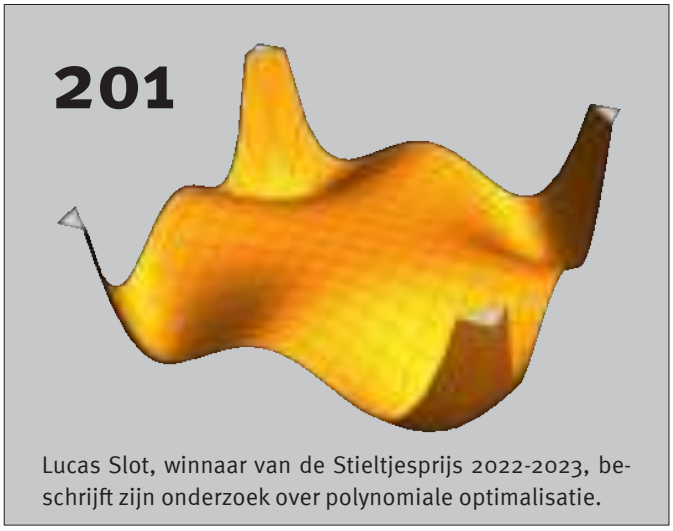
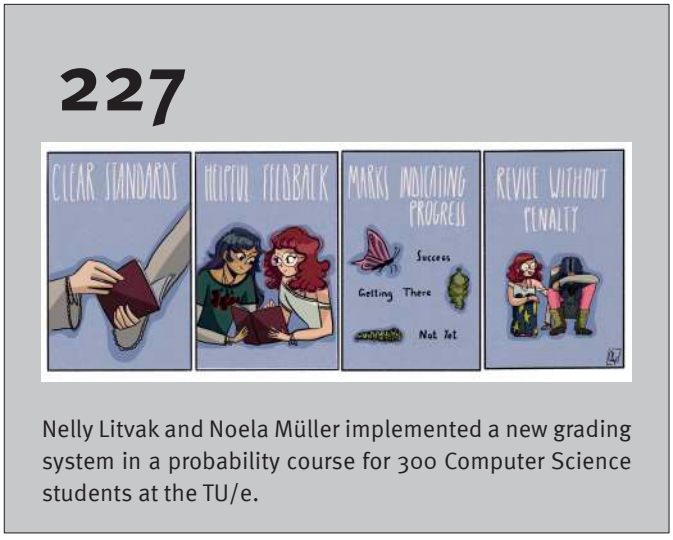
Inhoud | Contents



Lucas Slot, winnaar van de Stieltjesprijs 2022-2023, beschrijft zijn onderzoek over polynomiale optimalisatie.



Nelly Litvak and Noela Müller implemented a new grading system in a probability course for 300 Computer Science students at the TU/e.

Colofon

Het Nieuw Archief voor Wiskunde is een uitgave van het Koninklijk Wiskundig Genootschap en verschijnt vier maal per jaar. Het tijdschrift richt zich op eenieder die zich beroepsmatig met wiskunde bezighoudt, als academisch of industrieel onderzoeker, student, leraar, journalist of beleidsmaker. Het stelt zich ten doel te berichten over ontwikkelingen in de wiskunde in het algemeen en in de Nederlandse wiskunde in het bijzonder.

ISSN 0028-9825

Adres
Nieuw Archief voor Wiskunde
Centrum Wiskunde & Informatica
Postbus 94079
1090 GB Amsterdam
redactie@nieuwarchief.nl
www.nieuwarchief.nl

Hoofdredactie
Raf Bocklandt (r.r.j.bocklandt@uva.nl)
Renee Hoekzema (r.s.hoekzema@vu.nl)

Eindredactie/Bladmanager
Hester Breman (info@nieuwarchief.nl)

Redactie
Francesca Arici (UL), Edward Berengoltz (UvA), Viktor Blåsjö (UU), Hans Cuypers (TU/e), Marie Beth van Egmond (TNO), Robbert Fokkink (TUD), Teun Koetsier (VU), Nelly Litvak (TU/e), Diletta Martinelli (UvA), Nicolaos Starreveld (UvA), Hans Sterk (TU/e), Mark Timmer (UT)

Problemenrubriek (problems@nieuwarchief.nl)
Onno Berrevoets en Daan van Gent

Bureauredactie
Taeke Roukema

Illustraties
Ryu Tajiri

Vormgeving
Susanne Laws (omslag)
Kitty Molenaar (ontwerp)

Druk
Veldhuis Media

Advertenties
advertenties@nieuwarchief.nl

Koninklijk Wiskundig Genootschap
www.wiskgenoot.nl

Platform Wiskunde Nederland
www.platformwiskunde.nl

European Mathematical Society
www.euro-math-soc.eu

International Mathematical Union
www.mathunion.org

Koninklijk Wiskundig Genootschap

Het Koninklijk Wiskundig Genootschap (KWG) is een landelijke vereniging van beoefenaren van de wiskunde. In 1778 opgericht onder de zinspreuk 'Een onvermoeide arbeid komt alles te boven' is het 's werelds oudste nationale wiskundegenootschap. Leden ontvangen het Nieuw Archief voor Wiskunde als onderdeel van hun lidmaatschap.

Bestuur
Mathisca de Gunst (VU, voorzitter), Thomas Rot (VU, penningmeester), Charlene Kalle (UL, secretaris), Eric Cator (RU, vice-voorzitter), Danny Beckers (VU, inspecteur der Boekerij), Jop Briët (CWI), Rogier Bos (UU), Niels Kolenbrander (UL), Alef Sterk (RUG).

Secretariaat
Koninklijk Wiskundig Genootschap
Centrum Wiskunde & Informatica
Postbus 94079, 1090 GB Amsterdam
wiskgenoot@wiskgenoot.nl

Ledenadministratie KWG / Abonnementen
admin@wiskgenoot.nl
Wijzigingen of opzegging kunt u ook doorgeven door in te loggen op www.wiskgenoot.nl.

Contributie
Tarieven per jaar (bij betaling per automatische incasso krijgt u € 2,50 korting):
– gewoon lid: € 97,50
– reciprociteitslid: € 77,50
– gepensioneerden en werklozen: € 52,50
– aio's, oio's, studenten: € 42,50 (max. 4 jaar)
– lid zonder Nieuw Archief: € 57,50
Studenten en pas afgestudeerden kunnen een jaar lang gratis lid worden.
Voor verzending van het Nieuw Archief naar het buitenland wordt een portotoeslag van € 10 in rekening gebracht.
Instituten in Nederland en buitenland kunnen zich abonneren op het Nieuw Archief voor Wiskunde voor € 105 (Nederland), € 115 (Europa) of € 117,50 (buiten Europa).

Members of foreign societies
Members of *SIAM*, the *Société Mathématique de France*, the *Gesellschaft für Angewandte Mathematik und Mechanik*, the *Deutsche Mathematiker-Vereinigung*, and of the *American*, *Australian*, *Belgian*, *Indian*, *London*, *Spanish*, and *South-African Mathematical Societies* living outside of the Netherlands pay € 77,50 instead of the full membership fee of € 97,50 a year. Conversely, these foreign societies, as well as the VvS+OR and the NVORWO, have reduced membership fees for KWG members. A postage charge of € 10 is added for members living abroad but in Europe, and a charge of € 12,50 for members living outside of Europe.

Exchange subscriptions
Koninklijk Wiskundig Genootschap Library
Centrum Wiskunde & Informatica
P.O. Box 94079, NL-1090 GB Amsterdam
KWG-exchange@cwi.nl

Informatie voor auteurs

Kopij
Kopij dient per e-mail te worden aangeboden aan kopij@nieuwarchief.nl. Voor meer informatie en auteursinstructies zie www.nieuwarchief.nl.

Volgende nummers

nummer	*maand verschijnen*	*deadline kopij*
26(1)	maart 2025	verstreken
26(2)	juni 2025	01-02-2025
26(3)	september 2025	01-05-2025
26(4)	december 2025	01-08-2025

Instituuts- en bedrijfsleden

De publicaties van het KWG worden mede mogelijk gemaakt door de bijdragen van de volgende instituten en bedrijven.

- Centrum Wiskunde & Informatica
- Universiteit van Amsterdam
- Vrije Universiteit Amsterdam
- Rijksuniversiteit Groningen
- Universiteit Leiden
- Radboud Universiteit Nijmegen
- Universiteit Utrecht
- Technische Universiteit Delft
- Technische Universiteit Eindhoven
- Universiteit Twente

- Elsevier
- ORTEC

On the cover

Marton's conjecture concerns sumsets of subsets of finite vector spaces. If such a set has small doubling, it can be covered by a few cosets of a relatively small subspace. In 2023 a proof was found by Gowers, Green, Manners and Tao. Read more about the conjecture in the article by Jop Briët on page 217.

Polarisatiefilters

Begin november is de tijd waarin ik begin na te denken over wat ik in mijn redactioneel voor het Nieuw Archief voor Wiskunde wil schrijven. Vaak baseer ik me dan op wat er in ons decembernummer zal verschijnen, of laat ik me inspireren door de actualiteit. Wat dit laatste betreft, heeft deze novembermaand heel wat te bieden, al is het allemaal niet zo vrolijk nieuws: de presidentsverkiezingen in Amerika, rellen in Amsterdam, en zonet kwam ook nog het bericht binnen dat de demonstratie tegen de besparingen in het hoger onderwijs is afgelast uit vrees voor geweld.

Deze zaken passen allemaal in een fenomeen dat al door vele anderen is aangehaald, maar waar ik het toch even over wil hebben: de toegenomen polarisatie. In een tijd waarin debatten steeds scherper worden gevoerd, is het verleidelijk om alleen op de uitersten te focussen: de polen van een discussie, waar de standpunten het verst uit elkaar liggen. Bovendien hebben we vaak de neiging om iedereen in een van de kampen in te delen, en misschien wijzen we daardoor onbewust ook opinies toe die die persoon helemaal niet heeft. Het is al meerdere malen gebeurd dat ik verbaasd was toen ik een collega, vriend of familielid een mening hoorde verkondigen die niet paste in het beeld dat ik me van hem of haar gevormd had. Zulke momenten vind ik altijd bijzonder leerrijk omdat ze me zelf ook tot nadenken stemmen en soms dwingen mijn eigen mening te herzien.

In de wetenschap doet zich vaak een gelijkaardig fenomeen voor. Bij de analyse van meerdimensionale data is het handig om deze gegevens samen te vatten in een of meerdere hoofdcomponenten en daar dan mee te werken, maar door dat te doen kan je bepaalde fenomenen over het hoofd zien. Toen de eerste kaarten van de Cosmic Background Radiation werden gemaakt, viel op dat deze duidelijk gepolariseerd was in een bepaalde richting. Deze richting werd bepaald door de beweging van de aarde door de ruimte. Pas door dit weg te filteren en naar de hogere multipoolmomenten te kijken, konden astronomen diepere inzichten verwerven over het ontstaan van het heelal.

Analoog hieraan is het gezond om tijdens een verhitte discussie het ‘dipoolmoment’ er even uit te filteren en je te concentreren op de interessante multipolen die erachter verscholen zitten.

Ook in onze wiskundegemeenschap zijn er zaken waarbij het antwoord niet zwart-wit is; denk maar aan de recente discussie rond didactiek. Daarom sluit ik me graag aan bij de conclusie van de open brief van Jan Karel Lenstra die we in dit nummer publiceren: tussen de extremen van een strijdperk ligt er vaak een goed begaanbaar pad.

Raf Bocklandt, hoofdredacteur
Korteweg-de Vries Instituut, Universiteit van Amsterdam

Agenda

| Upcoming Events

januari 2025

11 januari 2025

❑ **KWG Wintersymposium 2025**

Jaarlijks congres voor wiskundedocenten en andere belangstellenden met dit jaar als thema 'Wiskunde en politiek'.

plaats *Academiegebouw, Utrecht*

info *sites.google.com/view/wintersymposium2025*

13-15 januari 2025

❑ **Conference on the Mathematics of Operations Research**

De 50ste editie van het jaarlijkse congres van het Landelijk Netwerk Mathematische Besliskunde.

plaats *Kontakt der Kontinenten, Soesterberg*

info *lnmb.nl/conferences*

20-25 januari 2025

❑ **Winter School on Mathematical Finance**

De 22ste editie van de jaarlijkse wintercursus binnen het domein der financiële wiskunde.

plaats *Kontakt der Kontinenten, Soesterberg*

info *staff.fnwi.uva.nl/a.khedher/winterschool/winterschool.html*

20-31 januari 2025

❑ **Eerste ronde Nederlandse Wiskunde Olympiade 2025**

De wiskundeolympiade gaat weer van start voor middelbareschoolklassen 1 t/m 5.

plaats *eigen school*

info *wiskundeolympiade.nl*

23-24 januari 2025

❑ **Higher Geometric Structures along the Lower Rhine XVIII**

Nederlands-Duitse workshop over meetkunde en topologie met onderwerpen als Liegroepoïden, differentieerbare schelven en hogere categorieën.

plaats *Radboud Universiteit, Nijmegen*

info *math.ru.nl/~sagave*

22-24 januari 2025

❑ **15th Central European Relativity Seminar**

Internationale conferentie over algemene relativiteitstheorie.

plaats *Radboud Universiteit, Nijmegen*

info *cers.univie.ac.at/cers15*

27–31 januari 2025

❑ **SWI 2025**

Jaarlijkse Studiegroep Wiskunde met de Industrie. Deelnemers werken een week lang samen aan wiskundige problemen voorgelegd door bedrijven.

