\varepsilon_4}. \end{array}$$

Let $\beta : \mathrm{B}_{\mathbf{Q}} \times \mathrm{B}_{\mathbf{Q}} \to \mathrm{B}_{\mathbf{Q}}$ be the multiplication map on $\mathrm{B}_{\mathbf{Q}}$. Write

$$\beta_{i,j,k} := \beta|^{\varepsilon_i \, \mathrm{B}_{\mathbf{Q}} \, \varepsilon_k}_{\varepsilon_i \, \mathrm{B}_{\mathbf{Q}} \, \varepsilon_j \times \varepsilon_j \, \mathrm{B}_{\mathbf{Q}} \, \varepsilon_k} : \varepsilon_i \, \mathrm{B}_{\mathbf{Q}} \, \varepsilon_j \times \varepsilon_j \, \mathrm{B}_{\mathbf{Q}} \, \varepsilon_k \to \varepsilon_i \, \mathrm{B}_{\mathbf{Q}} \, \varepsilon_k \ .$$

Now, we construct $\mathbf{Q}$-bilinear multiplication maps $\alpha_{i,j,k}$ for $i,j,k \in [1,4]$ such that the following quadrangle of maps commutes.

$$\begin{array}{ccc} A_{i,j} \times A_{j,k} & \xrightarrow{\alpha_{i,j,k}} & A_{i,k} \\ \downarrow{\scriptstyle \gamma_{i,j} \times \gamma_{j,k}} & & \downarrow{\scriptstyle \gamma_{i,k}} \\ \varepsilon_i \, \mathrm{B}_{\mathbf{Q}} \, \varepsilon_j \times \varepsilon_j \, \mathrm{B}_{\mathbf{Q}} \, \varepsilon_k & \xrightarrow{\beta_{i,j,k}} & \varepsilon_i \, \mathrm{B}_{\mathbf{Q}} \, \varepsilon_k \end{array}$$

I.e. we set $\alpha_{i,j,k} := \gamma_{i,k}^{-1} \circ \beta_{i,j,k} \circ (\gamma_{i,j} \times \gamma_{j,k})$. This leads to

- $\alpha_{i,j,k} = 0$ if (i,j), (j,k) or (i,k) is contained in $\{(1,2),(1,3),(2,1),(2,3),(3,1),(3,2),(3,4),(4,3)\}$
- $\alpha_{1,1,1} : A_{1,1} \times A_{1,1} \to A_{1,1}$, $(X,Y) \mapsto XY$
- $\alpha_{1,1,4} : A_{1,1} \times A_{1,4} \to A_{1,4}$, $(X,u) \mapsto Xu$
- $\alpha_{1,4,1} = 0$
- $\alpha_{1,4,4} : A_{1,4} \times A_{4,4} \to A_{1,4}$, $(u, a + b\overline{\eta} + c\overline{\xi}) \mapsto ua$
- $\alpha_{2,2,2} : A_{2,2} \times A_{2,2} \to A_{2,2}$, $(u,v) \mapsto uv$
- $\alpha_{2,2,4} : A_{2,2} \times A_{2,4} \to A_{2,4}$, $(u,v) \mapsto uv$
- $\alpha_{2,4,2} = 0$
- $\alpha_{2,4,4} : A_{2,4} \times A_{4,4} \to A_{2,4}$, $(u, a + b\overline{\eta} + c\overline{\xi}) \mapsto ua$
- $\alpha_{3,3,3} : A_{3,3} \times A_{3,3} \to A_{3,3}$, $(u,v) \mapsto uv$
- $\alpha_{4,1,1} : A_{4,1} \times A_{1,1} \to A_{4,1}$, $(v,X) \mapsto vX$
- $\alpha_{4,1,4} : A_{4,1} \times A_{1,4} \to A_{4,4}$, $(v,u) \mapsto vu\overline{\eta}$
- $\alpha_{4,2,2} : A_{4,2} \times A_{2,2} \to A_{4,2}$, $(u,v) \mapsto uv$
- $\alpha_{4,2,4} : A_{4,2} \times A_{2,4} \to A_{4,4}$, $(u,v) \mapsto uv(\overline{\xi} - 12\overline{\eta})$
- $\alpha_{4,4,1} : A_{4,4} \times A_{4,1} \to A_{4,1}$, $(a + b\overline{\eta} + c\overline{\xi}, v) \mapsto av$
- $\alpha_{4,4,2} : A_{4,4} \times A_{4,2} \to A_{4,2}$, $(a + b\overline{\eta} + c\overline{\xi}, v) \mapsto av$
- $\alpha_{4,4,4} : A_{4,4} \times A_{4,4} \to A_{4,4}$, $(a + b\overline{\eta} + c\overline{\xi}, \tilde{a} + \tilde{b}\overline{\eta} + \tilde{c}\overline{\xi}) \mapsto (a + b\overline{\eta} + c\overline{\xi}) \cdot (\tilde{a} + \tilde{b}\overline{\eta} + \tilde{c}\overline{\xi})$ where $a, b, c, \tilde{a}, \tilde{b}, \tilde{c} \in \mathbf{Q}$

For convenience, we fix a notation similar to matrices and matrix multiplication.

Notation 4. *Suppose given $r \in \mathbf{Z}_{\geq 0}$. Suppose given R-modules $M_{i,j}$ for $i,j \in [1,r]$. We write*

$$\bigoplus_{i,j\in[1,r]} M_{i,j} =: \begin{bmatrix} M_{1,1} & M_{1,2} & \dots & M_{1,r} \\ M_{2,1} & M_{2,2} & \dots & M_{2,r} \\ \vdots & \vdots & \dots & \vdots \\ M_{r,1} & M_{r,2} & \dots & M_{r,r} \end{bmatrix} .$$

Accordingly, elements of this direct sum are written as matrices with entries in the respective summands, i.e. in the form $[m_{i,j}]_{i,j}$ with $m_{i,j} \in M_{i,j}$ for $i,j \in [1,r]$.

Proposition 5. *Let*

$$A := \bigoplus_{i,j\in[1,4]} A_{i,j} = \begin{bmatrix} A_{1,1} & A_{1,2} & A_{1,3} & A_{1,4} \\ A_{2,1} & A_{2,2} & A_{2,3} & A_{2,4} \\ A_{3,1} & A_{3,2} & A_{3,3} & A_{3,4} \\ A_{4,1} & A_{4,2} & A_{4,3} & A_{4,4} \end{bmatrix} = \begin{bmatrix} \mathbf{Q}^{3\times 3} & 0 & 0 & \mathbf{Q}^{3\times 1} \\ 0 & \mathbf{Q} & 0 & \mathbf{Q} \\ 0 & 0 & \mathbf{Q} & 0 \\ \mathbf{Q}^{1\times 3} & \mathbf{Q} & 0 & \mathbf{Q}[\overline{\eta},\overline{\xi}] \end{bmatrix} .$$

Define the multiplication

$$\begin{array}{ccccc} A & \times & A & \to & A \\ ([a_{i,j}]_{i,j} & , & [a'_{s,t}]_{s,t}) & \mapsto & [\sum\limits_{r\in[1,4]} \alpha_{i,r,j}(a_{i,r}, a'_{r,j})]_{i,j} \end{array} .$$

We obtain a $\mathbf{Q}$-algebra isomorphism

$$\begin{array}{ccc} A & \xrightarrow{\sim\ \gamma} & \mathrm{B}_{\mathbf{Q}}(\mathrm{S}_3, \mathrm{S}_3) \\ [a_{i,j}]_{i,j\in[1,4]} & \mapsto & \sum\limits_{i,j\in[1,4]} \gamma_{i,j}(a_{i,j}) \end{array} .$$

4.2. $\mathrm{B}_{\mathbf{Q}}(\mathrm{S}_3, \mathrm{S}_3)$ **as path algebra modulo relations.** We aim to write

$$\mathrm{B}_{\mathbf{Q}} = \mathrm{B}_{\mathbf{Q}}(\mathrm{S}_3, \mathrm{S}_3) \cong A ,$$

up to Morita equivalence, as a path algebra modulo relations.

We denote by $\mathrm{e}_{i,j} \in A_{1,1} = \mathbf{Q}^{3\times 3}$ the elements that have a single non-zero entry 1 at position (i,j). We have $a_{1,1} := \gamma^{-1}(e) = \mathrm{e}_{1,1} \in \mathbf{Q}^{3\times 3} \subseteq A$, $\gamma^{-1}(g) = \mathrm{e}_{2,2} \in \mathbf{Q}^{3\times 3} \subseteq A$, $\gamma^{-1}(e) = \mathrm{e}_{3,3} \in \mathbf{Q}^{3\times 3} \subseteq A$ and $a_{k,k} := \gamma^{-1}(\varepsilon_k)$ for $k \in [2,4]$, cf. Proposition 5.

We have $Aa_{1,1} \cong A\,\mathrm{e}_{2,2}$ as A-modules, using multiplication with $\mathrm{e}_{1,2}$ from the right from $Aa_{1,1}$ to $A\,\mathrm{e}_{2,2}$ and multiplication with $\mathrm{e}_{2,1}$ from the right from $A\,\mathrm{e}_{2,2}$ to $Aa_{1,1}$. Note that $\mathrm{e}_{1,2}\,\mathrm{e}_{2,1} = a_{1,1}$ and $\mathrm{e}_{2,1}\,\mathrm{e}_{1,2} = \mathrm{e}_{2,2}$. Similarly $Aa_{1,1} \cong A\,\mathrm{e}_{3,3}$.

Therefore, A is Morita equivalent to

$$A' := (\sum_{i\in[1,4]} a_{i,i})A(\sum_{i\in[1,4]} a_{i,i}) = \bigoplus_{i,j\in[1,4]} a_{i,i}Aa_{j,j} = \bigoplus_{i,j\in[1,4]} a_{i,i}A_{i,j}a_{j,j}\ .$$

Write $A'_{i,j} := a_{i,i}A_{i,j}a_{j,j} = A_{i,j}$ for $i,j \in [2,4]$.

Identify $A'_{1,1} := \mathbf{Q} = \begin{pmatrix} \mathbf{Q} & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix} = a_{1,1}A_{1,1}a_{1,1} \subseteq A_{1,1} = \mathbf{Q}^{3\times 3}$.

Identify $A'_{1,4} := \mathbf{Q} = \begin{pmatrix} \mathbf{Q} \\ 0 \\ 0 \end{pmatrix} = a_{1,1}A_{1,4}a_{4,4} \subseteq A_{1,4} = \mathbf{Q}^{3\times 1}$.

Identify $A'_{4,1} := \mathbf{Q} = \begin{pmatrix} \mathbf{Q} & 0 & 0 \end{pmatrix} = a_{4,4}A_{4,1}a_{1,1} \subseteq A_{4,1} = \mathbf{Q}^{1\times 3}$. Let $A'_{1,j} := 0$ and $A'_{j,1} := 0$ for $j \in [2,3]$.

We have the $\mathbf{Q}$-linear basis of A'

$$a_{1,1} = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{bmatrix} \quad a_{2,2} = \begin{bmatrix} 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{bmatrix} \quad a_{3,3} = \begin{bmatrix} 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 \end{bmatrix}$$

$$a_{4,4} = \begin{bmatrix} 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix} \quad a_{1,4} := \begin{bmatrix} 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{bmatrix} \quad a_{4,1} := \begin{bmatrix} 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 \end{bmatrix}$$

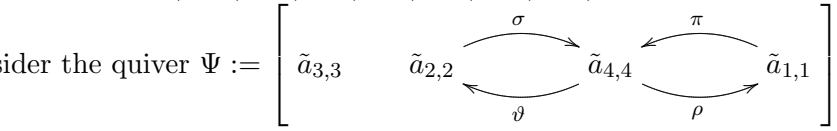
$$a_{2,4} := \begin{bmatrix} 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{bmatrix} \quad a_{4,2} := \begin{bmatrix} 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \end{bmatrix} \quad a'_{4,4} := \begin{bmatrix} 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & \overline{\eta} \end{bmatrix}$$

$$a''_{4,4} := \begin{bmatrix} 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & \overline{\xi} \end{bmatrix}$$

We have the following multiplication table for the basis elements.

$(\cdot)$	$a_{1,1}$	$a_{1,4}$	$a_{2,2}$	$a_{2,4}$	$a_{3,3}$	$a_{4,1}$	$a_{4,2}$	$a_{4,4}$	$a'_{4,4}$	$a''_{4,4}$
$a_{1,1}$	$a_{1,1}$	$a_{1,4}$	0	0	0	0	0	0	0	0
$a_{1,4}$	0	0	0	0	0	0	0	$a_{1,4}$	0	0
$a_{2,2}$	0	0	$a_{2,2}$	$a_{2,4}$	0	0	0	0	0	0
$a_{2,4}$	0	0	0	0	0	0	0	$a_{2,4}$	0	0
$a_{3,3}$	0	0	0	0	$a_{3,3}$	0	0	0	0	0
$a_{4,1}$	$a_{4,1}$	$a'_{4,4}$	0	0	0	0	0	0	0	0
$a_{4,2}$	0	0	$a_{4,2}$	$a''_{4,4} - 12a'_{4,4}$	0	0	0	0	0	0
$a_{4,4}$	0	0	0	0	0	$a_{4,1}$	$a_{4,2}$	$a_{4,4}$	$a'_{4,4}$	$a''_{4,4}$
$a'_{4,4}$	0	0	0	0	0	0	0	$a'_{4,4}$	0	0
$a''_{4,4}$	0	0	0	0	0	0	0	$a''_{4,4}$	0	0

We have $a'_{4,4} = a_{4,1} \cdot a_{1,4}$ and $a''_{4,4} = a_{4,2} \cdot a_{2,4} + 12a_{4,1} \cdot a_{1,4}$. Hence, as a $\mathbf{Q}$-algebra A' is generated by $a_{1,1}, a_{2,2}, a_{3,3}, a_{4,4}, a_{1,4}, a_{4,1}, a_{2,4}, a_{4,2}$.