plaats *Universiteit Utrecht*

info *swi-wiskunde.nl*

29–31 januari 2025

❑ **ORBEL-NGB Conference on Operations Research**

Conferentie over kwantitatieve technieken voor onderzoekers en gebruikers van besliskunde en aangrenzende vakgebieden.

plaats *Universiteit Maastricht*

info *maastrichtuniversity.nl/events*

februari 2025

3–21 februari 2025

❑ **OnderbouwWiskundeDag**

Wiskundewedstrijd voor derdeklassers. De kinderen werken in teams aan wiskundig georiënteerde opdrachten.

plaats *eigen school*

info *wiskundeinteams.sites.uu.nl*

maart 2025

6–7 maart 2025

❑ **15th Day on Computational Game Theory**

Conferentie over computationele speltheorie georganiseerd door de Universiteit van Tilburg.

plaats *MindLabs, Tilburg*

info *tilburguniversity.edu*

13 maart 2025

❑ **Werken aan basisvaardigheden rekenen-wiskunde in alle vakken**

Vijfde (tevens slot)editie van conferentie over wiskunde bij andere vakken in onderbouw voortgezet onderwijs, georganiseerd door o.a. NVvW.

plaats *De Domstad, Utrecht*

info *nvvw.nl*

Suggesties voor deze agenda zijn welkom.
Redacteur: Edward Berengoltz
agenda@nieuwarchief.nl

14 maart 2025
❑ **Internationale Dag van de Wiskunde 2025**
Wereldwijde viering van wiskunde met als thema dit keer 'Mathematics for a Better World'.
plaats *wereldwijd*
info *mathness.nl/pi-dag-idm*

14 maart 2025
❑ **Tweede ronde Nederlandse Wiskunde Olympiade 2025**
Ronde twee van de nationale wiskundeolympiade voor middelbareschoolklassen 1 t/m 5.
plaats *universiteiten*
info *wiskundeolympiade.nl*

14–15 februari 2025
❑ **Finaleweekend Wiskunde A-lympiade**
Finaleronde voor zes Nederlandse en wat buitenlandse ploegen.
plaats *Garderen*
info *wiskundeinteams.sites.uu.nl*

17 maart 2025
❑ **Diligentialezing van Daan Commelin**
Getiteld "Wiskunde en AI voor het simuleren van klimaat- en andere multischaalsystemen".
plaats *Lange Voorhout, Den Haag*
info *natuurwetenschappen-diligentia.nl*

19 maart 2025
❑ **Bekendmaking Abelprijs 2025**
De Noorse Academie van Wetenschappen en Letteren kondigt de winnaar van de Abelprijs van volgend jaar aan.
plaats *Oslo*
info *abelprize.no*

19 maart 2025
❑ **23ste Grote Rekendag**
Jaarlijkse dag in het teken van rekenen en hoe dat leuk en nuttig kan zijn, bedoeld voor basisschoolleerlingen. Het thema van 2025 is 'Eerlijk Delen'.
plaats *eigen school*
info *groterekendag.sites.uu.nl*

20 maart 2025
❑ **Kangoeroewedstrijd 2025**
Jaarlijkse reken- en wiskundewedstrijd voor lagere en middelbare scholen.
plaats *eigen school*
info *w4kangoeroe.nl*

21 maart 2025
❑ **Nationale Rekencoördinatoren Dag**
Dag in het teken van reken- en wiskundeonderwijs op lagere scholen met diverse lezingen en workshops georganiseerd door de NVORWO.
plaats *IPABO, Amsterdam*
info *nvorwo.nl/nationale-rekencoordinator-dag-2*

21 maart 2025
❑ **Prijsuitreiking Wiskunde B-dag**
Bespreking van de opdracht en prijsuitreiking met interactieve lezing en afsluitende borrel.
plaats *Academiegebouw, Utrecht*
info *wiskundeinteams.sites.uu.nl*

21 maart 2025
❑ **16de landelijke NWT-conferentie**
Jaarlijkse conferentie over natuur, wetenschap en techniek in het basisonderwijs, met dit jaar als thema 'Buiten de Lijntjes'.
plaats *Hotel Woudschoten, Zeist*
info *natuurwetenschapentechniek.nl/overzicht/conferenties*

25 maart 2025
❑ **Gecijferdheid telt mee! 2025**
Jaarlijkse conferentie met lezingen en workshops over de stand van 's lands gecijferdheid onder de bevolking.
plaats *Hogeschool Utrecht*
info *gecijferdheidteltmee.nl*

25–26 maart 2025
❑ **Dutch Days of Combinatorics 2025**
Bijeenkomst van de combinatoriekgemeenschap met verscheidene sprekers en voordrachten.
plaats *Aula, TU Delft*
info *sites.google.com/view/ddoc2025*

31 maart–2 april 2025
❑ **Algebra meets probability**
Congres over het samenspel van algebra en kansrekening, georganiseerd door Eurandom.
plaats *Eindhoven*
info *eurandom.tue.nl/event/algebra-meets-probability/*

april 2025

4–5 april 2025
❑ **NWD 2025**
De 31ste editie van de Nationale Wiskunde Dagen, een tweedaagse conferentie voor wiskundeleraren.
plaats *De Leeuwenhorst, Noordwijkerhout*
info *uu.nl/onderwijs/nationale-wiskunde-dagen*

7 april 2025
❑ **DIAMANT-Symposium**
Jaarlijkse bijeenkomst van het onderzoekscluster DIAMANT.
plaats *Universiteitsbibliotheek, De Uithof, Utrecht*
info *diamantcluster.nl/events*

11–17 april 2025
❑ **European Girls' Mathematical Olympiad 2025**
Internationale wiskundewedstrijd speciaal voor middelbare scholieres.
plaats *Prisjtina, Kosovo*
info *egmo.org*

22–23 april 2025
❑ **NMC 2025**
Nederlands Mathematisch Congres. Jaarlijkse bijeenkomst van wiskundig Nederland, georganiseerd door het KWG.
plaats *Kontakt der Kontinenten, Soesterberg*
info *wiskgenoot.nl*

25–27 april 2025
❑ **Benelux Mathematical Olympiad 2025**
17de editie van de jaarlijkse wiskundewedstrijd voor middelbare scholieren uit de Benelux.
plaats *Luik, België*
info *bxmo.org*

mei 2025

22–23 mei 2025
❑ **43ste Panamaconferentie**
Jaarlijkse conferentie voor docenten en beleidsmakers in het reken- en wiskundeonderwijs met deze keer als thema 'AI, tijd, rekenen-wiskunde'.
plaats *Hotel Woudschoten, Zeist*
info *panamaconferentie.sites.uu.nl*

Nieuws

| News

Deze rubriek is een kroniek van wiskundige activiteiten in Nederland. Toekomstige activiteiten worden aangekondigd en van voorbije activiteiten wordt verslag gedaan. Wilt u uw aankondiging of verslag in deze rubriek geplaatst zien? Stuur ons dan uw bijdrage, zo mogelijk met illustratie. De redactie behoudt zich het recht voor berichten te weigeren of in te korten.

Redacteur: Edward Berengoltz

nieuws@nieuwarchief.nl

26ste Christiaan Huygensprijs uitgereikt

Jan-Willem van Ittersum heeft op 16 oktober met zijn proefschrift *Partitions and quasimodular forms. Variations on the Bloch–Okounkov theorem* de Christiaan Huygensprijs voor wiskunde gewonnen. Deze beloont ieder jaar een onderzoeker in een van Huygens' vakgebieden voor zijn ''vernieuwende bijdrage aan de wetenschap''. De jury, voorgezeten door Eric Opdam, was zeer lovend over Van Ittersums ''spectaculaire nieuwe resultaten'' omtrent (uitbreidingen van) de Stelling van Bloch–Okoenkov en haar toepassingen. De Hollander, thans postdoctoraal onderzoeker aan de Universität zu Köln, is in 2021 aan de Universiteit Utrecht gepromoveerd bij Gunther Cornelissen en Don Zagier. De prijs is hem uitgereikt door Minister Bruins van Onderwijs, Cultuur en Wetenschap en hij gaat gepaard met een cheque ter waarde van 10 000 euro en een bronzen sculptuur van de Gouden Eeuwse wetenschapper. De andere genomineerden, Rosa Schwarz en Lucas Slot, hebben beiden een oorkonde en miniatuurbeeldje van Huygens bekomen. Voor een interview met Van Ittersum, zie pagina 242.

christiaanhuygensprijs.nl

Foto: Paul Voorham

Van Ittersum met Minister Bruins.

Nederlandse Wiskunde Olympiade 2024 afgesloten

De prijswinnaars van de 63ste nationale wiskundeolympiade zijn op 8 november gehuldigd op de TU Eindhoven. De zege van vierdeklasser Naïm Hofstede geniet de meeste luister: hij heeft alle opgaven foutloos op weten te lossen. In klas 5 ontvangt Josiah 't Hart de eerste prijs en Lucas van de Sande heeft de zesdeklassers de loef afgestoken. Er hebben 153 leerlingen meegedaan aan de finale van wie 31 doorgaan naar trainingen voor grensoverschrijdende wedstrijden. Opvallend is overigens dat vier van de vijf finaleopgaven ditmaal zijn bedacht door olympiadeveteraan Mike Daas, thans onderzoeker aan het Max-Planck-Institut te Bonn.

wiskundeolympiade.nl

Kabinet focust op basisvaardigheden onderwijs

In de begroting van het Ministerie van Onderwijs, Cultuur en Wetenschap voor 2025 is een Herstelplan kwaliteit onderwijs opgenomen. Dit gaat in het voorjaar van start en wordt verwezenlijkt in samenwerking met scholen en leerlingen. Het is erop gericht om de basisvaardigheden in het basis- en voortgezet onderwijs omtrent lezen, schrijven en rekenen te verbeteren alsook het lerarentekort

te lenigen. Voorts zal het Herstelplan mbo-studenten de mogelijkheid bieden om terdege aan deze vaardigheden te werken indien het niveau na de middelbare school niet voldoende is. “Dat leerlingen beter leren lezen, schrijven en rekenen, staat bovenaan mijn prioriteitenlijst. Om op eigen benen te kunnen staan, zijn die vaardigheden de absolute basis,” aldus Staatssecretaris Paul.

rijksoverheid.nl

Ig Nobelprijs voor muntjesopgooiers

In het NAW-Nieuws van december 2023 werd kond gedaan van een proefondervindelijk onderzoek naar de kansen op welke zijde een opgegooide munt landt. Daaraan hadden 49 mensen en, gedurende een totaal van 650 uur, ruim 350 000 muntjes van 44 verschillende denominaties en valuta meegedaan. Het resultaat schraagde de voorspelling dat een munt met 51% kans terecht zou komen op dezelfde kant als waarop zij aanvankelijk had gelegen. Een opmerkelijk uitvloeisel is echter dat deze voorkeur voor de beginzijde allengs af lijkt te nemen naarmate iemand vaker muntjes opgooit. De onderzoekers noemen 10 000 worpen als punt vanaf welk een munt plus opgooier als eerlijk kunnen worden beschouwd. Zult u zich eens vervelen...

Nu heeft de psycholoog Eric-Jan Wagenmakers (hoogleraar Bayesiaanse methodologie, UvA), die het onderzoek met zijn promovendus František Bartoš leidde, de Ig Nobelprijs voor Waarschijnlijkheid gewonnen. De prijs is hun, toepasselijk uitgedost in t-shirts met Julianaguldens, op 12 september uitgereikt aan het Massachusetts Institute of Technology. De Ig Nobelprijs bekroont ludiek maar danig wetenschappelijk onderzoek dat “mensen eerst aan het lachen maakt en vervolgens aan het denken zet”.

De ceremonie barst zelf ook van de strapatsen. Winnaars krijgen bijvoorbeeld een bankbiljet ter waarde van 10 biljoen (!) Zimbabwaanse dollar. Wagenmakers eindigde beider heren korte toespraak met een kwinkslag: “Wij moedigen iedereen aan om bij te dragen aan dit fascinerende onderzoek en wellicht ons experiment te reproduceren.” (Aan welk karwei het een vrouw in het publiek behaagde terstond te beginnen.)

De Telegraaf en E-J Wagenmakers

Wagenmakers en Bartoš bij hun toespraak.

Pierre Deligne viert 80ste verjaardag

De Brusselse wiskundige Pierre René, burggraaf Deligne, is op 3 oktober tachtig jaar oud geworden. Hij geniet grote bekendheid voor onder andere het bewijs van de Vermoedens van Weil en is één van de slechts vier wiskundigen die met zowel de Fieldsmedaille (1978) als de Wolfprijs (2008) én Abelprijs (2013) gedoteerd zijn, naast overigens ook andere eerbetonen.

De Belg is geboren in Etterbeek en in 1968 bij Alexandre Grothendieck aan de Université Libre de Bruxelles gepromoveerd op

Bron: Heiko Junge/The Abel Prize

Bron: numericana.com

Links Deligne met Abelprijs in 2013. Rechts: De burggrafelijke heraldiek met devies.

de Stelling van Lefschetz en ontaardingsvoorwaarden van spectraalrijen. Nadien heeft hij nog een staatsdoctoraat behaald op Hodgetheorie aan de Université Paris-Sud. Hij is jarenlang professor geweest aan het Institut des Hautes Études Scientifiques (IHES), alwaar hij beklijvende bijdragen heeft geleverd aan de algebraïsche meetkunde en Hodgetheorie, getaltheorie, kwantumgroepen en Hopfalgebra’s, en het Langlandsprogramma, met een bewijs van het derde Weilvermoeden als opus magnum. Hij is in 1980 getrouwd met de Russin Jelena Vladimirovna en vier jaar later neergezegen aan het Institute for Advanced Study in Princeton.

Koning Albert II heeft Deligne in 2006 in de adelstand verheven tot burggraaf (*vicomte*) voor zijn wiskundige verdienste. Aldus mocht hij een wapenschild ontwerpen. Dat is gebaseerd op een tautologisch kinderversje over te velde gaande hennen – zijns inziens verzinnebeeldt het de logica achter wiskundige verhandelingen. Deligne staat tevens afgebeeld op een Belgische postzegel uit 2007 samen met de ongelijkheid $|\tau(p)| \leq 2.p^{11/2}$. Deze heeft te maken met de Weilvermoedens.

In de boeken stuit men op ettelijke concepten die ’s burggraven naam dragen. Een kleine greep: Deligne–Mumfordmoduli en -schelven, Deligne–Lusztig-theorie, en de Stelling van Deligne over gemengde Hodgestructuren op de cohomologie van algebraische variëteiten.

MacTutor

ERC-beurzen voor Italianen in Nederland

De Europese ERC-subsidies zijn dit jaar weer uitgereikt, waarvan twee voor Nederlandse wiskundige onderzoeksprojecten. Ludovico Lami van de Universiteit van Amsterdam krijgt een ERC Starting Grant om een aanzienlijke fout in het bewijs van het Gegeneraliseerde Kwantumlemma van Stein op te lossen. Dit hiaat in het – nota bene door Lami zelf gefnuikte – bewijs vormt een apert probleem in de verstrengelingstheorie, een tak van de kwantuminformatie. (Hij zal het onderzoek nochtans aan de Scuola Normale Superiore in Pisa uitvoeren.)

Verder ontvangt Stefano Stramigioli, hoogleraar gevorderde robotica aan de Universiteit Twente, een ERC Advanced Grant ter waarde van € 2,8 miljoen voor het project *PortWings*. Dit poogt aan de hand van realistische robotvogels vluchtpatronen en hun achterliggende natuurkunde uit te vogelen. Stramigioli zal dit doen op basis van 'poort-Hamiltoniaanse' dynamica. "Ik ben ontzettend blij dat ik dankzij de ERC-subsidie weer echt tijd kan investeren in datgene waar mijn hart ligt [...], namelijk om heel diep in de wis- en natuurkunde te duiken." *uva.nl, utwente.nl*

'Redenerende' kunstmatige intelligentie?

Softwarebedrijf OpenAI heeft nieuwe modellen van kunstmatige intelligentie, summier o1 genaamd, ter markte gebracht. Ze zijn onderdeel van de vraagbaak ChatGPT Plus en speciaal bedoeld voor wetenschappers en AI-ontwikkelaars. Hun functie is nog steeds om vragen te beantwoorden, maar dankzij een techniek die *reinforcement learning* ("bekrachtigend leren") heet, wordt een antwoord stapsgewijs grondiger geanalyseerd en zo nodig verbeterd alvorens te worden gegeven. Kunstmatige intelligentie vordert met rasse schreden en dit is haar jongste stap richting menselijk redeneervermogen, zeggen de makers.

Het nadeel aan o1 is evenwel dat een antwoord langer op zich laat wachten. Het gebruik van deze nieuwe modellen is daarom baarlijk prijziger. Desondanks zijn de resultaten onder de streep beter dan voorheen. Zo hebben de o1-modellen een score van 83% behaald op de AIME (een Amerikaans kwalificatie-examen voor de Internationale Wiskundeolympiade). De schamele 13% van hun voorganger GPT-4o steekt hier maar schrilletjes bij af.

Financial Times

Nieuw grootste priemgetal ontdekt

Het grootst bekende priemgetal is sinds 12 oktober $2^{136.279.841}-1$ en bestaat, indien voluit geschreven, uit ruim 41 miljoen cijfers. Het is het 52ste Mersennepriemgetal (gegeven door een macht van twee min één) en werd gevonden door Luke Durant uit Californië in het kader van het programma Great Internet Mersenne Prime Search. De priemheid is bewezen middels de Lucas–Lehmertest. Het vorige Mersennepriemgetal stamt alweer uit 2018. *mersenne.org*

Zwitserse zeper door frappante formulefout

De Zwitserse federale overheid heeft een grove fout erkend in haar begroting voor de staatspensioenen. Het voorspelde tekort van de AHV/AVS (*Alters- und Hinterlassenenversicherung/assurance-vieillesse et survivants*) voor 2033 bedraagt na correctie circa 4 miljard frank. Dit is bijkans de helft van de eerder geraamde 7,3 miljard. Een oeps om u tegen te zeggen. Het federale verzekeringsorgaan heeft bij controle twee fouten ontdekt bij de in de voorspellingsmodellen gebruikte wiskundige formules.

Het onderwerp ligt gevoelig en zorgt voor wrevel bij de Eedgenoten, wier vertrouwen in de overheid nu een klap int. Per referendum is dit jaar een dertiende maand voor gepensioneerden bedongen terwijl het voorstel om de pensioenleeftijd met een jaar naar 66 te verhogen is gesneefd. Het echec met de formules speelt de regering dus parten, juist nu sommige partijen een belastingverhoging zouden willen bedisselen om die pensioenen te kunnen betalen. Controleert dus altijd uwe berekeningen.

euronews.com

Achtste Kanlezing verzorgd door John Jones

Ieder jaar wordt een tweedaagse lezing ter nagedachtenis aan de Nederlandse wiskundige Daniël Kan (1927–2013) gehouden aan de Universiteit Utrecht. De editie van 2024 heeft op 26 en 27 september plaatsgevonden met als spreker John Jones, hoogleraar emeritus aan de University of Warwick. Deze Engelsman pur sang heeft veel gewerkt aan cyclische cohomologie, operaden en snaartopologie. Zijn voordracht, getiteld *Exceptional phenomena in geometry and topology*, getuigde dienovereenkomstig van zijn bekwaamheid.

De lezing betrof de Riemannse symmetrische ruimten van uitzonderlijk type. Voor de kenners: dat zijn de twaalf symmetrische ruimten gekoppeld aan de exceptionele Liegroepen in Cartans classificatie. Jones laveerde tussen hun representatietheorie en topologische K-theorie, waarbij de Rosenfeldse projectieve vlakken als leidend voorbeeld dienden. Vergist u niet; dit zijn geen huis-tuin-en-keukenvariëteitjes! Hun dimensies gaan 's mensen inbeeldingsvermogen al fluks te boven, zodat Jones' vertelling naar exotische sferen rees. Figuurlijk tenminste: verrassenderwijs werd het door Atiyah veronderstelde verband met exotische sferen en het zogeheten Kervaire-invariantprobleem opgeduikeld. "Thank you for inviting me to give these lectures," besloot Jones ten slotte; "it has certainly cleared up a lot." *uu.nl*

L. Slot
Department of Computer Science
ETH Zürich
lucas.slot@inf.ethz.ch

Onderzoek Research

Polynomiale optimalisatie en sommen van kwadraten

Lucas Slot ontving op het Nederlands Mathematisch Congres 2024 de Stieltjesprijs voor zijn proefschrift "Asymptotic Analysis of Semi-definite Bounds for Polynomial Optimization and Independent Sets in Geometric Hypergraphs", verdedigd in 2022 aan de Universiteit van Tilburg. In dit artikel legt hij uit waar zijn proefschrift over ging.

Het doel van wiskundige optimalisatie is het minimaliseren (of maximaliseren) van een gegeven *doelfunctie* onder een set *voorwaarden*. Denk bijvoorbeeld aan het ontwerpen van een dienstregeling die de gemiddelde reistijd voor passagiers minimaliseert, maar binnen een voorgeschreven budget blijft. Formeel gesproken krijgen we een functie $f\colon \mathbb{R}^n \to \mathbb{R}$ (de doelfunctie) en functies $g_1, g_2, \ldots g_m\colon \mathbb{R}^n \to \mathbb{R}$ (de voorwaarden), en moeten we het minimum van f berekenen over de verzameling

$$\mathcal{X} := \{x \in \mathbb{R}^n : g_1(x) \geq 0, \ldots, g_m(x) \geq 0\}$$

van punten die aan de voorwaarden voldoen. Met andere woorden, we moeten de waarde bepalen van

$$\text{opt} := \inf_{x \in \mathcal{X}} f(x) \tag{1}$$

Omdat optimalisatieproblemen in het algemeen te complex zijn om met de hand op te lossen, zijn we geinteresseerd in het ontwikkelen van *efficiënte algoritmen* waarmee het optimum met behulp van een computer kan worden berekend.

Polynomiale optimalisatie

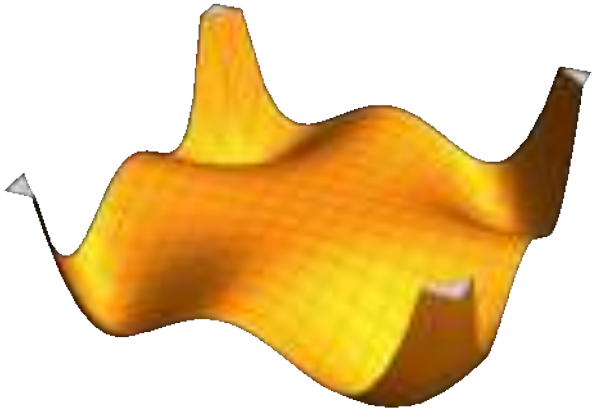
In mijn proefschrift [8] bestudeer ik zogenaamde *polynomiale optimalisatieproblemen* (POPs), waarin de doelfunctie en de voorwaarden polynomen zijn. Deze optimalisatieproblemen hebben brede toepassingen, zowel binnen als buiten de wiskunde. Daar staat tegenover dat het moeilijk (NP-hard) is om ze *exact* op te lossen. Dit motiveert de zoektocht naar efficiënte *benaderingsmethoden*, die het optimum berekenen met een (hopelijk) kleine foutmarge. De meest succevolle aanpak is gebasseerd op een link tussen polynomiale optimalisatie en algebraische meetkunde. Om deze link te kunnen leggen, hebben we eerst een alternatieve formulatie nodig van het probleem (1). We zeggen dat een polynoom p *niet-negatief* is op $\mathcal{X}$ wanneer $p(x) \geq 0$ voor alle $x \in \mathcal{X}$. We schrijven dan $p \in \mathcal{P}(\mathcal{X})$. Nu geldt dat

$$\text{opt} = \inf_{x \in \mathcal{X}} f(x) = \sup_{\lambda \in \mathbb{R}} \{\lambda : f - \lambda \in \mathcal{P}(\mathcal{X})\}. \tag{2}$$

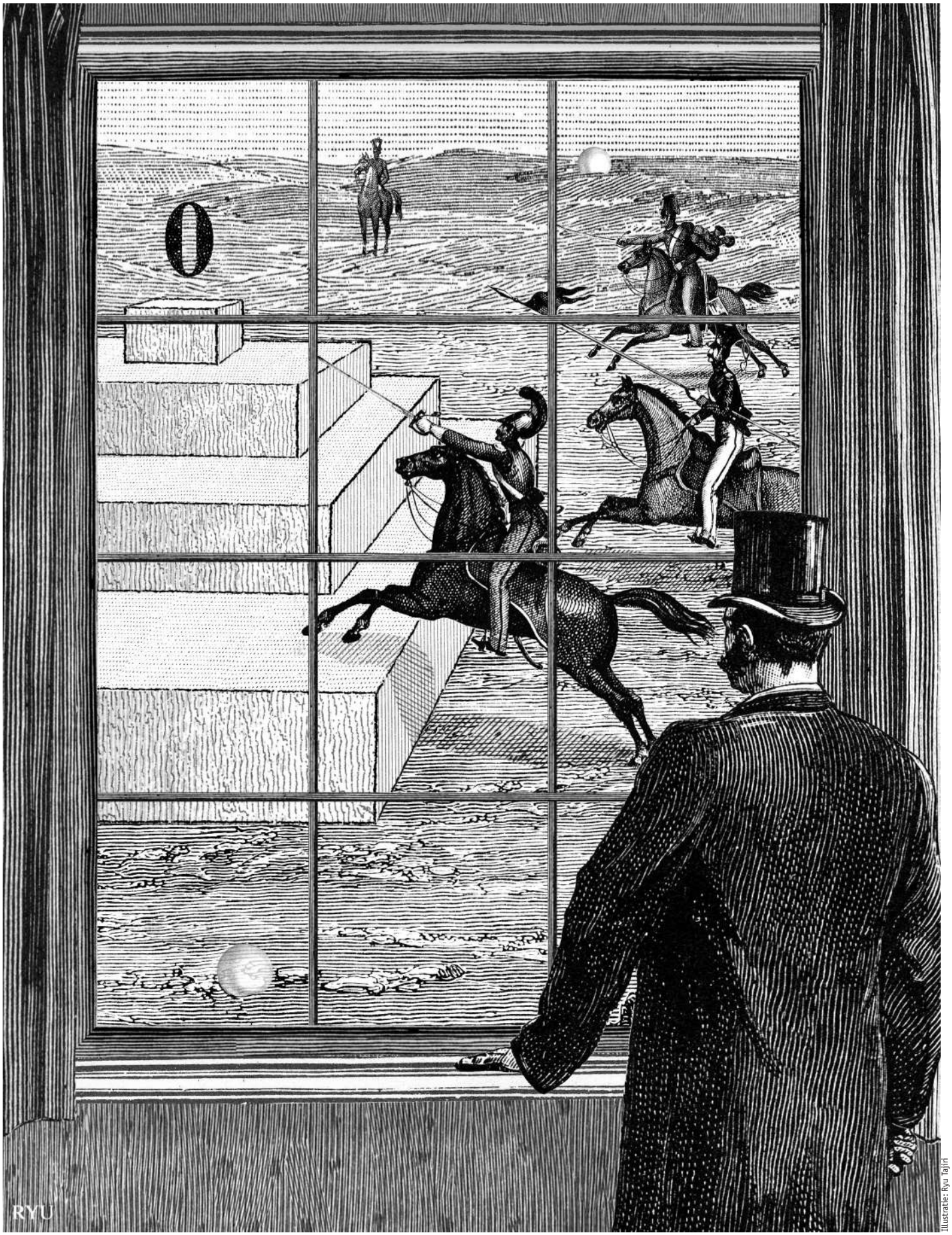
Dat wil zeggen, het minimum van f op $\mathcal{X}$ is gelijk aan het grootste getal λ zodanig dat $f - \lambda$ niet-negatief is op $\mathcal{X}$. Deze observatie laat zien dat het oplossen van polynomiale optimalisatieproblemen in feite equivalent is aan het bepalen van niet-negativiteit van polynomen.