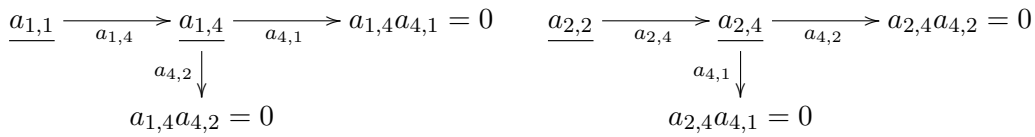
Consider the quiver $\Psi :=$ 

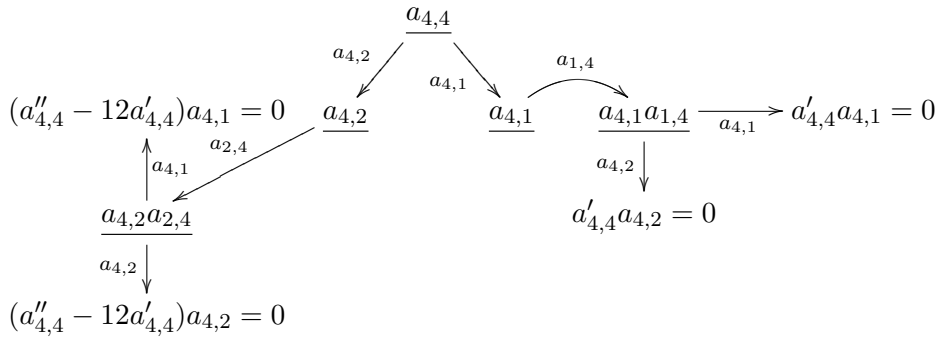
.

We have a surjective $\mathbf{Q}$-algebra morphism $\varphi : \mathbf{Q}\Psi \to A'$ by sending

$$\begin{array}{cccccccccccc} \tilde{a}_{1,1} & \mapsto & a_{1,1} & , & \tilde{a}_{2,2} & \mapsto & a_{2,2} & , & \tilde{a}_{3,3} & \mapsto & a_{3,3} & , & \tilde{a}_{4,4} & \mapsto & a_{4,4} & , \\ \rho & \mapsto & a_{4,1} & , & \pi & \mapsto & a_{1,4} & , & \vartheta & \mapsto & a_{4,2} & , & \sigma & \mapsto & a_{2,4} & . \end{array}$$

We establish the following multiplication trees, where we underline the elements that are not in a $\mathbf{Q}$-linear relation with previously underlined elements.





The multiplication tree of the idempotent $a_{3,3}$ consists only of the element $a_{3,3}$.
So the kernel of φ contains the elements:

$$\begin{array}{cccccccc} \pi\rho & , & \sigma\vartheta & , & \rho\pi\rho & , & \vartheta\sigma\rho & , \\ \pi\vartheta & , & \sigma\rho & , & \rho\pi\vartheta & , & \vartheta\sigma\vartheta & . \end{array}$$

Let I be the ideal in $\mathbf{Q}\Psi$ generated by those elements. So $I \subseteq \ker(\varphi)$. Therefore, φ induces a surjective $\mathbf{Q}$-algebra morphism from $\mathbf{Q}\Psi/I$ to A' .

Note that $\mathbf{Q}\Psi/I$ is $\mathbf{Q}$-linearly generated by

$$\mathcal{N} := \{\tilde{a}_{3,3}+I, \tilde{a}_{2,2}+I, \tilde{a}_{4,4}+I, \tilde{a}_{1,1}+I, \sigma+I, \pi+I, \vartheta+I, \rho+I, \vartheta\sigma+I, \rho\pi+I\},$$

cf. the underlined elements above. To see that, note that a product ξ of k generators may be written as a product in $\mathcal{N}$ of k' generators and a product of k'' generators, where $k = k'+k''$ and where k' is chosen maximal. We call k'' the excess of ξ. If $k'' \geq 1$ then, using the trees above, we may write ξ as an $\mathbf{Q}$-linear combination of products of generators that have excess $\leq k''-1$. In the present case, we even have $\xi = 0$.

Moreover, note that $|\mathcal{N}| = 10 = \dim_{\mathbf{Q}}(A')$.

Since we have a surjective $\mathbf{Q}$-algebra morphism from $\mathbf{Q}\Psi/I$ to A', this dimension argument shows this morphism to be bijective. In particular, $I = \ker(\varphi)$.

We may reduce this list to obtain $\ker(\varphi) = (\pi\rho, \sigma\vartheta, \pi\vartheta, \sigma\rho)$.

So we obtain the

Proposition 6. *Recall that $I = (\pi\rho, \sigma\vartheta, \pi\vartheta, \sigma\rho)$. We have the isomorphism of $\mathbf{Q}$-algebras*

$$A' \xrightarrow{\sim} \mathbf{Q}\left[\ \tilde{a}_{3,3} \qquad \tilde{a}_{2,2} \underset{\vartheta}{\overset{\sigma}{\rightleftarrows}} \tilde{a}_{4,4} \underset{\rho}{\overset{\pi}{\rightleftarrows}} \tilde{a}_{1,1}\ \right]/I = \mathbf{Q}\Psi/I$$

$$\begin{aligned}
a_{1,1} &\mapsto \tilde{a}_{1,1}+I\\
a_{2,2} &\mapsto \tilde{a}_{2,2}+I\\
a_{3,3} &\mapsto \tilde{a}_{3,3}+I\\
a_{4,4} &\mapsto \tilde{a}_{4,4}+I\\
a_{4,1} &\mapsto \rho+I\\
a_{1,4} &\mapsto \pi+I\\
a_{4,2} &\mapsto \vartheta+I\\
a_{2,4} &\mapsto \sigma+I\ .
\end{aligned}$$

In particular, $\mathbf{Q}\Psi/I$ is Morita equivalent to $A \cong \mathrm{B}_{\mathbf{Q}}(\mathrm{S}_3, \mathrm{S}_3)$.

5. The double Burnside R-algebra $\mathrm{B}_R(\mathrm{S}_3, \mathrm{S}_3)$ for $R \in \{\mathbf{Z}, \mathbf{Z}_{(2)}, \mathbf{F}_2, \mathbf{Z}_{(3)}, \mathbf{F}_3\}$

5.1. $\mathrm{B}_{\mathbf{Z}}(\mathrm{S}_3, \mathrm{S}_3)$ **via congruences.** Recall that

$$A = \bigoplus_{i,j\in[1,4]} A_{i,j} \xrightarrow[\gamma]{\sim} \mathrm{B}_{\mathbf{Q}}\ ,$$

cf. Proposition 5. In the $\mathbf{Q}$-algebra A, we define the $\mathbf{Z}$-order

$$A_{\mathbf{Z}} := \begin{bmatrix} A_{\mathbf{Z},1,1} & A_{\mathbf{Z},1,2} & A_{\mathbf{Z},1,3} & A_{\mathbf{Z},1,4}\\ A_{\mathbf{Z},2,1} & A_{\mathbf{Z},2,2} & A_{\mathbf{Z},2,3} & A_{\mathbf{Z},2,4}\\ A_{\mathbf{Z},3,1} & A_{\mathbf{Z},3,2} & A_{\mathbf{Z},3,3} & A_{\mathbf{Z},3,4}\\ A_{\mathbf{Z},4,1} & A_{\mathbf{Z},4,2} & A_{\mathbf{Z},4,3} & A_{\mathbf{Z},4,4} \end{bmatrix} := \begin{bmatrix} \mathbf{Z}^{3\times 3} & 0 & 0 & \mathbf{Z}^{3\times 1}\\ 0 & \mathbf{Z} & 0 & \mathbf{Z}\\ 0 & 0 & \mathbf{Z} & 0\\ \mathbf{Z}^{1\times 3} & \mathbf{Z} & 0 & \mathbf{Z}[\overline{\eta}, \overline{\xi}] \end{bmatrix} \subseteq A.$$

In fact, $A_{\mathbf{Z}}$ is a subring of A, as $\alpha_{i,j,k}(A_{\mathbf{Z},i,j} \times A_{\mathbf{Z},j,k}) \subseteq A_{\mathbf{Z},i,k}$ for $i,j,k \in [1,4]$.

Remark 7. As $A \cong \mathrm{B}_{\mathbf{Q}}$ is not semisimple, there are no maximal $\mathbf{Z}$-orders in A, [8, §10]. So $A_{\mathbf{Z}}$ is not a canonical choice of a $\mathbf{Z}$-order in A, but it nonetheless enables us to describe Λ inside $A_{\mathbf{Z}}$ via congruences.

Consider the following elements of $\mathrm{U}(A)$.

$$x_1 := \begin{bmatrix} 0 & -2 & 0 & 0 & 0 & 0 \\ 6 & 6 & -4 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 \end{bmatrix}, \; x_2 := \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 7 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 \end{bmatrix}, \; x_3 := \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 1 \\ 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 6 & 0 & 0 & 1 \end{bmatrix}.$$

We define the injective ring morphism $\delta : \mathrm{B}_{\mathbf{Z}} \to A,\ y \mapsto x_3^{-1} \cdot x_2^{-1} \cdot x_1^{-1} \cdot \gamma^{-1}(y) \cdot x_1 \cdot x_2 \cdot x_3$. The conjugating element x_1 was constructed such that the its image lies in $A_{\mathbf{Z}}$. The elements $x_2,\ x_3$ serve the purpose of simplifying the congruences of $\delta(\mathrm{B}_{\mathbf{Z}})$.

Theorem 8. *The image $\delta(\mathrm{B}_{\mathbf{Z}})$ in $A_{\mathbf{Z}}$ is given by*

$$\Lambda := \delta(\mathrm{B}_{\mathbf{Z}}) = \left\{ \begin{bmatrix} s_{1,1} & s_{1,2} & s_{1,3} & 0 & 0 & t_1 \\ s_{2,1} & s_{2,2} & s_{2,3} & 0 & 0 & t_2 \\ s_{3,1} & s_{3,2} & s_{3,3} & 0 & 0 & t_3 \\ 0 & 0 & 0 & u & 0 & v \\ 0 & 0 & 0 & 0 & w & 0 \\ x_1 & x_2 & x_3 & y & 0 & z_1 + z_2\overline{\eta} + z_3\overline{\xi} \end{bmatrix} \in A_{\mathbf{Z}} : \begin{array}{rl} 2w - 2z_1 \equiv_8 z_2 \equiv_4 z_3 \equiv_4 0 & \\ x_1 \equiv_4 0 & \\ x_2 \equiv_4 0 & \\ x_3 \equiv_4 0 & \\ y \equiv_2 0 & \\ t_1 \equiv_2 0 & \\ t_2 \equiv_2 0 & \\ t_3 \equiv_2 0 & \\ v \equiv_2 0 & \\ & \\ x_1 \equiv_3 0 & \\ x_2 \equiv_3 0 & \\ x_3 \equiv_3 0 & \\ z_2 \equiv_3 0 & \end{array} \right\}.$$

In particular, we have $\mathrm{B}_{\mathbf{Z}} = \mathrm{B}_{\mathbf{Z}}(\mathrm{S}_3, \mathrm{S}_3) \cong \Lambda$ as rings.

More symbolically written, we have

$$\Lambda = \begin{bmatrix} \mathbf{Z} & \mathbf{Z} & \mathbf{Z} & 0 & 0 & (2) \\ \mathbf{Z} & \mathbf{Z} & \mathbf{Z} & 0 & 0 & (2) \\ \mathbf{Z} & \mathbf{Z} & \mathbf{Z} & 0 & 0 & (2) \\ 0 & 0 & 0 & \mathbf{Z} & 0 & (2) \\ 0 & 0 & 0 & 0 & \mathbf{Z} & 0 \\ (12) & (12) & (12) & (2) & 0 & \mathbf{Z} \end{bmatrix} \begin{matrix} \\ \\ \\ \\ \overset{-2}{\curvearrowright} \\ \overset{2}{\curvearrowright} \\ \overset{1}{\curvearrowright} \end{matrix} \begin{matrix} \\ \\ \\ \\ \textcircled{8} \\ \\ \end{matrix} \begin{matrix} \\ \\ \\ \\ \\ +(12)\overline{\eta} \\ +(4)\overline{\xi} \end{matrix}.$$

Proof. We identify $\mathbf{Z}^{22\times 1}$ and $A_{\mathbf{Z}}$ along the isomorphism

$$\begin{pmatrix} s_{1,1}, s_{2,1}, s_{3,1}, s_{1,2}, s_{2,2}, s_{3,2}, s_{1,3}, s_{2,3}, s_{3,3}, \\ x_1, x_2, x_3, u, y, w, t_1, t_2, t_3, v, z_1, z_2, z_3 \end{pmatrix}^{\mathrm{t}} \mapsto \begin{bmatrix} s_{1,1} & s_{1,2} & s_{1,3} & 0 & 0 & t_1 \\ s_{2,1} & s_{2,2} & s_{2,3} & 0 & 0 & t_2 \\ s_{3,1} & s_{3,2} & s_{3,3} & 0 & 0 & t_3 \\ 0 & 0 & 0 & u & 0 & v \\ 0 & 0 & 0 & 0 & w & 0 \\ x_1 & x_2 & x_3 & y & 0 & z_1 + z_2\overline{\eta} + z_3\overline{\xi} \end{bmatrix}.$$

Let M be the representation matrix of δ, with respect to the bases $\tilde{\mathcal{H}} = (H_{0,0}, H_{0,1}, H_{1,0}, H_1^{\Delta}, H_{0,4}, H_{4,0}, H_4^{\Delta}, H_{1,1}, H_{0,5}, H_{5,0}, H_7, H_{1,4}, H_{4,1}, H_6, H_5^{\Delta}, H_{4,4}, H_{5,1}, H_{1,5}, H_{5,4}, H_{4,5}, H_8, H_{5,5})$ of $\mathrm{B}_{\mathbf{Z}}$ and the standard basis of $A_{\mathbf{Z}}$.