Sommen van kwadraten

Hoe bepalen we of een polynoom niet-negatief is? Neem bijvoorbeeld



Figuur 1 Het *Motzkin-polynoom* $p(x_1, x_2) = x_1^4 x_2^2 + x_1^2 x_2^4 - 3x_1^2 x_2^2 + 1$ is niet-negatief op geheel $\mathbb{R}^2$ (als gevolg van de AM-GM-ongelijkheid). Het is echter geen som van kwadraten.



Illustratie: Ryu Tajiri

$$p(x_1,x_2) = x_1^6 - 2x_1^3x_2^2 + x_1^2 - 4x_1x_2 + x_2^4 + 4x_2^2.$$

Aan de hand van de definitie is het niet onmiddelijk duidelijk of p negatieve waardes aan kan nemen. Een korte berekening leert echter dat p kan worden geschreven als een *som van kwadraten*, namelijk

$$p(x_1,x_2) = (x_1 - 2x_2)^2 + (x_1^3 - x_2^2)^2.$$

Dit laat meteen zien dat $p(x_1,x_2) \geq 0$ voor alle $x_1,x_2 \in \mathbb{R}$.

Definitie
Een polynoom p is een *som van kwadraten (svk)* wanneer het geschreven kan worden als

$$p(x) = p_1(x)^2 + p_2(x)^2 + \ldots p_\ell(x)^2 \ \big(p_i \in \mathbb{R}[x]\big).$$

We zeggen dan dat $p \in \Sigma$, en merken op dat $\Sigma \subseteq \mathcal{P}(\mathbb{R}^n)$.
We kunnen sommen van kwadraten ook toepassen om niet-negativiteit op $\mathcal{X} \subseteq \mathbb{R}^n$ te bepalen. Stel dat een polynoom p geschreven kan worden als

$$p(x) = \sigma_0(x) + \sigma_1(x)g_1(x) + \ldots + \sigma_m(x)g_m(x), \tag{3}$$

waar elk van de $\sigma_i \in \Sigma$ een som van kwadraten is. Dan volgt direct dat $p(x) \geq 0$ voor alle $x \in \mathcal{X}$. (Immers, per definitie geldt $g_i(x) \geq 0$ voor alle $x \in \mathcal{X}$.) We noemen de representatie (3) een *certificaat* van niet-negativiteit voor p op $\mathcal{X}$. De verzameling van alle polynomen met zulk een certificaat heet het *kwadratische moduul* $Q(\mathcal{X})$ van $\mathcal{X}$. Er geldt dus dat $Q(\mathcal{X}) \subseteq \mathcal{P}(\mathcal{X})$. Met het oog op formulatie (2) geeft deze inclusie ons een *ondergrens* voor het optimalisatieprobleem (3), namelijk

$$\mathrm{svk} := \sup_{\lambda \in \mathbb{R}} \{\lambda : f - \lambda \in Q(\mathcal{X}))\} \leq \mathrm{opt}. \tag{4}$$

Immers, we nemen het supremum hierboven over een kleinere verzameling dan in (2).

Hilbert, Artin en Positivstellensätze
Is de ondergens $\mathrm{svk} \leq \mathrm{opt}$ in het algemeen scherp? Anders gezegd, heeft elk niet-negatief polynoom een som-van-kwadraten-certificaat? Deze vraag werd al in de late 19e eeuw gesteld door Hilbert. Hij liet zien dat dit niet het geval is: voor $n \geq 2$ is de inclusie $\Sigma \subsetneq \mathcal{P}(\mathbb{R}^n)$ strict, en bijgevolg bestaan er polynomiale optimalisatieproblemen (met $\mathcal{X} = \mathbb{R}^n$) waar $\mathrm{svk} < \mathrm{opt}$. Hilbert's bewijs is niet constructief, en het eerste expliciete voorbeeld van een polynoom $p \in \mathcal{P}(\mathbb{R}^n) \setminus \Sigma$ werd pas in 1957 gevonden door Motzkin, zie Figuur 1.
Gelukkig verbetert de situatie wanneer we voorwaarden toevoegen: Putinar [7] bewees in 1993 dat, wanneer $\mathcal{X}$ compact is, elk *positief* polynoom op $\mathcal{X}$ een som-van-kwadraten certificaat heeft.

Stelling (Putinar's Positivstellensatz)
Neem aan dat $\mathcal{X} \subseteq \mathbb{R}^n$ compact [10] is. Laat $\mathcal{P}_{>0}(\mathcal{X})$ de verzameling van (strikt) positieve polynomen op $\mathcal{X}$. Dan geldt dat

$$\mathcal{P}_{>0}(\mathcal{X}) \subseteq Q(\mathcal{X}).$$

Hieruit volgt dat $\mathrm{svk} = \mathrm{opt}$ voor polynomiale optimalisatieproblemen over $\mathcal{X}$.

Stellingen van dit type worden *Positivstellensätze* genoemd, een verwijzing naar Hilbert's bekende *Nullstellensatz*. Ze laten net als de Nullstellensatz een correspondentie zien tussen een *meetkundige* eigenschap van polynomen (positiviteit) en een *algebraisch* object (het kwadratisch moduul). Overigens bewees Artin [1] in 1927 al dat elk niet-negatieve polynoom op $\mathbb{R}^n$ geschreven kan worden als som van *rationale* kwadraten, dat wil zeggen

$$p(x) = \frac{p_1(x)^2}{q_1(x)^2} + \frac{p_2(x)^2}{q_2(x)^2} + \ldots + \frac{p_\ell(x)^2}{q_\ell(x)^2}.$$

Hiermee loste hij destijds het 17e van Hilbert's lijst van 23 problemen op. De Positivstellensatz van Krivine [4] en Stengle [9] veralgemeniseert dit resultaat naar niet-negatieve polynomen over verzamelingen $\mathcal{X} \subseteq \mathbb{R}^n$. Rationale certificaten zijn echter computationeel lastig om mee te werken, en leiden derhalve niet tot efficiënte algoritmen. We laten ze daarom verder buiten beschouwing.

Efficiënte benaderingsalgoritmen
We hebben gezien dat polynomiale optimalisatie over compacte verzamelingen $\mathcal{X}$ kan worden gereduceerd naar de optimalisatie van een eenvoudige (lineare) functie over het kwadratisch moduul $Q(\mathcal{X})$, bestaande uit polynomen met een som-van-kwadraten certificaat (3). Op zichzelf is nu nog niet duidelijk hoe dit tot *efficiënte* algoritmen zou leiden. Het is namelijk niet duidelijk of eenvoudig kan worden gecontroleerd of een gegeven polynoom p zo'n certificaat heeft. Sterker nog, het is zeer onwaarschijnlijk dat efficiënt kan worden nagegaan of $p \in Q(\mathcal{X})$! We hebben een laatste inzicht nodig van Lasserre [5] en van Parrilo [6]. Voor $r \in \mathbb{N}$ beschouwen zij het *begrensde* kwadratisch moduul $Q(\mathcal{X})_r \subseteq Q(\mathcal{X})$ dat bestaat uit polynomen met een som-van-kwadraten certificaat van *graad ten hoogste* r. Hiermee wordt bedoeld dat elk van de factoren $\sigma_0, \sigma_1, \ldots, \sigma_m \in \Sigma$ in het certificaat (3) graad ten hoogste r heeft. Nu blijkt dat, voor vaste r, efficiënt kan worden bepaald of $p \in Q(\mathcal{X})_r$ middels het oplossen van een zogenaamd *semidefiniet programma*. De benodigde rekenkracht om dit programma op te lossen hangt onder meer af van de gekozen graad r. De conclusie van Lasserre en Parrilo is dat, wederom voor vaste r, de parameter

$$\mathrm{svk}_r := \sup_{\lambda \in \mathbb{R}} \{\lambda : f - \lambda \in Q(\mathcal{X})_r\}$$

efficiënt kan worden berekend. Tevens geldt dat

$$\mathrm{svk}_1 \leq \mathrm{svk}_2 \leq \mathrm{svk}_3 \leq \ldots \leq \mathrm{opt}.$$

Tot slot vertelt Putinar's Positivstellensatz ons dat

$$\lim_{r \to \infty} \mathrm{svk}_r = \mathrm{svk} = \mathrm{opt}$$

De rij $\mathrm{svk}_1, \mathrm{svk}_2, \ldots$ vormt daarmee een *convergente hiërarchie van ondergrenzen* op het optimum opt, waarvan iedere individuele term efficiënt kan worden berekend. Deze ondergrenzen staan bekend als de *som-van-kwadraten-hiërarchie* (of ook *Lassere's hierarchie*).

Foutmarges en quantitatieve Positivstellensätze
De vraag die centraal staat in mijn proefschrift is: *Hoe snel* convergeert de som-van-kwadraten-hiërarchie naar het ware optimum? Deze vraag kan zowel vanuit het perspectief van de optimalisatie of van de algebraïsche meetkunde worden geformuleerd: Binnen de optimalisatie is men geinteresseerd in de relatie tussen de graad r

van de certificaten (en daarmee de benodigde rekenkracht), en de *foutmarge* $\mathrm{opt}-\mathrm{svk}_r$ van de resulterende ondergrenzen. Binnen de algebraische meetkunde probeert men *quantitatieve* versies te bewijzen van Positivstellensätze, waarin de benodigde graad van certificaten wordt uitgedrukt in 'de mate van positiviteit' van een polynoom. In de afgelopen twee decennia zijn vanuit beide gemeenschappen tal van publicaties verschenen die deze vragen (gedeeltelijk) beantwoorden.

Een raamwerk voor snelle convergentie

In mijn proefschrift bewijs ik nieuwe stellingen over de convergentiesnelheid van Lasserre's hiërarchie voor optimalisatie over verzamelingen $\mathcal{X}$ met bepaalde *symmetrie*. Hieronder vallen de eenheidsbol, de standaardsimplex Δ^n, de kubus $[-1,1]^n$ en de Booleaanse kubus $\{-1,1\}^n$. Deze betrekkelijk eenvoudige domeinen omvatten desalniettemin veel van de fundamentele problemen die polynomiale optimalisatie motiveren. In deze bijzondere gevallen is het mogelijk sterke convergentiesnelheden te garanderen. Een voorbeeld:

Stelling (Slot 2022)
Voor optimalisatie over de eenheidsbol geldt dat

$$\mathrm{opt}-\mathrm{svk}_r = O(1/r^2)\ (r\to\infty).$$

Wanneer we het best beschikbare resultaat [2] voor *algemene* domeinen $\mathcal{X}$ direct op de eenheidsbol zouden toepassen, garandeert dit slechts een foutmarge in $O(1/\sqrt[10]{r})$ (een factor 20 verschil in de exponent). De belangrijkste bijdrage van mijn proefschrift is het ontwikkelen van een theoretisch raamwerk waarbinnen convergentiesnelheden voor elk van de bovengenoemde domeinen kunnen worden bewezen. Dit bouwt voort op eerder werk van Fang en Fawzi [3], die het geval $\mathcal{X}=S^{n-1}$ bestudeerden. Ter conclusie beschrijven we dit raamwerk (in zeer grove lijnen).

1. We definiëren een klasse $\mathcal{K}$ van lineaire operatoren op $\mathbb{R}[x]$ met de eigenschap dat, voor elke $K\in\mathcal{K}$,

$$K(\mathcal{P}(\mathcal{X}))\subseteq \mathcal{Q}(\mathcal{X})_r.$$

Dat wil zeggen, operatoren $K\in\mathcal{K}$ beelden niet-negatieve polynomen af op het (begrensde) kwadratisch moduul. Deze klasse bestaat uit bijzondere *convolutieoperatoren*, van de vorm

$$K{:}p\mapsto K\star p,\ \text{waar}$$
$$(K\star p)(x){:=}\int_{\mathcal{X}} p(y)K(x,y)\,dy.$$

Hier refereert K abusievelijk zowel naar een lineare operator, als naar een functie $\mathbb{R}^n\times\mathbb{R}^n\to\mathbb{R}$.

2. Binnen de klasse $\mathcal{K}$ gaan we op zoek naar een operator K die zich (bijna) gedraagt als de identiteit, dat wil zeggen $K\star p\approx p$. Als we zo een operator kunnen vinden, stelt ons dit in staat een certificaat voor $K\star p$ uit de vorige stap om te vormen tot een certificaat voor $p+\varepsilon$ betrekkelijk klein. Dit laat (ruwweg) zien dat de foutmarge van Lasserre's ondergrens svk_r ten hoogste ε is.

3. Om onze zoektocht te vereenvoudigen, maken we gebruik van de symmetrie van $\mathcal{X}$ om de speciale klasse van operatoren te karakteriseren. Kort gezegd kan de hele klasse worden gevat in termen van polynomen van één variabele. Deze beschrijving is het mooist in het geval van de eenheidssfeer. Daar bestaat de klasse uit alle operatoren van de vorm

$$(K\star p)(x)=\int_{S^{n-1}} p(y)\,q(x\cdot y)\,dy,$$

waar q een som van kwadraten in één variabele is.

4. Tot slot laten we zien dat 'de beste' operator $K\in\mathcal{K}$ gevonden kan worden door een relatief eenvoudig optimalisatieprobleem op te lossen over de ruimte van polynomen in één variabele. Door de juiste orthogonale basis voor deze ruimte te kiezen, kan dit probleem met de hand worden opgelost. Dit leidt dan uiteindelijk tot een convergentiesnelheid voor Lasserre's hiërarchie.

Stelling (Slot 2022)
De convergentiesnelheid van Lasserre's hiërarchie kan, in de aanwezigheid van voldoende symmetrie, worden beschreven in termen van het gedrag van klassieke orthogonale polynomen in één variabele.

Referenties en noten

1 E. Artin, Über die Zerlegung definiter Funktionen in Quadrate, *Abhandlungen aus dem Mathematischen Seminar der Universität Hamburg* 5, 1927.

2 L. Baldi and B. Mourrain, On moment approximation and the effective Putinar's Positivstellensatz, *Mathematical Programming* 200 (2023) 71–103.

3 K. Fang, H. Fawzi, The sum-of-squares hierarchy on the sphere, and applications in quantum information theory, *Mathematical Programming,* Series A 190 (2021) 331–360.

4 J.-L. Krivine, Anneaux préordonnés, *Journal d'Analyse Mathématique* 12 (1964) 307–326.

5 J.B. Lasserre, Global optimization with polynomials and the problem of moments, *SIAM Journal on Optimization*, 11(3), 796–817, 2001.

6 P.A. Parrilo, *Structured Semidefinite Programs and Semialgebraic Geometry Methods in Robustness and Optimization*, Ph.D. thesis, California Institute of Technology, 2000.

7 M. Putinar, Positive polynomials on compact semi-algebraic sets, *Indiana University Mathematics Journal* 42 (1993) 969–984.

8 L. Slot, *Asymptotic Analysis of Semidefinite Bounds for Polynomial Optimization and Independent Sets in Geometric Hypergraphs*, Ph.D. thesis, Tilburg University, 2022.

9 G. Stengle, A Nullstellensatz and a Positivstellensatz in Semialgebraic Geometry. *Mathematische Annalen*. 207(2) (1974) 87–97.

10 Om precies te zijn dienen de voorwaarden $g_1,g_2,\ldots g_m$ aan een zekere algebraische conditie te voldoen die compactheid van $\mathcal{X}$ impliceert, maar deze conditie kan in de context van optimalisatie zonder verlies van algemeenheid worden aangenomen, gegeven dat $\mathcal{X}$ compact is.

Marieke van Egmond Olf Jaïbi

In Memoriam I Bente Hilde Bakker (1989–2024)

Wie was Bente?

Bente Hilde Bakker beschouwde wiskunde als een kunstvorm. Creatief zowel als perfectionistisch voelde ze zich meer thuis bij de studie wiskunde aan de Vrije Universiteit dan op school. Ze was niet alleen getalenteerd in de wiskunde, maar bouwde ook zelf een fiets waarop ze reizen maakte. In deel I beschrijven Marieke van Egmond en Olf Jaïbi de levensloop van Bente.

Wie was Bente?

Bente Hilde Bakker werd geboren op 19 februari 1989 te Amersfoort. Ze was al op jonge leeftijd gefascineerd door de wereld en hoe deze werkte, en ontwikkelde vele interesses op allerhande gebieden. Van muziek tot techniek, van de natuur tot poëzie. Ze wilde altijd weten hoe en waarom iets zo was, de aanname 'dat het nou eenmaal zo werkte' was nooit voldoende.

Over haar schoolperiode sprak ze niet veel, school lag haar niet zo, ze vond liever zelf uit wat ze wilde weten op haar eigen manier. Nadat ze, na enige omzwervingen, had besloten wiskunde te gaan studeren aan de Vrije Universiteit bleek ze in de academische wereld met die instelling gelukkig stukken beter uit de voeten te kunnen. Wiskunde was voor haar een kunstvorm, die net als het maken van muziek uitdaagde tot creatief denken en verbeeldingskracht uitlokte. Ze kon haar perfectionistische aard erin kwijt.

Bente ging gebukt onder de zwaarte van het leven. Wiskunde, en de reizen die ze maakte op haar zelfgebouwde fiets, gaven haar houvast. Haar gedachten over haar werk in de wiskunde ervoer ze als een trein die haar eindeloos meevoerde, als een achtbaan wellicht. Ook toen ze ziek werd, en ervoor koos de strijd moedig te strijden.

Bente is tot ons aller verdriet op 11 juli 2024 overleden.

Bente Hilde Bakker

Stijn Maatje
Korteweg-de Vries Instituut voor Wiskunde
Universiteit van Amsterdam
stijnmaatje@gmail.com

History

Secret Communications: Enigma, Fialka and Rubicon

In October 2023, Raf Bocklandt and Stijn Maatje organized a visit to the Secret Communications exhibition of the Cryptomuseum for a visiting German school class. The Cryptomuseum is an online museum which provides information about everything to do with cryptography and espionage. While the museum itself is online, they do have a physical collection which they exhibit every few years. In this article Stijn Maatje will explore some personal highlights from the exhibition and tell the stories associated with these items.

Enigma

When talking about cryptographic equipment, we cannot omit the Enigma machine, which is arguably the most important cryptographic device from the 20th century. It was by used by Nazi Germany in the 1930s and 1940s to encrypt almost all military communication. If the Allies were to break this encryption, they would have access to incredibly valuable information which could help them in the war effort.

To understand the story of Enigma, we have to go back to the First World War. The Netherlands were neutral and wanted to remain neutral in this war. Belgian and German ships entering Dutch waters were closely watched to prevent smuggling. The tension between the countries was high.

Meanwhile, on the other side of the globe, maintaining neutrality in the Dutch East Indies proved to be difficult. The navy squadron there was small (only about ten ships) and would be obliterated if it were to engage in battle. The Dutch East Indies was an archipelago consisting of thousands of islands which were difficult to monitor with such a small fleet. Germany took advantage of this by building illegal refueling stations on some islands. This, in turn, provoked British, French and Japanese warships to patrol the surrounding area. This was a violation of Dutch neutrality, but the Dutch squadron present could not withstand the power of the larger fleets in the area, so declaring war was not really an option unless the situation escalated even more. It also wasn't always clear how to react to certain circumstances, since it may not be the smartest decision to start a war by following orders too strictly. To prevent this, the commander of the squadron was only allowed to act with permission from the Commander of the Navy in Batavia, the capital of the Dutch East Indies at the time.

The need of a secure communications link between the squadron and Batavia was very much needed. Back in the Netherlands, at the Navy Academy in Willemsoord, Den Helder, two sea lieutenants working at the naval base, Theo van Hengel and Rudolf Spengler, were tasked with creating a cipher machine to be used in the Dutch East Indies. Unfortunately, the drawings of their design have been lost to time and no machine was saved either. A description of the machine survives:

> "The machine is quite heavy and bulky, bearing a standard typewriter keyboard for input. It consisted of four rotors which were driven by four geared wheels. The four drive wheels each drove one rotor and were grapped in their number of teeth [...]. The rotor movement was quite irregular looking because rotors paused whenever they encountered a gapped sector of their drive wheel [...] ." [8]

The machine was never patented by Spengler and van Hengel, since they couldn't agree with the Navy Minister, Hendrik Bijleveld, about who owned the patent: Spengler and van Hengel or the Dutch Navy [14].

One country over, in Germany, an engineer called Arthur Scherbius also invented a cipher machine based on rotors, similar to the machine invented by Spengler and Van Hengel. He filed for a patent for this machine in 1918, and called his machine *Enigma*, Greek for 'riddle'. The machine itself resembled a typewriter, but with some notable differences. A keyboard was present to type a plaintext messages, the *Tastatur*. When a letter on this keyboard was pressed, a mechanical system of rotors was then set in motion and an electrical signal could flow through the machine, ultimately lighting up a light bulb on the *Lampenfeld*, corresponding to another letter. This is how messages were encryp-

An Enigma I machine. The plugboard can be seen on the front of the machine. The keyboard and lampboard are located on top of the machine. Above the lampboard are three little windows, through which one can see the current configuration of the rotors.

ted on the Enigma machine, and this is how the machine works and looks to the layman's eye. However, a deeper dive into the inner workings of the machine reveals some interesting mathematics.

Internally, the Enigma machine consists of turning rotors. A single rotor on the Enigma machine has 26 inputs contacts which are connected internally with 26 output contacts. Mathematically speaking, a rotor is just an element of the symmetric group on 26 letters, S_{26}. Only using this permutation as encryption is not very safe: it is a mono-alphabetic substitution, which can be cracked very easily using frequency analysis, a method devised by polymath Al-Kindi in the 9th century. Instead, we can turn the rotor after each letter we encrypt, changing the nature of the monoalphabetic substitution, and turning it into a polyalphabetic substitution of period 26 [11].

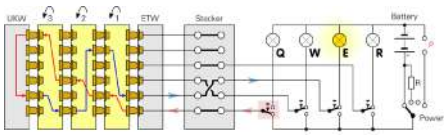
For example, let's imagine we are using an alphabet consisting of 6 letters. The wiring of the rotor inside is an element of the symmetric group on 6 letters, S_6, for example $\sigma = (aeb)(d)(cf)$. If we want to encrypt the word $cafe$ we determine $\sigma(c) = f$, after which the rotor turns one sixth of a full revolution. Mathematically, we can simulate this by including an extra permutation $\rho = (abcdef)$. To encrypt the second letter we determine $\rho\sigma\rho^{-1}(a) = f$. In general, to encrypt the i-th letter we determine its image under $\rho^{i-1}\sigma\rho^{-(i-1)}$. So in our simple one-rotor system $cafe$ gets encrypted as $ffed$. This is slightly different from the Enigma machine, where the internal mechanism already turns the rotor while pressing a button, so the encryption of the i-th letter is actually its image under $\rho^{i}\sigma\rho^{-i}$ [7].

The Enigma machine is slightly more complex than the machine described above. In fact, over the years multiple versions of the Enigma machine have been made, so there is no such thing as *the* Enigma machine. For now, we will look at the *Enigma I*, the most common version of the Enigma machine, which was introduced in 1930. More than 20,000 machines of this type were manufactured, and it was used by the *Heer* (Army) and the *Luftwaffe* (Air Force), and later adopted by the *Kriegsmarine* (Navy) as well. We will briefly explore some other types of Enigma machines as well.

In the Enigma I, there are three rotors (*Walzen*) in the machine, working as an odometer in a car, or as hands on a clock. After a button press, only the right-most rotor turns one 26th of a full revolution. The middle rotor only turns once the right-most rotor completed a full revolution, roughly once every 26 letter presses. The left-most rotor only turns once the middle rotor completed a full revolution, roughly once every 676 letter presses.

After a button press, an electric signal travels through these rotors, arriving at an essential part of the Enigma machine: the reflector (*Umkehrwalze*). When a signal enters the reflector, it sends an output signal through another letter, which is then sent through the rotors once more, essentially acting a sort of mirror.

The reflector is essential to the practicality of sending and receiving messages on the Enigma machine. As a permutation, the reflector is a product of 13 transpositions. Since the signal of a button press travels through the exact same rotors on the way to the reflector, as the way out of the reflector, a single setting of the Enigma machine can be viewed as a conjugation of the reflector. Since conjugation doesn't change the type of permutation, a single setting of the Enigma machine is also a product of 13 transpositions. This makes it easy to encrypt and decrypt: whenever a message is encrypted, the machine is set using the daily key and the message is typed in. To decrypt, the encrypted message can be typed in on the Enigma machine using the exact same setting that was used to encrypt the message. Since the rotors of the machine will turn in exactly the same manner in decrypting as in encrypting, and since every setting of the Enigma machine consists of only transpositions, the original message will appear. An important side effect of the reflector is that a letter can never be encrypted to itself, a fact that will become important later.

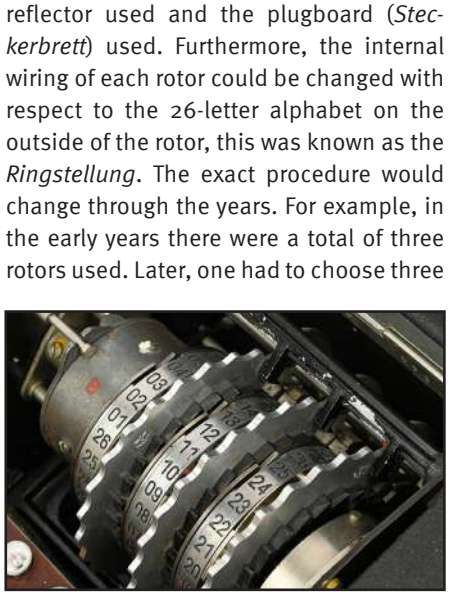


A simplified schematic of the Enigma machine.