We obtain that $M =$

$$\begin{pmatrix}
0 & 0 & 15 & -3 & 0 & 20 & 8 & 6 & 0 & 25 & 7 & 9 & 8 & -3 & 1 & 12 & 10 & 3 & 15 & 4 & 3 & 5 \\
0 & 0 & -18 & 0 & 0 & -24 & 0 & -9 & 0 & -30 & -12 & -6 & -12 & 0 & 0 & -8 & -15 & -3 & -10 & -4 & -4 & -5 \\
0 & 0 & 126 & -6 & 0 & 168 & 12 & 60 & 0 & 210 & 78 & 48 & 80 & -6 & 0 & 64 & 100 & 21 & 80 & 28 & 26 & 35 \\
-5 & -2 & -60 & 9 & -3 & -55 & -23 & -24 & -1 & -85 & -16 & -36 & -22 & 10 & 0 & -33 & -34 & -12 & -51 & -11 & -5 & -17 \\
6 & 3 & 72 & 3 & 2 & 66 & 2 & 36 & 1 & 102 & 33 & 24 & 33 & 1 & 1 & 22 & 51 & 12 & 34 & 11 & 11 & 17 \\
-42 & -20 & -504 & 2 & -16 & -462 & -46 & -240 & -7 & -714 & -208 & -192 & -220 & 15 & 0 & -176 & -340 & -84 & -272 & -77 & -65 & -119 \\
0 & 0 & -10 & 2 & 0 & -10 & -4 & -4 & 0 & -15 & -3 & -6 & -4 & 2 & 0 & -6 & -6 & -2 & -9 & -2 & -1 & -3 \\
0 & 0 & 12 & 0 & 0 & 12 & 0 & 6 & 0 & 18 & 6 & 4 & 6 & 0 & 0 & 4 & 9 & 2 & 6 & 2 & 2 & 3 \\
0 & 0 & -84 & 4 & 0 & -84 & -6 & -40 & 0 & -126 & -38 & -32 & -40 & 4 & 1 & -32 & -60 & -14 & -48 & -14 & -12 & -21 \\
0 & 0 & -756 & 36 & 0 & -1008 & -72 & -360 & 0 & -1260 & -468 & -288 & -480 & 72 & 0 & -384 & -600 & -108 & -480 & -144 & -120 & -180 \\
252 & 120 & 3024 & -12 & 96 & 2772 & 276 & 1440 & 36 & 4284 & 1248 & 1152 & 1320 & -228 & 0 & 1056 & 2040 & 432 & 1632 & 396 & 252 & 612 \\
0 & 0 & 504 & -24 & 0 & 504 & 36 & 240 & 0 & 756 & 228 & 192 & 240 & -48 & 0 & 192 & 360 & 72 & 288 & 72 & 48 & 108 \\
0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & -2 & 0 & 0 & 0 & 0 & 0 & 0 & -2 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 2 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & -10 & 2 & 0 & -10 & -4 & -4 & 0 & -10 & -4 & -6 & -4 & 2 & 0 & -6 & -4 & -2 & -6 & -2 & -2 & -2 \\
0 & 0 & 12 & 0 & 0 & 12 & 0 & 6 & 0 & 12 & 6 & 4 & 6 & 0 & 0 & 4 & 6 & 2 & 4 & 2 & 2 & 2 \\
0 & 0 & -84 & 4 & 0 & -84 & -6 & -40 & 0 & -84 & -40 & -32 & -40 & 4 & 0 & -32 & -40 & -14 & -32 & -14 & -14 & -14 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & -2 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & -2 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 504 & -24 & 0 & 504 & 36 & 240 & 0 & 504 & 240 & 192 & 240 & -48 & 0 & 192 & 240 & 72 & 192 & 72 & 24 & 72 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 4 & 0
\end{pmatrix}.$$

Let

$$\lambda := \begin{bmatrix}
s_{1,1} & s_{1,2} & s_{1,3} & 0 & 0 & t_1 \\
s_{2,1} & s_{2,2} & s_{2,3} & 0 & 0 & t_2 \\
s_{3,1} & s_{3,2} & s_{3,3} & 0 & 0 & t_3 \\
0 & 0 & 0 & u & 0 & v \\
0 & 0 & 0 & 0 & w & 0 \\
x_1 & x_2 & x_3 & y & 0 & z_1 + z_2\overline{\eta} + z_3\overline{\xi}
\end{bmatrix} \in A_{\mathbf{Z}},$$

identified with $\lambda \in \mathbf{Z}^{22\times 1}$.

We have $\lambda \in \Lambda$
$\Leftrightarrow \exists\, q \in \mathbf{Z}^{22\times 1}$ such that $\lambda = Mq$
$\Leftrightarrow \exists\, q \in \mathbf{Z}^{22\times 1}$ such that $M^{-1} \cdot \lambda = q$
$\Leftrightarrow 24M^{-1} \cdot \lambda \in 24\mathbf{Z}^{22\times 1}$
and this is equivalent to

$$\begin{pmatrix}
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 2 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 2 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 2 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 12 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 6 & 0 & 0 & 0 & 18 & 1 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 12 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 12 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 12 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 12 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 2 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 6
\end{pmatrix}
\begin{pmatrix}
s_{1,1} \\ s_{2,1} \\ s_{3,1} \\ \vdots \\ s_{3,3} \\ x_1 \\ x_2 \\ x_3 \\ u \\ y \\ w \\ t_1 \\ t_2 \\ t_3 \\ v \\ z_1 \\ z_2 \\ z_3
\end{pmatrix} \in 24\mathbf{Z}^{11\times 1}$$

and hence equivalent to

$$\left\{\begin{array}{ll} 2w-2z_1 \equiv_8 z_2 \equiv_4 z_3 \equiv_4 0 \\ x_1 \equiv_4 0 \\ x_2 \equiv_4 0 \\ x_3 \equiv_4 0 \\ y \equiv_2 0 \\ t_1 \equiv_2 0 \\ t_2 \equiv_2 0 \\ t_3 \equiv_2 0 \\ v \equiv_2 0 \\ \\ x_1 \equiv_3 0 \\ x_2 \equiv_3 0 \\ x_3 \equiv_3 0 \\ z_2 \equiv_3 0 \end{array}\right\}.$$

□

5.2. **Localisation at 2: $\mathrm{B}_{\mathbf{Z}_{(2)}}(\mathrm{S}_3,\mathrm{S}_3)$ via congruences.** Write $R := \mathbf{Z}_{(2)}$. In the $\mathbf{Q}$-algebra A, cf. Proposition 5, we have the R-order

$$A_R := \begin{bmatrix} A_{R,1,1} & A_{R,1,2} & A_{R,1,3} & A_{R,1,4} \\ A_{R,2,1} & A_{R,2,2} & A_{R,2,3} & A_{R,2,4} \\ A_{R,3,1} & A_{R,3,2} & A_{R,3,3} & A_{R,3,4} \\ A_{R,4,1} & A_{R,4,2} & A_{R,4,3} & A_{R,4,4} \end{bmatrix} := \begin{bmatrix} R^{3\times 3} & 0 & 0 & R^{3\times 1} \\ 0 & R & 0 & R \\ 0 & 0 & R & 0 \\ R^{1\times 3} & R & 0 & R[\overline{\eta},\overline{\xi}] \end{bmatrix} \subseteq A\ .$$

Corollary 9. *We have*

$$\Lambda_{(2)} = \left\{ \begin{bmatrix} s_{1,1} & s_{1,2} & s_{1,3} & 0 & 0 & t_1 \\ s_{2,1} & s_{2,2} & s_{2,3} & 0 & 0 & t_2 \\ s_{3,1} & s_{3,2} & s_{3,3} & 0 & 0 & t_3 \\ 0 & 0 & 0 & u & 0 & v \\ 0 & 0 & 0 & 0 & w & 0 \\ x_1 & x_2 & x_3 & y & 0 & z_1+z_2\overline{\eta}+z_3\overline{\xi} \end{bmatrix} \in A_R : \begin{array}{ll} 2w-2z_1 \equiv_8 z_2 \equiv_4 z_3 \equiv_4 0 \\ x_1 \equiv_4 0 \\ x_2 \equiv_4 0 \\ x_3 \equiv_4 0 \\ y \equiv_2 0 \\ t_1 \equiv_2 0 \\ t_2 \equiv_2 0 \\ t_3 \equiv_2 0 \\ v \equiv_2 0 \end{array} \right\} \subseteq A_R.$$

In particular, we have $\mathrm{B}_R = \mathrm{B}_R(\mathrm{S}_3,\mathrm{S}_3) \cong \Lambda_{(2)}$ *as R-algebras.*

More symbolically written, we have

$$\Lambda_{(2)} = \begin{bmatrix} R & R & R & 0 & 0 & (2) \\ R & R & R & 0 & 0 & (2) \\ R & R & R & 0 & 0 & (2) \\ 0 & 0 & 0 & R & 0 & (2) \\ 0 & 0 & 0 & 0 & R & 0 \\ (4) & (4) & (4) & (2) & 0 & R \end{bmatrix} \begin{array}{l} \\ \\ \\ \\ \overset{2}{\frown}\ \overset{-2}{\frown}\ \textcircled{8} \\ \overset{1}{\frown} \\ +(4)\overline{\eta} \quad +(4)\overline{\xi} \end{array}.$$

Remark 10. *We claim that* $1_{\Lambda_{(2)}} = e_1 + e_2 + e_3 + e_4 + e_5$ *is an orthogonal decomposition into primitive idempotents, where*

$$e_1 := \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \end{bmatrix}, \quad e_2 := \begin{bmatrix} 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \end{bmatrix}, \quad e_3 := \begin{bmatrix} 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \end{bmatrix},$$

$$e_4 := \begin{bmatrix} 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \end{bmatrix}, \quad e_5 := \begin{bmatrix} 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 \end{bmatrix}.$$

Proof. We have $\mathrm{e}_1 \Lambda_{(2)} \mathrm{e}_1 \cong R$, $\mathrm{e}_2 \Lambda_{(2)} \mathrm{e}_2 \cong R$, $\mathrm{e}_3 \Lambda_{(2)} \mathrm{e}_3 \cong R$ and $\mathrm{e}_4 \Lambda_{(2)} \mathrm{e}_4 \cong R$. So, it follows that $\mathrm{e}_1, \mathrm{e}_2, \mathrm{e}_3, \mathrm{e}_4$ are primitive.

As R-algebras, we have

$$\begin{aligned} \mathrm{e}_5 \Lambda_{(2)} \mathrm{e}_5 &\cong \left\{ \left(w,\ z_1 + z_2\overline{\eta} + z_3\overline{\xi} \right) \in R \times R[\overline{\eta}, \overline{\xi}] : 2w - 2z_1 \equiv_8 z_2 \equiv_4 z_3 \equiv_4 0 \right\} =: \Gamma \\ &\subseteq R \times R[\overline{\eta}, \overline{\xi}] \,. \end{aligned}$$

To show that e_5 is primitive, we show that Γ is local.

We have the R-linear basis (b_1, b_2, b_3, b_4) of Γ, where

$$\begin{aligned} b_1 &= \left(1,\ 1 \right), \quad b_2 = \left(0,\ 2 + 4\overline{\eta} \right), \\ b_3 &= \left(0,\ 8\overline{\eta} \right), \quad b_4 = \left(0,\ 4\overline{\xi} \right). \end{aligned}$$

We *claim* that the Jacobson radical of Γ is given by $J := {}_R\langle 2b_1, b_2, b_3, b_4 \rangle$, that $\Gamma/J \cong \mathbf{F}_2$ and that Γ is local.

In fact, the multiplication table for the basis elements is given by

$(\cdot)$	b_1	b_2	b_3	b_4
b_1	b_1	b_2	b_3	b_4
b_2	b_2	$2b_2 + b_3$	$2b_3$	$2b_4$
b_3	b_3	$2b_3$	0	0
b_4	b_4	$2b_4$	0	0

.

This shows that J is an ideal. Moreover, J is topologically nilpotent as

$$J^3 = {}_R\langle 8b_1, 4b_2, 2b_3, 4b_4 \rangle \subseteq 2\,\mathrm{e}_5 \Lambda_{(2)} \mathrm{e}_5 \,.$$

Since $\Gamma/J \cong \mathbf{F}_2$, the *claim* follows. □

5.3. $\mathrm{B}_{\mathbf{Z}_{(2)}}(\mathrm{S}_3,\mathrm{S}_3)$ **and** $\mathrm{B}_{\mathbf{F}_2}(\mathrm{S}_3,\mathrm{S}_3)$ **as path algebras modulo relations.** Write $R := \mathbf{Z}_{(2)}$. We aim to write $\Lambda_{(2)}$, up to Morita equivalence, as path algebra modulo relations. The R-algebra $\Lambda_{(2)}$ is Morita equivalent to $\Lambda'_{(2)} := (\mathrm{e}_3+\mathrm{e}_4+\mathrm{e}_5)\Lambda_{(2)}(\mathrm{e}_3+\mathrm{e}_4+\mathrm{e}_5)$ since $\Lambda_{(2)}\,\mathrm{e}_1 \cong \Lambda_{(2)}\,\mathrm{e}_2 \cong \Lambda_{(2)}\,\mathrm{e}_3$ using multiplication with elements of $\Lambda_{(2)}$ with a single nonzero entry 1 in the upper (3×3)-corner.

We have the R-linear basis of $\Lambda'_{(2)}$ consisting of

$$\mathrm{e}_3 := \begin{bmatrix} 0&0&0&0&0&0\\ 0&0&0&0&0&0\\ 0&0&1&0&0&0\\ 0&0&0&0&0&0\\ 0&0&0&0&0&0\\ 0&0&0&0&0&0 \end{bmatrix},\ \mathrm{e}_4 := \begin{bmatrix} 0&0&0&0&0&0\\ 0&0&0&0&0&0\\ 0&0&0&0&0&0\\ 0&0&0&1&0&0\\ 0&0&0&0&0&0\\ 0&0&0&0&0&0 \end{bmatrix},\ \mathrm{e}_5 := \begin{bmatrix} 0&0&0&0&0&0\\ 0&0&0&0&0&0\\ 0&0&0&0&0&0\\ 0&0&0&0&0&0\\ 0&0&0&0&1&0\\ 0&0&0&0&0&1 \end{bmatrix},$$

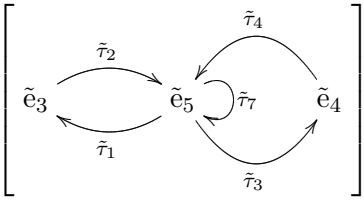
$$\tau_1 := \begin{bmatrix} 0&0&0&0&0&0\\ 0&0&0&0&0&0\\ 0&0&0&0&0&0\\ 0&0&0&0&0&0\\ 0&0&0&0&0&0\\ 0&0&4&0&0&0 \end{bmatrix},\ \tau_2 := \begin{bmatrix} 0&0&0&0&0&0\\ 0&0&0&0&0&0\\ 0&0&0&0&0&2\\ 0&0&0&0&0&0\\ 0&0&0&0&0&0\\ 0&0&0&0&0&0 \end{bmatrix},\ \tau_3 := \begin{bmatrix} 0&0&0&0&0&0\\ 0&0&0&0&0&0\\ 0&0&0&0&0&0\\ 0&0&0&0&0&0\\ 0&0&0&0&0&0\\ 0&0&0&2&0&0 \end{bmatrix},$$

$$\tau_4 := \begin{bmatrix} 0&0&0&0&0&0\\ 0&0&0&0&0&0\\ 0&0&0&0&0&0\\ 0&0&0&0&0&2\\ 0&0&0&0&0&0\\ 0&0&0&0&0&0 \end{bmatrix},\quad \tau_5 := \begin{bmatrix} 0&0&0&0&0&0\\ 0&0&0&0&0&0\\ 0&0&0&0&0&0\\ 0&0&0&0&0&0\\ 0&0&0&0&0&0\\ 0&0&0&0&0&8\overline{\eta} \end{bmatrix},$$

$$\tau_6 := \begin{bmatrix} 0&0&0&0&0&0\\ 0&0&0&0&0&0\\ 0&0&0&0&0&0\\ 0&0&0&0&0&0\\ 0&0&0&0&0&0\\ 0&0&0&0&0&4\overline{\xi} \end{bmatrix},\ \tau_7 := \begin{bmatrix} 0&0&0&0&0&0\\ 0&0&0&0&0&0\\ 0&0&0&0&0&0\\ 0&0&0&0&0&0\\ 0&0&0&0&0&0\\ 0&0&0&0&0&2+4\overline{\eta} \end{bmatrix}$$

We have $\tau_5 = \tau_1\tau_2$ and $\tau_6 = \tau_3\tau_4 + 6\tau_1\tau_2$. Hence, as an R-algebra $\Lambda'_{(2)}$ is generated by $\mathrm{e}_3, \mathrm{e}_4, \mathrm{e}_5, \tau_1, \tau_2, \tau_3, \tau_4, \tau_7$.

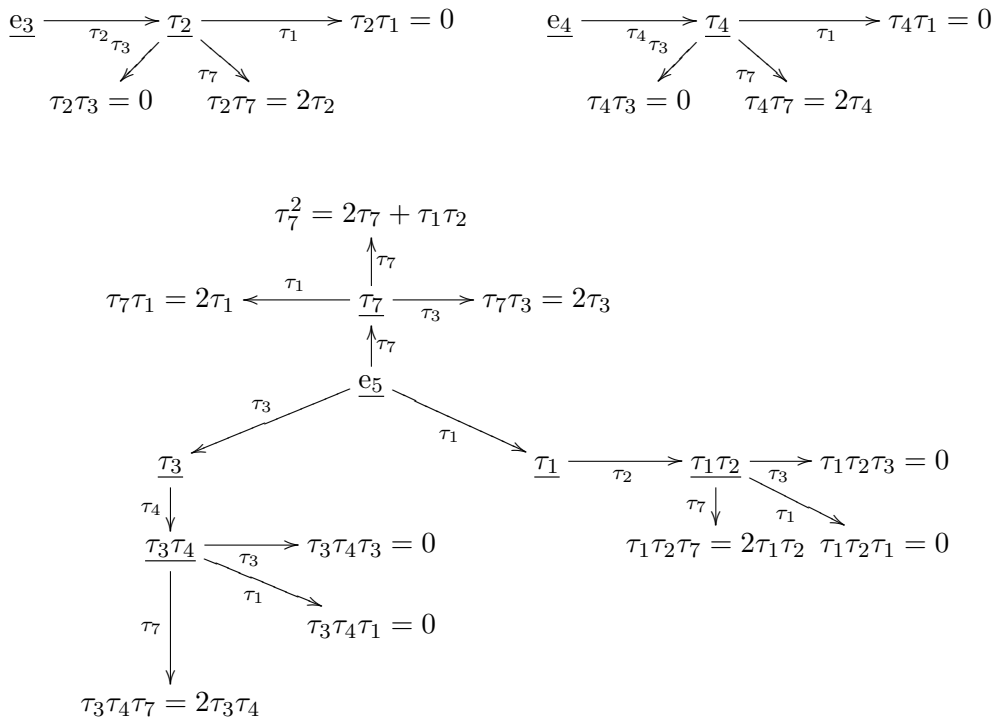
Consider the quiver $\Psi :=$



We have a surjective R-algebra morphism $\varphi : R\Psi \to \Lambda'_{(2)}$ by sending

$$\begin{array}{cccccccccccc} \tilde{\mathrm{e}}_3 & \mapsto & \mathrm{e}_3 & , & \tilde{\mathrm{e}}_4 & \mapsto & \mathrm{e}_4 & , & \tilde{\mathrm{e}}_5 & \mapsto & \mathrm{e}_5 & , & \tilde{\tau}_1 & \mapsto & \tau_1 & , \\ \tilde{\tau}_2 & \mapsto & \tau_2 & , & \tilde{\tau}_3 & \mapsto & \tau_3 & , & \tilde{\tau}_4 & \mapsto & \tau_4 & , & \tilde{\tau}_7 & \mapsto & \tau_7 & . \end{array}$$

We establish the following multiplication trees, where we underline the elements that are not in an R-linear relation with previous elements.



So, the kernel of φ contains the elements:

$$\begin{array}{ccccccccc}
\tilde\tau_2\tilde\tau_1 & , & \tilde\tau_4\tilde\tau_1 & , & \tilde\tau_1\tilde\tau_2\tilde\tau_1 & , & \tilde\tau_3\tilde\tau_4\tilde\tau_1 & , & \tilde\tau_7\tilde\tau_1 - 2\tilde\tau_1, \\
\tilde\tau_2\tilde\tau_3 & , & \tilde\tau_4\tilde\tau_3 & , & \tilde\tau_1\tilde\tau_2\tilde\tau_3 & , & \tilde\tau_3\tilde\tau_4\tilde\tau_3 & , & \tilde\tau_7\tilde\tau_3 - 2\tilde\tau_3, \\
\tilde\tau_2\tilde\tau_7 - 2\tilde\tau_2 & , & \tilde\tau_4\tilde\tau_7 - 2\tilde\tau_4 & , & \tilde\tau_1\tilde\tau_2\tilde\tau_7 - 2\tilde\tau_1\tilde\tau_2 & , & \tilde\tau_3\tilde\tau_4\tilde\tau_7 - 2\tilde\tau_3\tilde\tau_4 & , & \tilde\tau_7^2 - 2\tilde\tau_7 - \tilde\tau_1\tilde\tau_2\ .
\end{array}$$

Let I be the ideal generated by these elements. So $I \subseteq \ker(\varphi)$. Therefore, φ induces a surjective R-algebra morphism from $R\Psi/I$ to $\Lambda'_{(2)}$. We may reduce the list of generators to obtain

$$I = (\tilde\tau_2\tilde\tau_1, \tilde\tau_4\tilde\tau_1, \tilde\tau_7\tilde\tau_1 - 2\tilde\tau_1, \tilde\tau_2\tilde\tau_3, \tilde\tau_4\tilde\tau_3, \tilde\tau_7\tilde\tau_3 - 2\tilde\tau_3, \tilde\tau_2\tilde\tau_7 - 2\tilde\tau_2, \tilde\tau_4\tilde\tau_7 - 2\tilde\tau_4, \tilde\tau_7^2 - 2\tilde\tau_7 - \tilde\tau_1\tilde\tau_2)\ .$$

Note that $R\Psi/I$ is R-linearly generated by

$$\mathcal{N} := \{\tilde{\mathrm{e}}_3 + I, \tilde{\mathrm{e}}_4 + I, \tilde{\mathrm{e}}_5 + I, \tilde\tau_1 + I, \tilde\tau_2 + I, \tilde\tau_3 + I, \tilde\tau_4 + I, \tilde\tau_7 + I, \tilde\tau_3\tilde\tau_4 + I, \tilde\tau_1\tilde\tau_2 + I\},$$

cf. the underlined elements above. To see that, note that a product ξ of k generators may be written as a product in $\mathcal{N}$ of k' generators and a product of k'' generators, where $k = k' + k''$ and where k' is choosen maximal. We call k'' the excess of ξ. If $k'' \geq 1$ then, using the trees above, we may write ξ as an R-linear combination of products of generators that have excess $\leq k'' - 1$. Moreover, note that $|\mathcal{N}| = 10 = \mathrm{rk}_R(\Lambda'_{(2)})$.

Since we have a surjective R-algebra morphism from $R\Psi/I$ to $\Lambda'_{(2)}$, this rank argument shows this morphism to be bijective. In particular, $I = \ker(\varphi)$.

So, we obtain the

Proposition 11. *Recall that* $I = \begin{pmatrix} \tilde\tau_2\tilde\tau_1 & , & \tilde\tau_2\tilde\tau_3 & , & \tilde\tau_2\tilde\tau_7 - 2\tilde\tau_2, \\ \tilde\tau_4\tilde\tau_1 & , & \tilde\tau_4\tilde\tau_3 & , & \tilde\tau_4\tilde\tau_7 - 2\tilde\tau_4, \\ \tilde\tau_7\tilde\tau_1 - 2\tilde\tau_1 & , & \tilde\tau_7\tilde\tau_3 - 2\tilde\tau_3 & , & \tilde\tau_7^2 - 2\tilde\tau_7 - \tilde\tau_1\tilde\tau_2 \end{pmatrix}$.

We have the isomorphism of $\mathbf{Z}_{(2)}$*-algebras*

$$\Lambda'_{(2)} \quad \xrightarrow{\sim} \quad R\left[\begin{array}{ccccc} & \overset{\tilde\tau_2}{\curvearrowright} & & \overset{\tilde\tau_4}{\curvearrowleft} & \\ \tilde{\mathrm{e}}_3 & & \tilde{\mathrm{e}}_5 \;\overset{\tilde\tau_7}{\circlearrowright} & & \tilde{\mathrm{e}}_4 \\ & \underset{\tilde\tau_1}{\curvearrowleft} & & \underset{\tilde\tau_3}{\curvearrowright} & \end{array}\right]/I$$

$$\begin{array}{rcl} \mathrm{e}_i & \mapsto & \tilde{\mathrm{e}}_i + I \text{ for } i \in [3,5] \\ \tau_j & \mapsto & \tilde\tau_j + I \text{ for } j \in [1,7]\setminus\{5,6\}\ . \end{array}$$

Recall that $\mathrm{B}_{\mathbf{Z}_{(2)}}(\mathrm{S}_3,\mathrm{S}_3)$ *is Morita equivalent to* $\Lambda'_{(2)}$.

Corollary 12. *As* $\mathbf{F}_2$*-algebras, we have*

$$\Lambda'_{(2)}/2\Lambda'_{(2)} \;\cong\; \mathbf{F}_2\left[\begin{array}{ccccc} & \overset{\tilde\tau_2}{\curvearrowright} & & \overset{\tilde\tau_4}{\curvearrowleft} & \\ \tilde{\mathrm{e}}_3 & & \tilde{\mathrm{e}}_5 \;\overset{\tilde\tau_7}{\circlearrowright} & & \tilde{\mathrm{e}}_4 \\ & \underset{\tilde\tau_1}{\curvearrowleft} & & \underset{\tilde\tau_3}{\curvearrowright} & \end{array}\right] \Big/ \left(\begin{array}{ccccc} \tilde\tau_2\tilde\tau_1 & , & \tilde\tau_2\tilde\tau_3 & , & \tilde\tau_2\tilde\tau_7, \\ \tilde\tau_4\tilde\tau_1 & , & \tilde\tau_4\tilde\tau_3 & , & \tilde\tau_4\tilde\tau_7, \\ \tilde\tau_7\tilde\tau_1 & , & \tilde\tau_7\tilde\tau_3 & , & \tilde\tau_7^2 - \tilde\tau_1\tilde\tau_2 \end{array}\right).$$

Recall that $\mathrm{B}_{\mathbf{F}_2}(\mathrm{S}_3,\mathrm{S}_3)$ *is Morita equivalent to* $\Lambda'_{(2)}/2\Lambda'_{(2)}$.