The Enigma machine as described above is how Scherbius sold the machine for commercial use. Banks, police and companies all have interest in being able to communicate sensitive information securely. For the military version, the *Wehrmacht* added something extra: before the signal of a button press travels through the rotors, it enters the plugboard, located at the front of the machine. The plugboard is a board of all 26 letters, where cables can be used to connect two letters. This has the effect of swapping two letters before a signal enters the rotors, or after a signal leaves the rotors. In early procedures (1931-1937) six cables were used, while in later procedures (1940-1945) ten cables were used [11].

The plugboard offers an enormous amount of starting possibilities [16]. This was one of the reasons the Germans thought Enigma to be unbreakable. It is notable that the number of possible plugboard settings is highest using eleven cables, though the Germans never used eleven cables to decrypt messages.

To decrypt an Enigma message, one needs to know the basic setting of the machine. This is the setting of the machine when encryption starts and acts as the key of the message. The key consisted of the order of the rotors (*Walzenlage*), the basic setting of the rotors (*Grundstellung*), the reflector used and the plugboard (*Steckerbrett*) used. Furthermore, the internal wiring of each rotor could be changed with respect to the 26-letter alphabet on the outside of the rotor, this was known as the *Ringstellung*. The exact procedure would change through the years. For example, in the early years there were a total of three rotors used. Later, one had to choose three



A closeup of the rotors of the Enigma machine. Sometimes the numbers 01-26 would be used instead of the letters A-Z.

rotors out of a total of five - and for the Navy even eight - different rotors. Making some assumptions, the total size of the key space is in the order of 10^{20}. The key would change every day, known to all Enigma operators. Brute forcing the key was an impossible task. Since the contents of the message were highly time sensitive, it was key to obtain the daily key as fast as possible. Clever linguists and mathematicians were needed to exploit structure or mistakes introduced into the encryption process [11].

In later years, many versions of the Enigma machine would arise, some significantly more difficult (but not impossible) to break. The Kriegsmarine would unexpectedly adopt the Enigma M4 in 1942 which used four rotors instead of three, with added complexity by the addition of a rotating reflector. Some versions (Enigma T, Enigma A28, Enigma G) had rotors that stepped more often and more irregularly, making the ciphertext much less predictable [13].

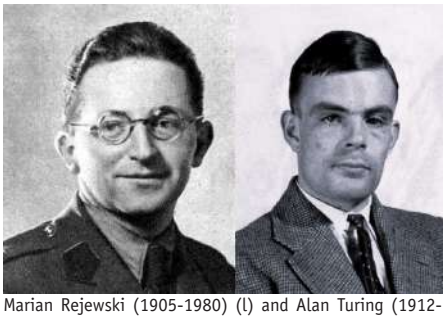
After winning the Polish-Soviet war (1918-1921), the Polish government decided to found a cryptographic bureau in the interwar years, the *Biuro Szyfrów*, in Warsaw. The Polish-Russian war was won, partly because of the codebreaking capabilities of the Polish. The Biuro had two main goals: to determine the internal wiring of the rotors, and to develop a fast, reliable way to decipher Enigma messages. One of the mathematicians employed at the Biuro was Marian Rejewski (1905-1980), who would ultimately be responsible for cracking Enigma.

Little was known to the public about German cryptography. The only information available to Rejewski was intercepted messages from Germany, which were still encrypted. At this point in time, Rejewski roughly knew how the Enigma machine worked, but no information about the internal wiring of the rotors or reflectors was known to him. To determine the wiring of the rotors, Rejewski used basic permutation theory, some information from espionage and exploited the laziness of Enigma operators and insecurities of Enigma procedures. After this, he could deduce the internals of the Enigma machine, which could then be used to build replicas of the machine, to be studied further. Since Rejewski only used the ciphertext, he employed a *ciphertext-only attack*.

This technique could then also be used to determine the daily key. To aid them in determining this key, Rejewski and his colleagues invented a machine called the *bomba kryptologiczna* and built one for each possible order of the rotors. Since the Germans used a total of three possible rotors, there were $3! = 6$ possible orders. In 1933, the Bomba was used together with other techniques to find the daily key in ten to twenty minutes. This means that in the year that Hitler came to power, the Polish had already cracked Enigma [1].

To prepare for the War, the Germans changed the procedures of Enigma, which meant the codebreaking techniques employed by the Poles would no longer work. Fearing they might soon be invaded, the Polish met with the French and the British, and gave them all of their code breaking efforts: blueprints, mathematical analyses, etc. The British brought all of this to the intelligence bureau of the United Kingdom, the Government Code and Cipher School (GC&CS). Preparations for an outbreak of war were already underway and GC&CS had recently moved to an estate just an hour north of London, to Bletchley Park. Just far away enough from London to avoid bombings, but strategically located equidistant between Cambridge and Oxford, where much of Bletchley's workforce would be coming from [13].

One of the mathematicians working at Bletchley Park was Alan Turing (1912-1954). Turing devised a alternative technique to crack Enigma messages. Turing's technique exploited the biggest weakness of Enigma: humans. In the encryption procedure, Enigma operators often had to use a random string of three letters. Since they would send many messages each day, they usually opted for easy to generate strings, which resulted in predictable strings like `ABC`, `AAA` or `QWE`. The German army also had to report when all was quiet, which resulted in predictable messages like `KEINEX-BESONDERENXVORKOMMISSE`. When intercepting a message the exact location could also be determined using triangulation. Combining this with the fact that the first message of the day at 6 a.m. would often be the weather forecast, one could expect to see messages like `WETTERVORHERSA-GEXBISKAYA` for the weather forecast of the Bay of Biscay. This (educated) guess of the plaintext is called a *crib*, making this type of attack a *known-plaintext attack*.



Marian Rejewski (1905-1980) (l) and Alan Turing (1912-1954) (r).

After finding a probable crib, one could use the fact that a letter can never be encrypted to itself to determine where in the ciphertext this crib would occur, known as the *depth* of the crib. This is the guess of what part of the ciphertext corresponds with the plaintext. From this correspondence a special graph called a *menu* was made. The vertices of this graph are the letters in the crib, and we draw lines between the i-th letter of the ciphertext and the i-th letter of the crib.

For example, we intercepted a message which we think is about general Rommel, and we think that in this message, `JTGEF-PG` corresponds with `ROMMELF`. We can then draw the following menu:

A machine called the *Bombe* could then be set according to this menu. The Bombe was an invention by Turing, and it was improved upon by Gordon Welchman. Given a menu, it brute forced possible Enigma setting in a clever manner, essentially doing a proof by contradiction electrically. When the Bombe had found a possible setting, it would stop and the operator would note the position the Bombe stopped at and would then let the machine continue. There might be multiple possible Enigma settings for a given menu, but only one of these would correctly decrypt the original message. One could greatly improve the Bombe's accuracy by choosing a crib that yielded a menu with more cycles. This eliminated an enormous number of possible settings.

The Bombe was used together with countless other techniques (Banburismus, Rodding, etc.) to determine the daily key. The first Bombe prototype *Victory*, cost one hundred thousand pounds to build and took a week to find the right key. After some refining, a proper Bombe, called *Ag-*

The Bombe was set according to a menu, and would stop when it had found a possible solution.

nus Dei, was built and took only an hour to find the right key [13].

The people of Bletchley Park

Nowadays, everybody rightfully celebrates Alan Turing as one the most important mathematicians at Bletchley Park. It is however also important to note that cracking Enigma was far from an individual achievement. In fact, on the height of its success, around ten thousand people were employed at Bletchley Park, with around three quarters of them being women [15]. I want to highlight two people who worked at Bletchley Park, who, in my view, embody the spirit of codebreakers at Bletchley Park: Dillwyn (Dilly) Knox (1884-1943) and Mavis Batey, née Lever (1921-2013). To get an idea of the type of people working at Bletchley Park, this excerpt from the biography of senior codebreaker Emily Anderson gives an idea:

> "A lifelong proponent of teamwork and synergy, Denniston [Commander Alastair Denniston (1881 - 1961), head of GC&CS] had, from the outset, provided an environment that encouraged individuality and harnessed it to enable a disparate team of often quirky individuals to work successfully towards a common goal. [...] Denniston recruited prospective cryptographers and cryptanalysts irrespective of their age, gender or background, valuing talent and potential above all else. Experience had shown that codebreakers had to be able to think laterally. Dilly Knox, for example, brilliant but a noted eccentric, had been known for doing most of his thinking sitting in the bathtub installed in his office in MI1(b) [the army's intelligence division during the First World War]." [2]

During the First World War, Knox helped decrypt the famous Zimmerman Telegram which resulted in the involvement of the United States in the War. During the Second World War, Knox founded his own department: *Intelligence Services Knox* (ISK). Everybody at Bletchley Park referred to the unit as *Dilly's Fillies*, since Knox only wanted to employ female codebreakers. Mavis Batey, who would later write Knox's biography, explained:

> "Dilly chose people who were language orientated. There was an actress, and some girls who'd been at drama school and they were quite glamorous, but they also understood rhythms and patterns of speech. Dilly was always looking for rhythms and patterns. There were linguists like me, and one girl was a speech therapist. We were always referred to as 'Dilly's Girls' or 'Dilly's Fillies', even in places like Whitehall, but he chose us because he liked the fact we were intelligent, made good coffee, and we could pick up his ideas and work on them while he came up with more. It was no use asking the mathematicians because they were too busy with their own ideas. But we could give him the attention he needed and try to pin down his ideas and try them. Some worked, some didn't, but he was never short of them. He was an extraordinary man." [2]

Knox's unit focused on cracking the versions of Enigma which could not be cracked using techniques developed by other departments such as Hut 8, which was Alan Turing's unit.

Mavis Batey arrived at Bletchley Park when she was just 19 years old. When she arrived at the ISK unit, Knox said to her: '*Oh, hello, we're breaking machines, have you got a pencil?*' [12]. She was then thrown in the deep end and had to figure out herself what to do. Her first result came very quickly. Knox himself had previously cracked the version of Enigma used by the Italian Navy, which was notoriously difficult to crack. This version had since become unreadable by some procedural changes from the Italians. In the new procedure messages had to be of a certain length. When reading the ciphertext of an intercepted message, Batey noticed that the second part of the message didn't contain any L's. Knowing that on an Enigma machine a letter cannot be encrypted to itself, she suspected that the sender of the message had repeatedly pressed the L to pad the original messages. Sure enough the key could be recovered and the plaintext could be read: *Today's the day minus three*. After waiting three days, a very long message came in, detailing a planned attack on a Royal Navy convoy carrying supplies from Cairo to Greece. An attack was planned by the British and thanks to the information supplied by Batey; it was a landslide victory. After that, the Italians never attacked the Royal Navy in the Mediterranean again. Following this victory, Knox wrote the following 'epitaph to Mussolini':

> "These have knelled your fall and ruin, but your ears were far away. English lassies rustling papers through the sodden Bletchley day." [2]

Batey's biggest contribution was a collaboration with Knox and Marget Rock, another leading female codebreaker. The Enigma G was a version of Enigma mainly used by the German intelligence Agency (Abwehr). In the 'normal' version of Enigma, a notch was present on each rotor so the rotor to the left of it would advance by one position every revolution. Enigma G had rotors with 11, 15 and 17 notches (all coprime), making rotor movements much more unpredictable. In addition to this, the reflector which is stationary in Enigma I also turns in the Enigma G. The department tasked with cracking Army and Air Force Enigma machines, Hut 6, lead by Gordon Welchman, could not crack this version of Enigma and deemed it unbreakable. At this point, the problem was forwarded to ISK where, on 8 December 1941, Mavis Batey broke a message intercepted from Belgrade. This allowed them to reconstruct part of the machine and break Enigma G.

Breaking Enigma G was an important step in the way the war would progress. The British now knew exactly how to decrypt Enigma G messages, but also how to encrypt messages. The British security services MI5 and MI6 came up with a plan to feed false information to the German intelligence agency by encrypting it using Enigma and sending it as if it came from a German source, essentially creating fake news. This scheme was known as the Double-Cross System (XX System), which would play a hugely important role in Operation Fortitude. The Germans were fed information that the Normandy landings of 1944 (D-Day) would take place in

Calais, where the Channel is at its narrowest, when in fact they would take place in Normandy, hundreds of kilometers to the south. This meant that a significant portion of the German Army was stationed at Calais. Since the British could now read Enigma G messages, they knew for a fact the Germans believed the deception and that the Normandy landings could take place as planned, without much resistance.

The intelligence gathered at Bletchley Park was codenamed *ULTRA* and was instrumental in the victory of the Allies in the War. At the start of the war Churchill was sure he could win the battle on land and in the air, but he feared the Battle of the Atlantic, since German U-boats employed very sophisticated attack tactics which were difficult to predict. Churchill credits the Ultra intelligence gathered at Bletchley Park as the reason the Allies won on sea. Even early on in the war Churchill recognized the importance of the codebreakers at Bletchley, calling them *the geese who laid golden eggs and never cackled*. When the codebreakers at Bletchley felt they were understaffed in important sections, they asked Churchill for more personnel, to which he replied with a now famous memo:

> "ACTION THIS DAY: Make sure they have all they want on extreme priority and report to me that this has been done." [3]

Fialka

During and after the Second World War, the USSR gathered intelligence from espionage about Enigma and started development on their own cryptographic machine. After two years of development, this resulted in the introduction of a new machine in 1956 based on the Enigma machine: the M-125, codenamed FIALKA (ФИАЛКА)[17]. The Soviets noted all flaws present in the Enigma machine and improved every single one of them. Fialka was used by the Soviets well into the 1990s.