5.4. **Localisation at 3:** $\mathrm{B}_{\mathbf{Z}_{(3)}}(\mathrm{S}_3,\mathrm{S}_3)$ **via congruences.** Write $R = \mathbf{Z}_{(3)}$. In the $\mathbf{Q}$-algebra A, cf. Proposition 5, we have the R-order

$$A_R := \begin{bmatrix} A_{R,1,1} & A_{R,1,2} & A_{R,1,3} & A_{R,1,4} \\ A_{R,2,1} & A_{R,2,2} & A_{R,2,3} & A_{R,2,4} \\ A_{R,3,1} & A_{R,3,2} & A_{R,3,3} & A_{R,3,4} \\ A_{R,4,1} & A_{R,4,2} & A_{R,4,3} & A_{R,4,4} \end{bmatrix} := \begin{bmatrix} R^{3\times3} & 0 & 0 & R^{3\times1} \\ 0 & R & 0 & R \\ 0 & 0 & R & 0 \\ R^{1\times3} & R & 0 & R[\overline\eta,\overline\xi] \end{bmatrix} \subseteq A\ .$$

Corollary 13. *We have*

$$\Lambda_{(3)} = \left\{ \begin{bmatrix} s_{1,1} & s_{1,2} & s_{1,3} & 0 & 0 & t_1 \\ s_{2,1} & s_{2,2} & s_{2,3} & 0 & 0 & t_2 \\ s_{3,1} & s_{3,2} & s_{3,3} & 0 & 0 & t_3 \\ 0 & 0 & 0 & u & 0 & v \\ 0 & 0 & 0 & 0 & w & 0 \\ x_1 & x_2 & x_3 & y & 0 & z_1 + z_2\overline\eta + z_3\overline\xi \end{bmatrix} \in A_R : \begin{array}{r} x_1 \equiv_3 0 \\ x_2 \equiv_3 0 \\ x_3 \equiv_3 0 \\ z_2 \equiv_3 0 \end{array} \right\} \subseteq A_R.$$

In particular, we have $\mathrm{B}_R = \mathrm{B}_R(\mathrm{S}_3,\mathrm{S}_3) \cong \Lambda_{(3)}$ *as* R*-algebras.*

More symbolically written, we have

$$\Lambda_{(3)} = \begin{bmatrix} R & R & R & 0 & 0 & R & & \\ R & R & R & 0 & 0 & R & & \\ R & R & R & 0 & 0 & R & & \\ 0 & 0 & 0 & R & 0 & R & & \\ 0 & 0 & 0 & 0 & R & 0 & & \\ (3) & (3) & (3) & R & 0 & R & +(3)\overline\eta & +R\overline\xi \end{bmatrix}.$$

Remark 14. *We claim that* $1_{\Lambda_{(3)}} = \mathrm{e}_1 + \mathrm{e}_2 + \mathrm{e}_3 + \mathrm{e}_4 + \mathrm{e}_5 + \mathrm{e}_6$ *is an orthogonal decomposition into primitive idempotents, where*

$$\mathrm{e}_1 := \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \end{bmatrix}, \quad \mathrm{e}_2 := \begin{bmatrix} 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \end{bmatrix}, \quad \mathrm{e}_3 := \begin{bmatrix} 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \end{bmatrix},$$

$$\mathrm{e}_4 := \begin{bmatrix} 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \end{bmatrix}, \quad \mathrm{e}_5 := \begin{bmatrix} 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \end{bmatrix}, \quad \mathrm{e}_6 := \begin{bmatrix} 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 \end{bmatrix}.$$

Proof. We have $\mathrm{e}_s \Lambda_{(3)} \mathrm{e}_s \cong R$ for $s \in [1,5]$. Therefore it follows that $\mathrm{e}_1, \mathrm{e}_2, \mathrm{e}_3, \mathrm{e}_4, \mathrm{e}_5$ are primitive.

To show that that e_6 is primitive, we *claim* that the ring $\mathrm{e}_6 \Lambda_{(3)} \mathrm{e}_6 \cong R[\overline{\eta}, \overline{\xi}]$ is local.

We have $\mathrm{U}(R[\overline{\eta}, \overline{\xi}]) = R[\overline{\eta}, \overline{\xi}] \setminus (3, \overline{\eta}, \overline{\xi})$. In fact, for $u := a + b\overline{\eta} + c\overline{\xi}$ with $a \in R \setminus (3)$ and $b, c \in R$, the inverse is given by $u^{-1} = a^{-1} - a^{-2}b\overline{\eta} - a^{-2}c\overline{\xi}$ as

$$uu^{-1} = aa^{-1} + (-a^{-1}b + a^{-1}b)\overline{\eta} + (-a^{-1}c + a^{-1}c)\overline{\xi} = 1 \, .$$

Thus the nonunits of $R[\overline{\eta}, \overline{\xi}]$ form an ideal and so $R[\overline{\eta}, \overline{\xi}]$ is a local ring. This proves the *claim*. □

5.5. $\mathrm{B}_{\mathbf{Z}_{(3)}}(\mathrm{S}_3, \mathrm{S}_3)$ **and** $\mathrm{B}_{\mathbf{F}_3}(\mathrm{S}_3, \mathrm{S}_3)$ **as path algebras modulo relations.** Write $R := \mathbf{Z}_{(3)}$. We aim to write $\Lambda_{(3)}$, up to Morita equivalence, as path algebra modulo relations. The R-algebra $\Lambda_{(3)}$ is Morita equivalent to $\Lambda'_{(3)} := (\mathrm{e}_3 + \mathrm{e}_4 + \mathrm{e}_5 + \mathrm{e}_6)\Lambda_{(3)}(\mathrm{e}_3 + \mathrm{e}_4 + \mathrm{e}_5 + \mathrm{e}_6)$ since $\Lambda_{(3)} \mathrm{e}_1 \cong \Lambda_{(3)} \mathrm{e}_2 \cong \Lambda_{(3)} \mathrm{e}_3$ using multiplication with elements of $\Lambda_{(3)}$ with a single nonzero entry 1 in the upper (3×3)-corner. We have the R-linear basis of $\Lambda'_{(3)}$ consisting of

$$\mathrm{e}_3 := \begin{bmatrix} 0&0&0&0&0&0\\ 0&0&0&0&0&0\\ 0&0&1&0&0&0\\ 0&0&0&0&0&0\\ 0&0&0&0&0&0\\ 0&0&0&0&0&0 \end{bmatrix}, \quad \mathrm{e}_4 := \begin{bmatrix} 0&0&0&0&0&0\\ 0&0&0&0&0&0\\ 0&0&0&0&0&0\\ 0&0&0&1&0&0\\ 0&0&0&0&0&0\\ 0&0&0&0&0&0 \end{bmatrix}, \quad \mathrm{e}_5 := \begin{bmatrix} 0&0&0&0&0&0\\ 0&0&0&0&0&0\\ 0&0&0&0&0&0\\ 0&0&0&0&0&0\\ 0&0&0&0&1&0\\ 0&0&0&0&0&0 \end{bmatrix},$$

$$\mathrm{e}_6 := \begin{bmatrix} 0&0&0&0&0&0\\ 0&0&0&0&0&0\\ 0&0&0&0&0&0\\ 0&0&0&0&0&0\\ 0&0&0&0&0&0\\ 0&0&0&0&0&1 \end{bmatrix}, \quad \tau_1 := \begin{bmatrix} 0&0&0&0&0&0\\ 0&0&0&0&0&0\\ 0&0&0&0&0&0\\ 0&0&0&0&0&0\\ 0&0&0&0&0&0\\ 0&0&3&0&0&0 \end{bmatrix}, \quad \tau_2 := \begin{bmatrix} 0&0&0&0&0&0\\ 0&0&0&0&0&0\\ 0&0&0&0&0&1\\ 0&0&0&0&0&0\\ 0&0&0&0&0&0\\ 0&0&0&0&0&0 \end{bmatrix},$$

$$\tau_3 := \begin{bmatrix} 0&0&0&0&0&0\\ 0&0&0&0&0&0\\ 0&0&0&0&0&0\\ 0&0&0&0&0&0\\ 0&0&0&0&0&0\\ 0&0&0&1&0&0 \end{bmatrix}, \quad \tau_4 := \begin{bmatrix} 0&0&0&0&0&0\\ 0&0&0&0&0&0\\ 0&0&0&0&0&0\\ 0&0&0&0&0&1\\ 0&0&0&0&0&0\\ 0&0&0&0&0&0 \end{bmatrix}, \quad \tau_5 := \begin{bmatrix} 0&0&0&0&0&0\\ 0&0&0&0&0&0\\ 0&0&0&0&0&0\\ 0&0&0&0&0&0\\ 0&0&0&0&0&0\\ 0&0&0&0&0&3\overline{\eta} \end{bmatrix},$$

$$\tau_6 := \begin{bmatrix} 0&0&0&0&0&0\\ 0&0&0&0&0&0\\ 0&0&0&0&0&0\\ 0&0&0&0&0&0\\ 0&0&0&0&0&0\\ 0&0&0&0&0&\overline{\xi} \end{bmatrix}.$$

We have $\tau_5 = \tau_1\tau_2$ and $\tau_6 = \tau_3\tau_4 + 4\tau_1\tau_2$. Hence, as an R-algebra $\Lambda'_{(3)}$ is generated by $\mathrm{e}_3, \mathrm{e}_4, \mathrm{e}_5, \mathrm{e}_6, \tau_1, \tau_2, \tau_3, \tau_4$.

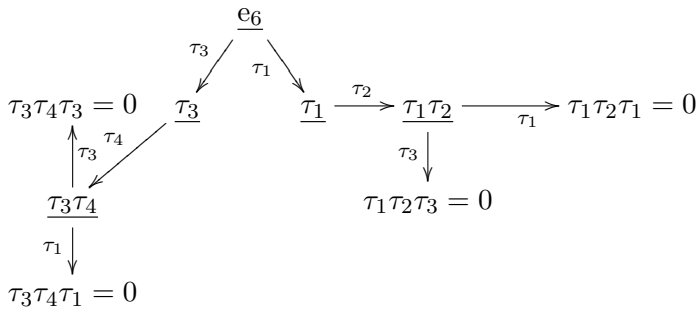
Consider the quiver $\Psi := \left[\tilde{\mathrm{e}}_5 \qquad \tilde{\mathrm{e}}_3 \underset{\tilde{\tau}_1}{\overset{\tilde{\tau}_2}{\rightleftarrows}} \tilde{\mathrm{e}}_6 \underset{\tilde{\tau}_3}{\overset{\tilde{\tau}_4}{\rightleftarrows}} \tilde{\mathrm{e}}_4 \right]$. We have a surjective R-algebra morphism $\varphi : R\Psi \to \Lambda'_{(3)}$ by sending

$$\begin{array}{cccccccccccc} \tilde{\mathrm{e}}_3 & \mapsto & \mathrm{e}_3 & , & \tilde{\mathrm{e}}_4 & \mapsto & \mathrm{e}_4 & , & \tilde{\mathrm{e}}_5 & \mapsto & \mathrm{e}_5 & , & \tilde{\mathrm{e}}_6 & \mapsto & \mathrm{e}_6 & , \\ \tilde{\tau}_1 & \mapsto & \tau_1 & , & \tilde{\tau}_2 & \mapsto & \tau_2 & , & \tilde{\tau}_3 & \mapsto & \tau_3 & , & \tilde{\tau}_4 & \mapsto & \tau_4 & . \end{array}$$

We establish the following multiplication trees, where we underline the elements that are not in an R-linear relation with previous elements.

The multiplication tree of the idempotent e_5 consists only of the element e_5.

$$\begin{array}{ccccc} \underline{\mathrm{e}_4} & \xrightarrow[\tau_4]{} & \underline{\tau_4} & \xrightarrow[\tau_3]{} & \tau_4\tau_3 = 0 \\ & & \downarrow{\scriptstyle \tau_1} & & \\ & & \tau_4\tau_1 = 0 & & \end{array} \qquad \begin{array}{ccccc} \underline{\mathrm{e}_3} & \xrightarrow[\tau_2]{} & \underline{\tau_2} & \xrightarrow[\tau_1]{} & \tau_2\tau_1 = 0 \\ & & \downarrow{\scriptstyle \tau_3} & & \\ & & \tau_2\tau_3 = 0 & & \end{array}$$



So the kernel of φ contains the elements:

$$\tilde{\tau}_4\tilde{\tau}_1,\ \tilde{\tau}_4\tilde{\tau}_3,\ \tilde{\tau}_2\tilde{\tau}_1,\ \tilde{\tau}_2\tilde{\tau}_3,\ \tilde{\tau}_3\tilde{\tau}_4\tilde{\tau}_3,\ \tilde{\tau}_2\tilde{\tau}_3,\ \tilde{\tau}_3\tilde{\tau}_4\tilde{\tau}_1,\ \tilde{\tau}_1\tilde{\tau}_2\tilde{\tau}_3,\ \tilde{\tau}_1\tilde{\tau}_2\tilde{\tau}_1\ .$$

Let I be the ideal generated by these elements. So, $I \subseteq \ker(\varphi)$. Therefore, φ induces a surjective R-algebra morphism from $R\Psi/I$ to $\Lambda'_{(3)}$. We may reduce the list of generators to obtain $I = (\tilde{\tau}_4\tilde{\tau}_3,\ \tilde{\tau}_4\tilde{\tau}_1,\ \tilde{\tau}_2\tilde{\tau}_1,\ \tilde{\tau}_2\tilde{\tau}_3)$.