Mavis Batey (1921-2013) (l) and Dilly Knox (1884-1943) (r). Batey would later write Knox's biography 'Dilly, the man who broke Enigma'.

The Enigma keyboard used the Latin alphabet which consists of twenty-six letters. The Cyrillic alphabet used in the Russian language has thirty-three letters, but only thirty are present on the Fialka, where some less frequently used letters have been omitted. On a later version of Fialka a button was present where one could switch between the Latin and Cyrillic alphabet.

Broadly speaking, the working of the mechanism on the Fialka machine is similar to that of the Enigma machine. Once a letter on the keyboard has been pressed a signal is sent through some rotors, reflected in the reflector and sent back through the rotors. The lamps of the Enigma have been replaced by a printhead. Instead of having to write down each encrypted letter manually, each letter is automatically encoded using a Cyrillic version of the Baudot code. Every letter is encoded using five bits, and is punched on a standard teleprinter tape, which could then easily be transmitted by telegram. This way of encoding was much faster and less prone to human error than manually writing down letters and sending them with Morse code, as was done with Enigma.

The most obvious difference between the Enigma machine and the Fialka machine is the number of rotors: ten instead of three. Furthermore, adjacent rotors rotated in opposite direction. On every rotor of the Enigma machine, a notch was present so that a rotor could turn the rotor to the left of it after a full revolution. In practice, this meant that the left most rotor almost never turned during encryption, rendering it (almost) useless.

The turning mechanism on the Fialka machine worked slightly differently. One rotor didn't influence the movement of the rotor next to it, but was instead connected to the rotor next to that one. On the Enigma a single pin on a rotor controlled the stepping of the rotor next to it. On the Fialka numerous pins were present on a rotor, controlling the stepping of the rotor next to the rotors neighbor.

The M-125 Fialka

This increased size of the keyspace considerably and made the turning of the rotors highly irregular. The pins were present on the outer part of a rotor, while the inner part contained the actual wiring of the rotor. In 1978 new rotors were introduced where the inner wiring and outer pins could be separated and interchanged with other rotors, increasing the size of the keyspace once again.

One flaw of the Enigma machine was that a letter could never be encrypted to itself, which turned out to be an enormous vulnerability, exploited by the cryptanalysts at Bletchley Park. The Soviets solved this problem by slightly modifying the reflector. In the Enigma machine, the reflector is a product of thirteen transpositions. The Fialka utilized a thirty letter alphabet, so the naive equivalent of the Enigma reflector would be a product of fifteen transpositions. The Soviets, however, made a reflector which was a product of thirteen transpositions, one 3-cycle and one 1-cycle:

$$\rho = (А, Б)\ (Э, Г)\ \ldots\ (Ж, В, Ц)\ (Й).$$

Note that this 1-cycle makes it possible for a letter to encrypt to itself. Having a 3-cycle in the reflector meant that the encryption and decryption process became slightly more complicated. If the reflector above was used during encryption, the machine now has to make sure to invert this 3-cycle during decryption:

$$\rho^{-1} = (А, Б)\ (Э, Г)\ \ldots\ (Ж, Ц, В)\ (Й),$$

which could be easily done using a small electronic circuit.

The addition of the plugboard in the Enigma machine provided a lot of possible starting settings, increasing security. It was very tedious for an operator to use the plugboard, so for the Fialka, the Soviets thought of an easier equivalent, which was also more secure. Instead of physically connecting letters on a plugboard, a punchcard was used which could slide into the side of the machine. This punch-

The Fialka standard for 5-bit encoding of the Cyrillic alphabet.

card consisted of a 30×30 matrix, indexed by the letters of the alphabet. The operator received this punchcard in a sealed bag from the Soviet High Command with holes pre-punched. The punchcards were changed daily. A punched hole in this matrix represented a 1, signifying a swap of two letters. A 1 at position (i,j) lets the machine know to send input i to letter j. Every column and every row would have exactly one non-zero entry, which makes the punchcard a permutation matrix. Essentially, the punchcard is an additional (static) rotor with completely random wiring. Compare the $2.0 \cdot 10^{14}$ possible settings of the plugboard on the Enigma machine (with 11 cables) to the $30! \approx 2.7 \cdot 10^{32}$ possible settings of the punchcard, and you can understand why the Soviets opted for the latter option. When the punchcard was not in use, a metal triangle would be inserted into the machine: a physical identity matrix!

The use of punched tape on the Fialka made it much easier to work with than the Enigma machine. However, the Soviets noticed some flaws in the machine. When pressing a button, a certain chain of events is set in motion, unique to that button press. This means that every button press produces a different sound and by analyzing the acoustics one could figure out what buttons were pressed in what order. To prevent this, the mechanics of Fialka have been produced in such a way that every button press produces the exact same sound.

Another flaw was present in the way the tape was punched. Whenever a key is pressed, the paper puncher punches a letter on the paper tape. For example, when this letter is A the string 10000 is punched on the strip and when this letter is Д the string 11110 is punched on the strip. In the former case only one puncher is activated, while in the latter case four punchers are activated, drawing four times as much current from the power supply. One can analyze the current drawn by the machine to deduce how many punchers were activated by the keypress, which in turn gives valuable information about the printed letter. To overcome this, the Soviets modified the power supply to produce a stable amount of voltage, while also producing a constant current. In addition, they added a noise generator, which superimposes stochastic noise onto the power line to obfuscate any further hidden signals. This type of attack is called a *side channel attack*, and proves that when analyzing a cryptographic system, one should never only consider the mathematical framework, but also take outside factors into consideration.

The equivalent of the plugboard on the Fialka. Have you ever seen a physical identity matrix?!

The Soviets had a very strict protocol for using Fialka. Only the operator was allowed to use the machine, the sender or recipient were usually not allowed to operate the machine. On big military exercises, the machine was operated in a hut or tent where only a handful of people were allowed inside. The outside area was heavily guarded, everybody who entered the restricted area was in danger of being arrested or being shot on the spot.

The existence of Fialka was kept secret for many years, so little was known about the procedures and the internals of the machine. The first publication about Fialka, including a detailed description of the machine, was published in 2005 by Paul Reuvers and Marc Simons of the Cryptomuseum. To this day, little research has been done about the Fialka and its security, so no successful attack is known, but in 1989 it was believed by Russian cryptologists that Fialka messages could be cracked within 24 hours. This was possible, since Israel captured some Fialka machines during the Six Day War in 1967. Furthermore, the American National Security Agency (NSA) had supercomputers running special Fialka cracking software in the 1970s and there is also proof that the Austrians decrypted a substantial amount of Fialka traffic.

Every country in the Warsaw Pact had their own version of Fialka, with different wired rotors than the other countries. This was because the Soviets didn't want countries to communicate amongst themselves, without informing Moscow first. After the collapse of the Soviet Union all Fialka machines were ordered to be destroyed. The machines were thrown on big piles and would then be set on fire. Most Fialka machines were destroyed in fires or by simply smashing them. There are, however, multiple stories of officers coming to oversee the destruction process, getting intoxicated with alcohol, and not noticing some unburned machines deeper in the stack being sneaked out of the fire. The Cryptomuseum has a fully restored and working Fialka M-125 from Russia, which is (as far as we know) one of only two Fialka machines in the West with Russian wired rotors [10].

Operation Rubicon

The United States and the Soviet Union were constantly spying on each other during the entire Cold War. This made the use of good encryption more important than ever.

Russian-born Swede Boris Hagelin (1892-1983) founded Crypto AG in 1952 to produce cryptographic and communications equipment. Unlike the Enigma, most of Hagelin's machines were pinwheel machines, where mechanical pins would decide the stepping of the machine, making it purely mechanical and therefore ideal to use in the field. Hagelin based his company in neutral Switzerland and provided cryptographic equipment to more than 120 countries in both the Eastern and Western Bloc.

During World War II, Hagelin sold the rights to his M-209 pinwheel machine to the United States for over eight million dollars [18]. This deal solidified the relationship between Hagelin and the United States.

One of the people who Hagelin had good relations with, was American cryptographer William Friedman (1891-1969) [19], who would later become known as 'the dean of cryptography'. Since Friedman was also born in Russia, the two quickly bonded and became good friends. In 1949 Friedman became head of the cryptographic division of Armed Forces Security Agency (AFSA) until 1952, in which the organization was succeeded by the National Security Agency (NSA), where Friedman also became chief cryptologist.

The United States had released large quantities of the M-209 machines to be sold for as little as fifteen dollars for use in other countries. Many of these machines were bought by South American countries.

Boris Hagelin (1892-1983)

Meanwhile, the NSA started development on a machine (WARLOCK) designed to crack messages encrypted on pinwheel devices.

In 1954 Hagelin was working on a new pinwheel machine called the CX-52 with very unpredictable cryptographic behavior, making it very cryptographically secure. The NSA did not like this. They benefited from other countries using cryptographic equipment which was secure, but not too secure, since that would hinder the breaking of this equipment using their relatively powerful computers, and thus hinder their ability to gather intelligence to use against the Eastern Bloc. Part of Friedman's job was to identify cryptographic developments that would pose risks to the stream of intelligence coming into the NSA and CIA.

Friedman was sent to negotiate with Hagelin, and more than a year later, in February 1955, they agreed on a deal between Hagelin and the NSA. This deal was called 'the Gentleman's agreement'. Hagelin did not want anything to be written down. Still, the agreement had to be authorized by the director of the NSA. This authorization is still classified, but we know the contents of the deal. Although Hagelin would not be paid for this deal, the US Army would be using his cryptographic equipment. Furthermore, we can assume he and his family would receive personal favors from the NSA, like job offers at the NSA or US army. In return, the NSA would provide Hagelin with a list of countries, to which he was not allowed to sell his most sophisticated equipment. The loss of sales would be compensated: Hagelin received seven hundred thousand dollars up front. The countries that Hagelin was allowed to sell to, would receive manuals written by the NSA. NATO countries, however, would receive a different manual, detailing how to 'properly' use the machine. For example, if one were to follow the procedure in the CX-52 manuals provided to non-NATO countries, the cryptographic security would be significantly smaller than if one were to use a NATO manual. [4]

In 1957 Hagelin intended to retire, but the Americans did not want to lose control over Crypto AG. Hagelin discussed this matter with Friedman, saying that the only options he had was to either hand over the management to his son, Bo Hagelin, or to sell his company to Siemens (which Hagelin had considered before). Then Friedman reminded him of a third option: sell his company to the Americans. After exploring several options, the CIA offered a licensing agreement, which essentially formalized the Gentleman's agreement from a few years prior. In addition, Hagelin would receive six hundred thousand dollars, plus an annual bonus of seventy-five thousand dollars. This operation was codenamed SPARTAN.

In the coming years, it became clearer and clearer that mechanical cryptographic equipment would soon be replaced by electronic cryptographic equipment. Instead of mechanical rotors like in the Enigma and Fialka machines, a shift register would be used, which is roughly the electronic equivalent of the rotors from early twentieth century cipher machines and can be used to quickly generate a pseudo random stream of bits.

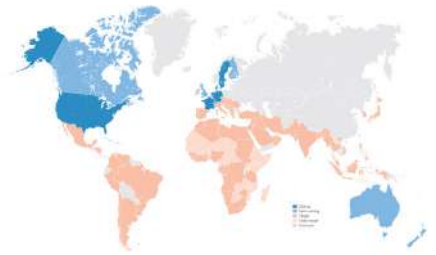
From 1965 onwards Crypto AG focused on electronic cryptographic equipment, since it would otherwise lose business to other manufacturers. Peter Jenks (1924-1989) was cryptanalyst at the NSA and came up with a way to make shift registers which looked pseudo random, but actually inhabited much structure, which could be exploited by NSA cryptographers. These algorithms could then be used in Hagelin's equipment to be sold worldwide. This was the beginning of a closer working relationship between the NSA and Hagelin.

Then, in 1970, using a complex scheme of hard to trace companies and fiduciaries, the German *Bundesnachrichtendienst* (BND) and the American Central Intelligence Agency (CIA) bought Crypto AG in secret from Hagelin, for around seven million dollars. This joint project would be codenamed THESAURUS (treasury) and was changed in 1987 to RUBICON (point of no return). For the purposes of RUBICON, the CIA worked closely together with the NSA to develop algorithms to be put on Crypto AG equipment [6].

Crypto AG controlled 80-90% of all cipher equipment used worldwide, partly because the agreement that no Crypto AG equipment could be used by NATO countries was forfeited. The NSA could read about 57% of all intercepted messages. In comparison: without operation THESAURUS this would be less than 29%. By the 1980s, a mere 10 years after the start of operation THESAURUS, the NSA could read 96% of all messages sent through Crypto AG machines. A CIA report on the evaluation of operation THESAURUS concludes with *'It was the intelligence coup of the century'* [9].

An operation of this scale would surely not go unnoticed, right? Some codebreaking organizations, like the British GCHQ, received intelligence from the United States, but were not aware of operation THESAURUS/RUBICON. Other countries, like Denmark, France, Israel, Sweden and the Netherlands were informed by the NSA and BND how to crack certain Crypto AG equipment, but were not informed about the scale of the operation. In 2020, Bart Jacobs, a Dutch Professor of Security, Privacy and Identity at the Radboud University, revealed that a codebreaking alliance between Denmark, Sweden, Germany, the Netherlands and France, codenamed MAXIMATOR, was established in 1976. Information about operation THESAURUS/RUBICON was presumably also shared amongst the countries in this alliance [5].