Note that $R\Psi/I$ is R-linearly generated by

$$\mathcal{N} := \{\tilde{\mathrm{e}}_3 + I, \tilde{\mathrm{e}}_4 + I, \tilde{\mathrm{e}}_5 + I, \tilde{\mathrm{e}}_6 + I, \tilde{\tau}_1 + I, \tilde{\tau}_2 + I, \tilde{\tau}_3 + I, \tilde{\tau}_4 + I, \tilde{\tau}_3\tilde{\tau}_4 + I, \tilde{\tau}_1\tilde{\tau}_2 + I\},$$

cf. the underlined elements above. To see that, note that a product ξ of k generators may be written as a product in $\mathcal{N}$ of k' generators and a product of k'' generators, where $k = k' + k''$ and where k' is choosen maximal. If $k'' \geq 1$ then, using the trees above, we have $\xi = 0$. Moreover, note that $|\mathcal{N}| = 10 = \mathrm{rk}_R(\Lambda'_{(3)})$.

Since we have an surjective algebra morphism from $R\Psi/I$ to $\Lambda'_{(3)}$, this rank argument shows this morphism to be bijective. In particular, $I = \ker(\varphi)$.

So, we obtain the

Proposition 15. *Recall that* $I = (\tilde{\tau}_4\tilde{\tau}_3,\ \tilde{\tau}_2\tilde{\tau}_1,\ \tilde{\tau}_4\tilde{\tau}_1,\ \tilde{\tau}_2\tilde{\tau}_3)$.
We have the isomorphisms of R*-algebras*

$$\begin{array}{rcl} \Lambda'_{(3)} & \xrightarrow{\sim} & R\left[\ \tilde{\mathrm{e}}_5 \qquad \tilde{\mathrm{e}}_3 \underset{\tilde{\tau}_1}{\overset{\tilde{\tau}_2}{\rightleftarrows}} \tilde{\mathrm{e}}_6 \underset{\tilde{\tau}_3}{\overset{\tilde{\tau}_4}{\rightleftarrows}} \tilde{\mathrm{e}}_4\ \right]/I \\ \mathrm{e}_i & \mapsto & \tilde{\mathrm{e}}_i + I \text{ for } i \in [3,6] \\ \tau_i & \mapsto & \tilde{\tau}_i + I \text{ for } i \in [1,4] \end{array}$$

Recall that $\mathrm{B}_{\mathbf{Z}_{(3)}}(\mathrm{S}_3, \mathrm{S}_3)$ *is Morita equivalent to* $\Lambda'_{(3)}$.

Corollary 16. *As* $\mathbf{F}_3$*-algebras, we have*

$$\Lambda'_{(3)}/3\Lambda'_{(3)} \ \cong\ \mathbf{F}_3\left[\ \tilde{\mathrm{e}}_5 \qquad \tilde{\mathrm{e}}_3 \underset{\tilde{\tau}_1}{\overset{\tilde{\tau}_2}{\rightleftarrows}} \tilde{\mathrm{e}}_6 \underset{\tilde{\tau}_3}{\overset{\tilde{\tau}_4}{\rightleftarrows}} \tilde{\mathrm{e}}_4\ \right]/(\tilde{\tau}_4\tilde{\tau}_3,\ \tilde{\tau}_4\tilde{\tau}_1,\ \tilde{\tau}_2\tilde{\tau}_1,\ \tilde{\tau}_2\tilde{\tau}_3)\ .$$

Recall that $\mathrm{B}_{\mathbf{F}_3}(\mathrm{S}_3, \mathrm{S}_3)$ *is Morita equivalent to* $\Lambda'_{(3)}/3\Lambda'_{(3)}$.

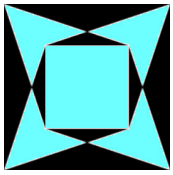
References

[1] B. Masterson, *On the table of marks of a direct product of finite groups,* `http://hdl.handle.net/10379/5550`, PhD thesis, NUI Galway, 2016.

[2] B. Masterson, G. Pfeiffer *On the table of marks of a direct product of finite groups,* arXiv:1704.03433v3, 2018.
[3] S. Bouc, *Foncteurs d'ensembles munis d'une double action*, J. Algebra 183, 664-736, 1996.
[4] S. Bouc, *Burnside rings*, Handbook of Algebra, volume 2, section 6E, 739-804, 2000.
[5] S. Bouc, *Biset Functors for Finite Groups,* Springer, 2010.
[6] P. Webb, *A guide to Mackey functors*, Handbook of Algebra, volume 2, section 6E, 805-836, 2000.
[7] R. Boltje, S. Danz, *A ghost algebra of the double Burnside algebra in characteristic zero,* arXiv:1203.1346, 2013.
[8] I. Reiner, *Maximal Orders*, Oxford University Press, 2003.
[9] G. D. James, *The irreducible representations of symmetric groups*, Bull. London Math. Soc. 8, no. 3, 229-232, 1976.
[10] Wieb Bosma, John Cannon, and Catherine Playoust, *The Magma algebra system. I. The user language*, J. Symbolic Comput., 24, 235-265, 1997.

Nora Krauss has written a Master's Thesis at the University of Stuttgart on double Burnside rings, where she in particular studied the case S_3 in detail. At present, she is a PhD student at the University of Stuttgart.

(author) University of Stuttgart
E-mail address: `kraussna@mathematik.uni-stuttgart.de`



Irish Math. Soc. Bulletin
Number 86, Winter 2020, 103–106
ISSN 0791-5578

Goldbach's Conjecture: if it's unprovable, it must be true

PETER LYNCH

Abstract. Goldbach's Conjecture is one of the best-known unsolved problems in mathematics. Over the past 280 years, many brilliant mathematicians have tried and failed to prove it. If a proof is found, it will likely involve some radically new idea or approach. If the conjecture is unprovable using the usual axioms of set theory, then it must be true. This is because, if a counter-example exists, it can be found by a finite search.

In 1742, Christian Goldbach wrote a letter to Leonhard Euler proposing that every integer greater than 2 is the sum of three primes. Euler responded that this would follow from the simpler statement that *every even integer greater than 2 is the sum of two primes.*

Goldbach's Conjecture is one of the best-known unsolved problems in mathematics. It is a simple matter to check the conjecture for the first few cases:

$$\begin{array}{lll} 4=2+2 & 6=3+3 & 8=5+3 \\ 10=7+3 & 12=7+5 & 14=11+3 \\ 16=13+3 & 18=13+5 & 20=17+3 \\ \cdots & \cdots & \cdots \end{array}$$

But, with an infinite number of cases, this approach can never prove the conjecture.

If, for an even number $2n$ we have $2n = p_1 + p_2$ where p_1 and p_2 are primes, then obviously

$$n = \frac{p_1 + p_2}{2} \tag{1}$$

If every even number can be partitioned in this way, then *any number, even or odd, must be the arithmetic average, or mean, of two primes.*

In Fig. 1 we plot the natural numbers from 1 to 25 (blue) and the first nine primes (red) in rows above and below the number line.

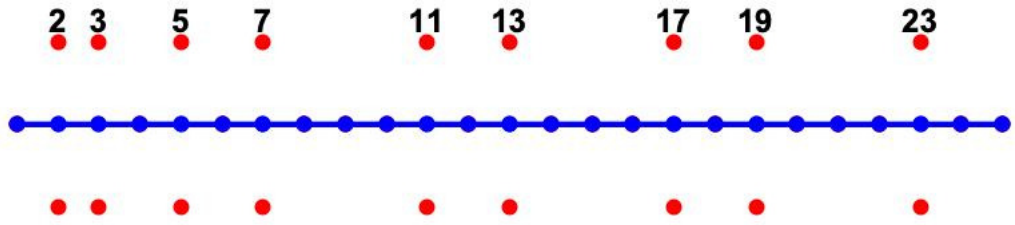


Figure 1. The natural numbers from 1 to 25, with the first nine primes plotted (in red) at equal distances above and below.

2010 *Mathematics Subject Classification.* 11P32, 03B25.
Key words and phrases. Number Theory, Logic.
Received on 31-8-2020; revised 10-9-2020.

In Fig. 2 we plot some lines joining primes in the upper row to primes in the lower row. Each such line intersects the central line at the mean value of the two primes. We see that there is a crossing line passing through every whole number: this is in agreement with the conjecture as expressed in (1).

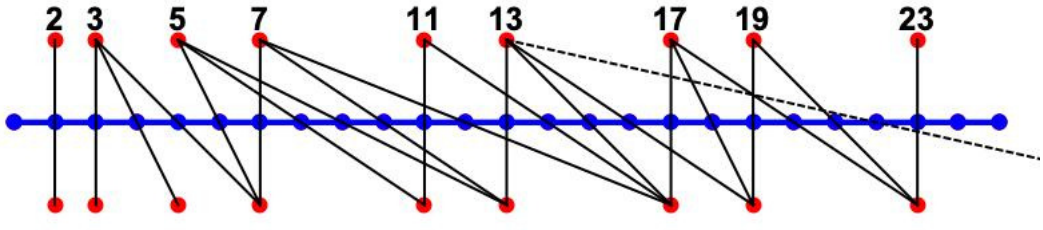


FIGURE 2. The line from p_1 above to p_2 below crosses the number line at the mean value $(p_1 + p_2)/2$. There is an intersection of some line of this sort for every $n \geq 2$.

It is clear from the conjecture that every even number can be expressed in terms of primes in two distinct ways: as a sum of two primes and as the mean of two primes:

$$\begin{aligned} \forall n \in \mathbb{N} \quad \exists\, p_1, p_2 \in \mathbb{P} \;:\; & \quad 2n = p_1 + p_2 \\ \forall n \in \mathbb{N} \quad \exists\, p_3, p_4 \in \mathbb{P} \;:\; & \quad 2n = (p_3 + p_4)/2\,. \end{aligned}$$

For the second of these forms, we have assumed that $4n = p_3 + p_4$.

Uncle Petros and Goldbach's Conjecture

The Goldbach Conjecture is the central theme of a novel by Apostolos Doxiadis, *Uncle Petros and Goldbach's Conjecture,* published in Greek in 1992 and in English in 2000. The hero is Petros Papachristos, a gifted, reclusive Greek mathematician who has spent most of his career trying to prove Goldbach's Conjecture. The narrator is his nephew, who tells the story of how, when he was a young teenager, his eccentric Uncle Petros set him the task of proving the conjecture.

The novel describes aspects of the recent history of mathematics, and gives some brilliant insights into the mental state and methods of a research mathematician. Although it is a work of fiction, Doxiadis gets the mathematical details right. He gives a great feeling for the passion that drives a research mathematician, and a good flavour of the nature of pure mathematics. He makes it clear that, while mathematical research is an enthralling and creative activity, it can become an obsession, obliterating all other interests, captivating the researcher and compelling him or her to work for years on a problem that may seem to others to be unimportant.

Several real-life mathematicians appear as characters in the book, including Constantin Carathéodory, G. H. Hardy, J. E. Littlewood, Srinivasa Ramanujan, Kurt Gödel and Alan Turing. The hero, Petros Papachristos, interacts with Hardy, Littlewood and Ramanujan, and he is profoundly affected by the work of Gödel and Turing. He realises the implication of advances in mathematical logic: Goldbach's Conjecture may be unprovable; the goal of his life's work may be unattainable.

To generate publicity for the book, the publishers offered a $1 million prize to anyone who could prove Goldbach's Conjecture within two years of the date of publication. The prize was never claimed.

The Entscheidungsproblem

Can every true mathematical statement be proved? The great German mathematician David Hilbert believed so and in 1928, together with Wilhelm Ackermann, he formulated the "Decision Problem", asking for an algorithm to establish *a priori* the validity or otherwise of any conjecture. He was destined to be disappointed.

In 1931 Kurt Gödel proved that mathematics is incomplete: whatever system of axioms we assume, there are statements that are true but that cannot be proved using only these axioms. Adding additional axioms may make such statements true but then new true-but-unprovable statements inevitably arise.

So, do we know of any statements that are unprovable using the usual axioms of mathematics? The Zermelo-Fraenkel (ZF) axioms of set theory form one of the standard starting-points. We now know that the axiom of choice (C) is independent of ZF, and that the continuum hypothesis is independent of ZF+C.

But what if we have a conjecture that we wish to prove, starting from the usual axioms of mathematics? Can we know in advance whether a mathematical proof is possible, or whether the conjecture is unprovable?

Hilbert's Decision Problem (Entscheidungsproblem) asks, in essence, if there is a way to determine — in the absence of a proof — whether any given mathematical statement or proposition is true or false. More specifically: Is there an algorithm that will take a logical statement in a formal language, and that will output its truth value. The algorithm does not need to indicate how it obtains the answer. Nor does it have to provide a proof. It just has to determine whether the statement is or is not valid.

In 1936, the American logician Alonzo Church showed that there can be no positive answer to the Entscheidungsproblem. Independently, and at about the same time, Alan Turing reached the same conclusion using a completely different method.

Church and Turing showed that it is impossible for an algorithm to decide in general whether a given statement in arithmetic is true or false. The implication of this is that, within a given system of axioms, there is no way to tell, ahead of time, whether a given conjecture can or cannot be proved. Hilbert's dream was shattered.

When Uncle Petros learned of these results, he too was devastated. He realised that a proof of Goldbach's Conjecture, on which he had laboured for decades, might not be possible. His life's work could have been in vain.

Unprovable but True?

We have no solid reason for suggesting that Goldbach's Conjecture cannot be proved on the basis of the usual axioms of mathematics. Although it is amusing to speculate, the only justification for such a claim is that the problem has been around for almost 280 years, and some of the most brilliant mathematicians have tried and failed to prove it. If a proof is found, it will likely involve some radically new idea or approach.

But let us suppose the conjecture is unprovable. Then it must be true!

Why? Because, if it is false, there exists an even number B that is not the sum of two primes. Since partitioning into primes has been confirmed for numbers up to more than a million million million, B must be enormous. However, it is finite, and a finite search must confirm that there are no two primes that add to B.

This would make the conjecture "provably false". In other words, falsehood of the conjecture is incompatible with unprovability. This contradiction forces us to an ineluctable conclusion: if Goldbach's Conjecture is unprovable, it must be true!

References

[1] Doxiadis, Apostolos, 2000: *Uncle Petros and Goldbach's Conjecture*. Faber & Faber, London. ISBN: 978-0-5712-0511-0.
[2] Wikipedia article *Goldbach's Conjecture*. `https://en.wikipedia.org/wiki/Goldbach%27s_conjecture` (accessed 01-09-2020)
[3] Wikipedia article *The Entscheidungsproblem*. `https://en.wikipedia.org/wiki/Entscheidungsproblem` (accessed 01-09-2020)

Peter Lynch is emeritus professor at UCD. His interests include all areas of mathematics and its history. He writes an occasional mathematics column in *The Irish Times* and has published a book of articles entitled *Thats Maths*. His blog is at `http://thatsmaths.com`.

School of Mathematics & Statistics, University College Dublin
E-mail address: `Peter.Lynch@ucd.ie`

Irish Math. Soc. Bulletin
Number 86, Winter 2020, 107–108
ISSN 0791-5578

Some shorter proofs for p-groups

ROBERT HEFFERNAN AND DESMOND MACHALE

Abstract. We give short proofs of elementary results about groups of prime power order.

One of the prettiest results in elementary group theory is the following:

Theorem 1. *If p is a prime number and G is a group with $|G| = p^2$, then G is abelian.*

The usual proof of this result runs like this:

Proof. $|Z(G)|$, being a divisor of $|G|$ is either 1, p of p^2. By a well-known result, since G is a p-group, $|Z(G)|$ is non-trivial, so $|Z(G)| = 1$ is ruled out. Next, if $|Z(G)| = p$, then $|G/Z(G)| = p$, so $G/Z(G)$ is cyclic. But, if $G/Z(G)$ is cyclic, then G is abelian, a contradiction. [Alternatively, if $|Z(G)| = p$, choose $a \in G, a \notin Z(G)$. Then $C_G(a) \supseteq \langle Z(G), a\rangle = G$, so $a \in Z(G)$, a contradiction.]

Thus $|Z(G)|$ must be p^2 and G is abelian. □

However, there is a shorter proof using group representation theory. We use the facts that

$$|G| = \sum_{i=1}^{k} d_i^2$$

where the d_i are the degrees of the irreducible complex representations of G; each d_i is a divisor of $|G|$, and the number of representations of degree 1 is $(G : G')$, where G' is the commutator subgroup of G.

The degree equation $|G| = \sum_{i=1}^{k} d_i^2$ gives

$$p^2 = (G : G') + tp^2$$

for some integer t. This is impossible unless $t = 0$ and $G' = \{1\}$, forcing G to be abelian.

We remark that groups of order n^2 are not necessarily abelian if n is not a prime. A minimal counterexample for $n = 4$ is given by D_8, the dihedral group of order 16. For p odd, there are non-abelian groups of order $81 = 9^2$, for example $G(27) \times C_3$, where $G(27)$ is a non-abelian group of order 27.

In general, the degree equation is in many ways a dual of the class equation of a group. Just as the class equation can be used to show that the centre of a p-group is non-trivial, the degree equation can be used to show that the commutator subgroup of a non-abelian p-group cannot have index 1 or p.

Theorem 2. *If G is a non-abelian p-group, then $(G : G') = 1$ or $(G : G') = p$ are not possible.*

Proof. (i) Suppose that $(G : G') = 1$. Then, for $n > 2$, $p^n = (G : G') + \sum p^{2i}$, for $i > 0$. So, $p^n = 1 + \sum p^{2i}$, which is a contradiction. [The usual method of proof of this is to show that G has a normal subgroup H with $(G : H) = p$. Thus, G/H is abelian, so $H \supseteq G'$, a contradiction.]

2020 *Mathematics Subject Classification.* 20-01.
Key words and phrases. groups, p-groups.
Received on 8-6-2020.

(ii) Suppose that $(G : G') = p$. Then, for $n > 2$, we have $p^n = (G : G') + \sum p^{2i}$, for $i > 0$ or $p^n = p + \sum p^{2i}$ and $p^{n-1} = 1 + \sum p^{2i-1}$, a contradiction.

□

We note that D_4, the dihedral group of order 8, and $G(27)$ show that $(G : G') = p^2$ is possible and that the above results can be extended to finite nilpotent groups, which are the direct product of p-groups.

Robert Heffernan is a Lecturer in the Department of Mathematics at Cork Institute of Technology. His mathematical interests are primarily in group theory.

Desmond MacHale is Emeritus Professor of Mathematics at University College Cork where he taught for nearly forty years. His mathematical interests are in abstract algebra but he also works in number theory, geometry, combinatorics and the history of mathematics. His other interests include humour, geology and words.

(Robert Heffernan) Department of Mathematics, Cork Institute of Technology, Ireland

(Desmond MacHale) Department of Mathematics, University College Cork, Ireland
E-mail address, R. Heffernan: robert.heffernan@cit.ie
E-mail address, D. MacHale: d.machale@ucc.ie

Irish Math. Soc. Bulletin
Number 86, Winter 2020, 109–113
ISSN 0791-5578

Cornel Ioan Vălean: (Almost) Impossible Integrals, Sums, and Series, Springer, 2019. ISBN:978-3-030-02461-1, EUR 64.99, 539+xxxviii pp.

REVIEWED BY SEÁN M. STEWART

On first opening this book it did not take me long to realise there was something Boschian about it. It is a vast store of results for definite integrals and infinite series that at first glance seem to defy what is possible to achieve analytically. Those drawn to the evaluation of integrals or series will find the present volume particularly difficult to pass by. Evaluating integrals has always had its coterie of dedicated admirers. G. H. Hardy once famously remarked 'he could never resist the challenge of a definite integral' [9, p. xi]. From the predilections of the current author it seems he would tend to have to agree.

Forming part of Springer's 'Problem Books in Mathematics' series the book is divided into two parts. The first three chapters on integrals forms the first half of the book (Chapter 1 the problems, Chapter 2 some hints, Chapter 3 their solutions), the last three chapters on series and a few finite sums forms the second half of the book (Chapter 4 the problems, Chapter 5 some hints, Chapter 6 their solutions). There are sixty problems in each part. Classical but tricky integrals such as (Problem 1.7 (i))

$$\int_0^1 \frac{\log^2(1+x)}{x}\,dx = \frac{1}{4}\zeta(3), \tag{1}$$

where ζ denotes the Riemann zeta function make an appearance but there is much more besides. As an example of the latter consider (Problem 1.33)

$$\int_0^1 \mathrm{Li}_2\left(\frac{x}{x-1}\right)\mathrm{Li}_2\left(\frac{x}{x+1}\right)\frac{dx}{x}.$$

Here Li_2 is the dilogarithm. It is problems like this that live up to the title of the book as being 'almost' impossible. Such an integral is sure to leave many scratching their head and wondering how a closed-form solution is even possible. That it is I leave to the interested reader.

Part of the fun and unusualness of the book is each of the 120 problems appear under their own headings. Here one finds, for example (Problem 1.41)

> A Little Integral-Beast from *Inside Interesting Integrals* Together with a Similar Version of It Tamed by Real Methods

or (Problem 4.37)

> Preparing the *Weapons* of *The Master Theorem of Series* to Breach the Fortress of the Challenging Harmonic Series of Weight 7: The 1st Episode

While the titles are delightfully curious and at times contain an interesting turn of phase, a small quibble is in other places the text could have benefited from tighter editing from the publisher given the first language of the author is not English.

Key words and phrases. Definite integrals, series, harmonic numbers, Euler sums, Riemann zeta function, polylogarithms.

Received on 19-8-2020; revised 7-9-2020.

As expected from a problem book there is little given in the way of preliminaries. It is more a case of diving in head first and hoping you do not immediately hit the bottom. A course in integral calculus is a given and one in the elements of real analysis would be helpful. The reader is also expected to have a high degree of fluency with 'standard' special functions such as polylagarithms, the polygamma function, and the Riemann zeta function, and to a lesser extent the Dirichlet beta function, the inverse tangent integral, Lerch transcendent, and Legendre's chi function of order two. Without knowledge of these progress will be largely impossible. Some familiarity in the manipulation of infinite series is also expected.

The first half of the book is devoted to definite integrals. Most of these are single integrals with a handful of double integrals and the occasional triple integral. The solutions given are comprehensive. An interesting feature is only real methods are considered – there is no contour integration – and seems to be very much the preference of the author. Sometimes two different methods are given and alternative approaches are referenced. Occasionally interesting pieces of information about a particular integral or its method of solution is included. As an example of this, for the first of the integrals given in Problem 1.3 we learn it is believed to have first appeared in a book containing a collection of problems suitable for the Cambridge course published in 1867 by the English mathematician Joseph Wolstenholme (1829–1891) [12, p. 214]. Some of the integrals are classical. Several were proposed by the author, having first appeared in the problem sections of journals such as *The American Mathematical Monthly* and *La Gaceta de la Real Sociedad Matemática Española*. Others still are completely new and original.

The methods used in solving the integrals are varied. Some are well known, others are inventive and creative. These include differentiating under the integral sign after the introduction of a parameter; what is commonly known as 'Feynman's trick'; converting a single integral to a double integral, and the use of infinite series. Still other ways is by exploiting algebraic identities, employing symmetry, or by creating a system of relations involving the integrals I and J and finding $I+J$ and $I-J$ first. As an example of the first of these latter approaches, from the algebraic identity

$$(A+B)^2+(A-B)^2=2A^2+2B^2,$$

on setting $A=\log(1-x)$ and $B=\log(1+x)$ the integral in (1) can be found. Such an ingenious approach was extensively used by De Doelder to evaluate many interesting integrals [5]. On display is the author's considerable manipulative dexterity and even for those who may know how to solve a particular problem there is much one can learn from a close reading of the provided solutions.

The second half of the book is devoted to the evaluation of series but it is really a rumination by the author on a particular type of series known as *Euler sums*. These are infinite series involving the harmonic numbers. As their name suggests, these series are named after the great Swiss mathematician Leonhard Euler, who along with the German mathematician Christian Goldbach initiated their study in the mid-eighteenth century. The nth generalised harmonic number of order $p\in\mathbb{N}$ is defined by

$$H_n^{(p)}=\sum_{k=1}^{n}\frac{1}{k^p},$$

such that $H_0^{(p)}\equiv 0$. When $p=1$ we have $H_n\equiv H_n^{(1)}$, the nth harmonic number. If we let $\pi=(\pi_1,\pi_2,\ldots,\pi_k)$ be a partition of integer p into k summands so that $p=\pi_1+\cdots+\pi_k$, $\pi_1\leqslant\pi_2\leqslant\cdots\leqslant\pi_k$, and q is an integer such that $q\geqslant 2$, the classical

(non-linear) Euler sum is defined by [6, p. 16]

$$S_{\pi,q} = \sum_{n=1}^{\infty} \frac{H_n^{(\pi_1)} H_n^{(\pi_2)} \cdots H_n^{(\pi_k)}}{n^q}. \tag{2}$$

One of Euler's famous early results is

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

Indeed, thirty-two different proofs of this classic result can be found in [4]. Later Euler found a generalisation

$$\sum_{n=1}^{\infty} \frac{H_n}{n^q} = \frac{1}{2}(q+2)\zeta(q+1) - \frac{1}{2}\sum_{n=1}^{q-2} \zeta(n+1)\zeta(q-n),$$

but it is disappointing to find this is not one of the problems given in the text (it is however stated without proof; see Eq. (3.45) on page 87). Perhaps the author considered the linear case far too elementary? A multitude of mostly non-linear Euler sums or closely related series involving the harmonic numbers appear. Seven problems towards the end deal specifically with alternating Euler sums.

My favourite of all the Euler sums is what is today referred to as the series of Au-Yeung. It is (Problem 4.22)

$$\sum_{n=1}^{\infty} \left(\frac{H_n}{n}\right)^2 = \frac{17}{4}\zeta(4) = \frac{17\pi^4}{360}. \tag{3}$$

Missed by Euler this series is largely responsible for the renewed fortunes of these sums. Starting in the mid-1990s with the work of Bailey, Borwein, and Girgensohn [1] and Borwein, Borwein, and Girgensohn [2] interest in series of this type was revived by an accidental discovery of (3). On this latter point the Borwein brothers write [3, p. 1191]

> This identity [namely (3)] was surprising and new to us when Enrico Au-Yeung (an undergraduate student in the Faculty of Mathematics in Waterloo) conjectured it on the basis of a computation of 500,000 terms (five digit accuracy!); our first impulse was to perform a higher-order computation to show it to be false. It is not easy to naively compute the value of the sum to more than about eight places.

The brothers went on to prove the result with the literature on Euler sums now vast. Ironically the proof of (3) responsible for rejuvenating interest in Euler sums was itself a rediscovery having first appeared, surprisingly, as a problem in the September 1948 issue of *The American Mathematical Monthly* [8].

From (2) we see a seemingly endless variety of Euler sums are possible. Many of the problems found in the second half of the book are devoted to evaluating particular examples of such sums. Beyond the literature little in the way of Euler sums has so far found itself a place in modern texts. A handful of problems are given in [10, pp. 228–229] and a more substantial set, but at a level slightly easier than those found in the current text, can be found in [7, pp. 148–151], which makes the present collection a welcome addition. Having problems and their solutions for a large collection of Euler sums in one location means the text should serve as a future source of reference for sums of this type.

Not all the series problems appearing in the second half of the book are straight up evaluation of Euler sums. More general and unusual sums containing a product between

the nth harmonic number and the tail of the Riemann zeta function can be found. One example of this is (Problem 4.45 (i))

$$\sum_{n=1}^{\infty} \frac{H_n}{n} \left(\zeta(4) - 1 - \frac{1}{2^4} - \cdots - \frac{1}{n^4} \right) = \frac{5}{48}\zeta(6) = \frac{\pi^6}{9072}.$$

As was the case for the integrals presented in the first half of the book, solutions to the series are found using only real methods. The methods used in their evaluation are a combination of conversion to an integral (often one already found in the first half of the book), the use of generating functions, or through series manipulation, of which the author makes heavy use. Here Abel's summation, changing the order of double summations, and the author's own *Master Theorem of Series* [11] are among the various techniques used. In the hands of the present author these are a powerful armamentaria.

I love Euler sums and would like to think they are useful. The author gives no hint of their usefulness. They simply appear as distant peaks that need to be scaled and conquered. In terms of usefulness they can often serve in the evaluation of integrals. But must a use be found for everything? Who cannot help but marvel at a beautiful closed-form solution to a problem many think is not possible? Euler sums may be a minor but scenic tributary of modern day mathematics but is one deeply rooted in the past that can be considered interesting for their own sake. If they are to eventually find wide applicability the fact remains for this to be discovered by others.

For the most part the author's manipulations with series and integrals are very clever and a lot of fun to watch. At times an integral or series that seems impossible disappears under a sea of what initially seems to be unrelated calculations only for it to re-emerge several pages later with its victor clutching at it solution. At other times invoking a hidden symmetry of the problem sees the initial impasse or but melt away. Many times my reaction to this was one of wonderment. Where do people get such ideas from? On encountering this we marvel that there are those who can imagine such things and make such unexpected connections.

So what is one to make of the book? Some readers may feel they have been transported back in time, finding themselves negotiating some rich undiscovered vein of late eighteenth or early nineteenth century mathematics. Pure mathematicians will probably grumble at the cavalier approach taken to rigour such as interchanges made between infinite summations and integrations, but for the type of person this book is most likely to appeal to this is but a small cavil. The book can serve as a useful supply of difficult definite integrals and infinite series problems for undergraduates or as a useful starting point for those wishing to attempt similar types of problems that arise from time to time in the various journals with dedicated problem pages. And there are of course a small group of those for whom the challenge of a definite integral is difficult to resist. In this book they have found themselves the perfect antidote.

References

[1] D. H. Bailey, J. M. Borwein, R. Girgensohn: *Experimental evaluation of Euler sums*, Exp. Math. (3) 1 (1994), 17–30.

[2] D. Borwein, J. M. Borwein, R. Girgensohn: *Explicit evaluation of Euler sums*, Proc. Edinb. Math. Soc. (38) 2 (1995), 277–294.

[3] D. Borwein, J. M. Borwein: *On an intriguing integral and some series related to* $\zeta(4)$, Proc. Amer. Math. Soc. (123) 4 (1995), 1191–1198.

[4] J. M. Borwein, D. M. Bradley: *Thirty-two Goldbach variations*, Int. J. Number Theory (2) 1 (2006), 65–103.

[5] P. J. De Doelder: *On some series containing* $\psi(x) - \psi(y)$ *and* $(\psi(x) - \psi(y))^2$ *for certain values of* x *and* y, J. Comput. Appl. Math. (37) 1–3 (1991), 125–141.

[6] P. Flajolet, B. Salvy: *Euler sums and contour integral representations*, Exp. Math. (7) 1 (1998), 15–35.
[7] O. Furdui: *Limits, Series, and Fractional Part Integrals. Problems in Mathematical Analysis*, Problem Books in Mathematics, Springer, 2013.
[8] H. F. Sandham: *Problem 4305*, Amer. Math. Monthly (55) 7 (1948), 431.
[9] F. A. Sherk, P. McMullen, A. C. Thompson, A. I. Weiss: *Kaleidoscopes: Selected Writings of H. S. M. Coxeter*, Canadian Mathematical Society Series of Monographs and Advanced Texts, John Wiley and Sons, Inc., New York, 1995.
[10] H. M. Srivastava, J. Choi: *Zeta and q-Zeta Functions and Associated Series and Integrals*, Elsevier, Amsterdam, 2012.
[11] C. I. Vălean: *A master theorem of series and an evaluation of a cubic harmonic series*, J. Class. Anal. (10) 2 (2017), 97–107.
[12] J. Wolstenholme: *A Book of Mathematical Problems, on Subjects Included in the Cambridge Course*, MacMillian, London, 1867.

Seán M. Stewart After leaving Australia, for many years Seán taught mathematics to engineers in Kazakhstan and the United Arab Emirates. He has always found it hard to resist the challenge of a definite integral and is the author of *How to integrate it: A practical guide to finding elementary integrals* published by Cambridge University Press.

9 Tanang Street, Bomaderry NSW 2541, Australia
E-mail address: sean.stewart@physics.org

Irish Math. Soc. Bulletin
Number 86, Winter 2020, 114–116
ISSN 0791-5578

PROBLEMS

IAN SHORT

Problems

The first problem this issue is due to Yagub Aliyev of ADA University, Azerbaijan. A similar problem attracted popular interest in Azerbaijan during 2020.

Problem 86.1. Find the nearest integer to

$$10^{2021} - \sqrt{(10^{2021})^2 - 10^{2021}}.$$

The second problem was proposed by Seán Stewart of Bomaderry, Australia.

Problem 86.2. Evaluate

$$\int_0^1 \frac{1}{x} \arctan\left(\frac{2rx}{1+x^2}\right) dx,$$

where r is a real constant.

The third problem comes from Finbarr Holland of University College Cork.

Problem 86.3. Prove that

$$\sum_{n=0}^{\infty} \frac{9n+5}{9n^3+18n^2+11n+2} = 3\log 3.$$

Solutions

Here are solutions to the problems from *Bulletin* Number 84.

The first problem in Issue 84 was a corrected version of Problem 82.1, which was missing some hypotheses. The problem uses the usual notation $x_1, x_2, \ldots, x_n$ for the components of a vector x in $\mathbb{R}^n$. It was solved by the North Kildare Mathematics Problem Club and the proposer, Finbarr Holland. We present a version of Finbarr's solution with modifications from the Problem Club.

Problem 84.1. Suppose that u and v are linearly independent vectors in $\mathbb{R}^n$ with

$$0 < u_1 \leqslant u_2 \leqslant \cdots \leqslant u_n \quad \text{and} \quad v_1 > v_2 > \cdots > v_n > 0.$$

Given $x \in \mathbb{R}^n$, let y be the orthogonal projection of x onto the subspace spanned by u and v; thus $y = \lambda u + \mu v$, for uniquely determined real numbers λ and μ. Prove that if

$$x_1 > x_2 > \cdots > x_n > 0,$$

then μ is positive.

Solution 84.1. A straightforward calculation shows that

$$\mu = \frac{x \cdot w}{|w|^2}, \quad \text{where} \quad w = v - \frac{u \cdot v}{|u|^2} u.$$

Thus it suffices to show that

$$|u|^2 (v \cdot x) > (u \cdot x)(u \cdot v).$$

Received 19-1-2021.

Let us now define

$$a_i = \frac{x_i}{u_i}, \quad b_i = \frac{v_i}{u_i}, \quad c_i = u_i^2, \quad \text{for } i = 1, 2, \ldots, n,$$

the coordinates of vectors a, b and c. Then

$$\begin{aligned} |u|^2(v \cdot x) - (u \cdot x)(u \cdot v) &= \sum_{i=1}^{n} c_i \sum_{j=1}^{n} a_j b_j c_j - \sum_{i=1}^{n} a_i c_i \sum_{j=1}^{n} b_j c_j \\ &= \sum_{i,j=1}^{n} c_i c_j (a_j b_j - a_i b_j) \\ &= \tfrac{1}{2} \sum_{i,j=1}^{n} c_i c_j (a_j b_j - a_i b_j + a_i b_i - a_j b_i) \\ &= \tfrac{1}{2} \sum_{i,j=1}^{n} c_i c_j (a_i - a_j)(b_i - b_j). \end{aligned}$$

Observe that $a_1 > a_2 > \cdots > a_n > 0$ and $b_1 > b_2 > \cdots > b_n > 0$. Hence

$$c_i c_j (a_i - a_j)(b_i - b_j) \geqslant 0, \quad \text{for } i, j = 1, 2, \ldots, n,$$

with equality if and only if $i = j$. Thus $|u|^2(v \cdot x) - (u \cdot x)(u \cdot v) > 0$, as required. □

The next problem was solved by JP McCarthy of the Cork Institute of Technology, the North Kildare Mathematics Problem Club and the proposer, Finbarr Holland. We present JP's solution.

Problem 84.2. Given any finite collection $L_1, L_2, \ldots, L_n$ of infinite straight lines in the complex plane, find a formula in terms of data specifying $L_1, L_2, \ldots, L_n$ for a differentiable function $f\colon \mathbb{R} \longrightarrow \mathbb{C}$ with the property that each line L_i is tangent to the curve $f(\mathbb{R})$.

The following solution assumes that none of the lines L_j are vertical; it can easily be adjusted to deal with the omitted special cases.

Solution 84.2. Each line L_j has a parametrization

$$\ell_j(t) = t + i(m_j t + c_j), \quad \text{for } t \in \mathbb{R}.$$

For $j = 2, 3, \ldots, n$ and $t \in \mathbb{R}$, we define

$$\begin{aligned} \phi_j(t) = (1-t)^3(1 + i(m_{j-1} + c_{j-1})) + 3(1-t)^2 t(2 + i(2m_{j-1} + c_{j-1})) \\ + 3(1-t)t^2(-1 + i(-m_j + c_j)) + t^3 i c_j. \end{aligned}$$

This is the cubic Bézier curve from the point on L_{j-1} with real part 1 to the point on L_j with real part 0. It uses the point on L_{j-1} with real part 2 and the point on L_j with real part -1 to match the slopes of L_{j-1} and L_j at $t = 0$ and $t = 1$.

By construction, the function $f\colon \mathbb{R} \to \mathbb{C}$ that, for $j = 2, 3, \ldots, n$, satisfies

$$f(x) = \begin{cases} \ell_1(x) & \text{if } x < 1, \\ \phi_j(x - (2j-3)) & \text{if } 2j - 3 \leqslant x < 2j - 2, \\ \ell_j(x - (2j-2)) & \text{if } 2j - 2 \leqslant x < 2j - 1, \\ \ell_n(x - (2n-2)) & \text{if } x \geqslant 2n - 1, \end{cases}$$

has the desired properties. □

The third problem was solved by the North Kildare Mathematics Problem Club, and it is their solution presented here.

Problem 84.3. Suppose that each edge of a finite directed graph G is coloured in one of some finite collection of different colours, with the property that for each colour c and vertex v, there is precisely one directed edge with colour c and target vertex v. Prove that for any infinite sequence of colours $c_1, c_2, \ldots$ there is an infinite walk $e_1, e_2, \ldots$ of directed edges of G such that, for each index i, e_i has colour c_i and the target vertex of e_i equals the source vertex of e_{i+1}.

Solution 84.3. (We assume G has a nonempty vertex set V and there is at least one colour.) The finite edge set E is nonempty. We give it the discrete topology, give $E^{\mathbb{N}}$ the product topology, and give the set $W \subset E^{\mathbb{N}}$ of infinite walks the relative topology. Observe that W is compact, since it is a closed subset of the compact Hausdorff space $E^{\mathbb{N}}$. Note also that $E^{\mathbb{N}}$ is metrizable, and a sequence (w_n) of walks converges if and only if for each $i \in \mathbb{N}$ the sequence formed by taking the ith edge $w_n(i)$ of w_n, $n = 1, 2, \ldots$, is eventually constant.

Let $c_1, c_2, \ldots$ be a given sequence of colours. For any $n \in \mathbb{N}$ and each vertex $v \in V$ we see by working backwards that there is a finite walk $e \in E^{\{1,2,\ldots,n\}}$ ending at v such that e_i has colour c_i for $1 \leqslant i \leqslant n$. By taking n greater than the order $|V|$ of V we see that G contains a cycle.

If we remove terminal vertices and the edges to those vertices from G, we are left with a nonempty graph having the same property – nonempty because it will contain each loop. Repeating the process at most $|V|$ times, we obtain a graph without terminal vertices having the same property. Thus we may assume without loss in generality that G has no terminal vertices. Then each finite walk may be continued to some infinite walk. In particular, each set

$$K_n = \{w \in W : w(i) \text{ has colour } c_i,\ \forall i \leq n\}$$

is nonempty. Moreover $K_{n+1} \subset K_n$ for each $n \in \mathbb{N}$, and each K_n is closed and hence compact. Thus

$$K = \bigcap_{n=1}^{\infty} K_n \neq \varnothing,$$

and any element $w \in K$ is an infinite walk having colour sequence $c_1, c_2, \ldots$. □

We invite readers to submit problems and solutions. Please email submissions to `imsproblems@gmail.com` in any format (we prefer 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. Please include solutions to any problems you submit, if you have them.

School of Mathematics and Statistics, The Open University, Milton Keynes MK7 6AA, United Kingdom

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.