In 1992 a sales representative of Crypto AG, Hans Bühler, flew to Iran on a business trip. While in Iran, Bühler was arrested by the Iranian authorities for spying, bribery, illegal contacts and illegal use of alcohol. The CIA didn't know what Bühler knew about operation RUBICON, and they were afraid he would make incriminating statements. The decision was made to pay the full million dollars of bail. Crypto AG itself didn't have the funds to pay this bail, so the BND and CIA had to come up with the money themselves. The BND was prepared to pay half of the money, but the CIA



The witting countries (blue) can be seen, as well as countries which we know for certain were targeted by operation THESAURUS/RUBICON (pink). [4]

was afraid it was illegal. Eventually the CIA agreed to pay their share, but this plan was later rejected by the White House. Months later, the BND paid all the money to the Iranian authorities and Bühler was released. Bühler felt that Crypto AG had not done enough to release him and accused Crypto AG of selling equipment with a weakened algorithm. The German *Bundespolizei* conducted several investigations regarding Crypto AG, but no evidence for Bühler's claims could be found. In the years to come, Bühler would accuse the BND to be the secret owners of Crypto AG.

This series of events was later dubbed 'The Hans Bühler Affair', codenamed HYDRA, and permanently damaged the relationship between the CIA and BND. In 1994 the BND backed out of operation RUBICON, making the CIA the sole owners of Crypto AG.

The CIA's ownership continued until 2018, when Crypto AG was bought by Swedish entrepreneur Andreas Linde and split into two companies. The old Crypto AG no longer exists. In February 2020 operation RUBICON was revealed to the public after an extensive two-year investigation of German, Swiss and American journalists [9].

The story of Crypto AG proves the need to do cryptography according to Kerckhoffs's principle: the security of a cryptosystem should never come from the secrecy of the algorithm, only of the secrecy of the key: the algorithm used should always be public knowledge. The Cryptomuseum has a lot of Crypto AG equipment which has been backdoored.

Closing Remarks

These stories about cryptography are already interesting on their own, but the fact that the Cryptomuseum has so many artifacts which make the stories tangible and come alive, elevates them to another level. The students did not only listen to me talk about Enigma, they actively participated in discussions with me and the people from the Cryptomuseum. They were curious, asked interesting questions and learned about the history of cryptography, and with that, about the importance of cryptography. After the class had sailed back to Germany, Raf received an email from them thanking us for the day we organized, saying that they only talked about cryptography on the journey back home and that *'the highlight of our week was in a basement in Duivendrecht'*, which is the greatest compliment one can get.

Acknowledgements

The author would like to thank Paul Reuvers and Marc Simons of the Cryptomuseum in Eindhoven. Without them, none of this would have been possible. They opened the exhibition especially for us and answered all the students' questions with great enthusiasm and insight. They also took the time to proofread this article and allowed me to use their photographs of the machines.

Furthermore, my longtime friend Ruud Bos has given me valuable feedback on this article from his persepective as a student of history.

I would also like to express my gratitude to Anette Schröder and her students from the Ubbo-Emmius-Gymnasium in Leer, Germany, for taking an interest in the world of cryptography, asking good questions and being curious, for which I am incredibly grateful.

References and notes

1 F. L. Bauer, *The History of Information Security: A Comprehensive Handbook*, 381-446, Elsevier, 2007.

2 J. Uí Chionna, *Queen of Codes: The Secret Life of Emily Anderson, Britain's Greatest Female Codebreaker*, Headline, 2023.

3 A. Hodges, *Alan Turing: The Enigma*, Vintage, 2014.

4 Cryptomuseum, *Operation Rubicon: The secret purchase of Crypto AG by BND and CIA*, https://www.cryptomuseum.com/intel/cia/rubicon.htm, 2020.

5 B. Jacobs, European signals intelligence cooperation, from a Dutch perspective, *Intelligence and National Security* 35:5, 659-668, 2020.

6 H. Jaspers, *De cryptoleaks van CIA en BND: 'Dit was de inlichtingen-coup van de eeuw'*

7 R. Klima, N. Sigmon, *Cryptology: Classical and Modern*. Second Edition, CRC Press, 2019, https://www.vpro.nl/argos/lees/onderwerpen/cryptoleaks/2020/decryptoleaks-van-cia-en-bnd.html, Argos, 2020.

8 K. De Leeuw, *Dutch Invention of the Rotor Machine*, 1915-1923, Cryptologia 27:1, 73-94, 2003.

9 G. Miller, The intelligence coup of the century, *The Washington Post*, 2020.

10 P. Reuvers & M. Simons, *Fialka Reference Manual*, Cryptomuseum, 2005.

11 S. Singh, *The Code Book*, Anchor Books, 1999.

12 Mavis Batey Obituary, The Telegraph, 2013.

13 G. Welchman, *The Hut Six Story, M&M Baldwin*, 2023

14 Spengler and van Hengel accused another Dutchman, Hugo Alexander Koch, of stealing their drawings of the rotor machine and applying for a patent with those drawings. Unfortunately for them, Koch's brother-in-law, A.E. Jurriaanse, was partner in N.V. Vereenigde Octrooibureaux, the company responsible for giving out patents. Spengler and van Hengel took this matter to court, but more bad luck would come their way, since the court was presided by none other than former Navy Minister H. Bijleveld.

15 Many codebreakers at Bletchley Park would later become famous mathematicians. J.H.C Whitehead worked at Bletchley Park during the Second World War and would later become one of the founders of homotopy theory. William (Bill) Tutte would be instrumental in cracking the Lorenz cipher, which was used by Hitler and his high command. Tutte would later publish foundational work in matroid theory and algebraic graph theory, in which the Tutte polynomial was named after him.

16 A fun exercise is to calculate the number of possible plugboard settings using k cables, and to prove this is exactly the number of involutions that consist of k 2-cycles in the symmetric group S_{26}.

17 Like the Enigma, Fialka is not the name of a machine, but rather of the procedure itself. However, we will use the name Fialka throughout for clarity.

18 Adjusted for inflation, this is around $192 million in 2024.

19 Friedman was a very prolific cryptanalyst. Among other things, he first described the *Index of Coincidence* of a text, a statistic of a piece of text which could determine if a monoalphabetic or polyalphabetic cipher had been used to decrypt a text. Furthermore, if a polyalphabetic cipher had been used, the Index of Coincidence could be used to find the length of the keyword used during the encryption process.

Jan Bouwe van den Berg
Departement Wiskunde
VU Amsterdam
janbouwe@few.vu.nl

Hermen Jan Hupkes
Mathematisch Instituut
Universiteit Leiden
hhupkes@math.leidenuniv.nl

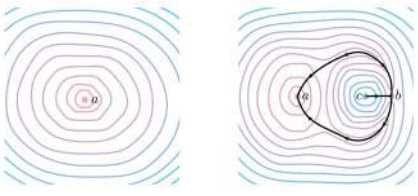
Roeland Merks
Wiskunde en Natuurwetenschappen
Universiteit Leiden
merksrmh@math.leidenuniv.nl

In Memoriam II Bente Hilde Bakker (1989–2024)

Bente als wiskundige

Bente Hilde Bakker beschouwde wiskunde als een kunstvorm. Creatief zowel als perfectionistisch voelde ze zich meer thuis bij de studie wiskunde aan de Vrije Universiteit dan op school. Ze was niet alleen getalenteerd in de wiskunde, maar bouwde ook zelf een fiets waarop ze reizen maakte. In deel II van deze In Memoriam beschrijven Jan Bouwe van den Berg, Hermen Jan Hupkes en Roeland Merks de wiskunde door Bente. De jury van de Stieltjesprijs merkten het uitzonderlijk hoge niveau van Bentes wiskunde op, en kenden haar daarom de prijs voor 2019-2020 toe. Ze bracht technieken uit de algebraïsche topologie over naar niet-lokale differentiaalvergelijkingen en schreef een uitgebreid softwarepakket voor mathematische biologie. Ze gaf enthousiast les aan studenten en 12 tot 16 jarigen, in de mathematische biologie en in de electro- en mechanotechniek.

Bente promoveerde aan de Vrije Universiteit onder begeleiding van Jan Bouwe van den Berg en Robert van der Vorst.
In haar proefschrift, getiteld 'Nonlinear waves in local and nonlocal media: A topological approach', ontwikkelde Bente een zeer creatieve en technische theorie die het mogelijk maakt om fundamentele Floer-Conley technieken die geworteld zijn in de algebraïsche-topologie, over te brengen naar de setting van niet-lokale differentiaalvergelijkingen. Deze aanpak opende de deur naar een beter wiskundig begrip van fundamentele zelforganiserende structuren zoals watergolven, lichtpulsen en spiraalvormige groeipatronen, die overal in de wereld om ons heen te zien zijn. De uitzonderlijke kwaliteit van haar werk leverde Bente de Stieltjesprijs 2019-2020 op, die jaarlijks wordt uitgereikt voor het beste proefschrift in de wiskunde verdedigd op een Nederlandse universiteit. In de woorden van één van de juryleden: 'Naar mijn mening is Bakkers proefschrift van een niveau dat je maar eens in een decennium ziet.'
In 2019 begon Bente bij de Universiteit Leiden waar zij drie jaar als postdoc werkte. Vanaf de start was zij gedreven om te ontdekken hoe andere wetenschappelijke disciplines konden profiteren van haar abstracte wiskundige perspectief. Dit resulteerde in diverse onderzoeksprojecten op het gebied van de mathematische biologie. Bente schreef bijvoorbeeld een uitgebreid softwarepakket dat helpt bij het begrijpen van de mechanische interactie tussen cellen en de omringende extracellulaire matrix, die een fundamentele rol speelt in het ontstaan van collectief celgedrag in weefsels. Het project haalde de voorkant van het Biophysical Journal en werd opgenomen in de Tissue Simulation Toolkit, die nog steeds wordt gebruikt en onderhouden op de Universiteit Leiden en vele andere plaatsen over de hele wereld. Door dit werk en haar andere bijdragen, die ze altijd graag met collega's wilde delen en bespreken, zullen veel onderzoekers profiteren van Bentes nalatenschap.
Bente besteedde regelmatig haar tijd aan het trainen van de volgende generatie wetenschappers en deed dit met veel enthousiasme. Zij begeleidde bijvoorbeeld een bachelorproject over het golfachtige transport van het fytohormoon auxine, dat een essentiële rol speelt bij de groei van planten. Naast een wetenschappelijke publicatie leidde dit tot een posterprijs voor de student, die goede herinneringen heeft aan het project en zijn carrière in de wetenschap voortzet. Ook coachte Bente 12 tot 16 jarigen in de electronica en de mechanica bij de technische hobbyclub De Jonge Onderzoekers in Amersfoort.
Onze gedachten gaan uit naar Marieke en Bentes familie en vrienden. Wij wensen hen kracht bij het dragen van dit diepe en voortijdige verlies. De wetenschappelijke gemeenschap heeft een zeer getalenteerd lid verloren en zij zal erg gemist worden.



Figuur 1.1 uit het proefschrift `Nonlinear waves in local and nonlocal media: A topological approach' door Bente Hilde Bakker

Otto van Koert
Department of Mathematical Sciences
Seoul National University
okoert@snu.ac.kr

Column Wiskundigen in den vreemde

Van Koert in Korea

In deze rubriek doen wiskundigen verslag van hun ervaringen als wetenschapper in den vreemde. In 2009 belandde Otto van Koert na postdocs in België en Japan in Zuid-Korea, alwaar hij zich vestigde en zich redt met stroef Koreaans.

Na mijn promotie in Keulen in 2005 heb ik twee postdocs gedaan. De eerste was in Brussel bij de Franstalige ULB en mijn tweede postdoc was in Sapporo, in Hokkaido, het noordelijke eiland van Japan. Er was eind 2008 een vacature in Seoul National University (SNU) voor "foreign faculty". Omdat het van Hokkaido uit niet zo ver was, heb ik voor de positie gesolliciteerd, en sinds September 2009 werk ik als wiskundige aan de SNU. Ik was enigszins voorbereid op de taal en cultuurschok door mijn verblijf in Japan; Koreaans heeft een grammatica die wat lijkt op Japans. Die grammatica van het Koreaans (en Japans) is heel anders dan die van talen in Europa. Om een wat simplistische samenvatting te geven: er zijn geen lidworden, de woordvolgorde is anders, en er worden achtervoegsels gebruikt om de rol van onderwerp, lijdend voorwerp, etc aan te duiden (anders dan naamvallen, maar een beetje vergelijkbaar). Verder worden werkwoorden vervoegd naar beleefdheid/senioriteit en niet naar persoon. Het inschatten van welk niveau gepast is, is hier belangrijk. Er is een standaardvorm die werkt voor het dagelijks leven, maar in veel gevallen past die niet. Als een buitenlander word je dat gelukkig wel vergeven. De woorden komen voor de helft uit het Chinees en de andere helft is "puur" Koreaans. Hierbij zijn er veel synoniemen, en het passende woord hangt van het beleefdheidsniveau af.

Hoewel ik nu al vijftien jaar in Korea woon, blijft de taal een probleem. Ik ben met een Koreaanse getrouwd en spreek thuis Koreaans. Zij klaagt er niet over, maar het blijft lastig, en mijn kinderen merken natuurlijk ook dat mijn Koreaans wat stroef is.
De cultuur is hier heel anders, maar veel dingen veranderen erg snel en lijken te verwesteren. In de straat waar ik tot een paar jaar geleden woonde, was er bijvoorbeeld een restaurant dat zich specialiseerde in 사철탕, vierseizoenssoep. Dit is hondensoep met kleine stukjes hondenvlees erin.
Een ander restaurant had "levende" octopus. Inmiddels is het hondenrestaurant in deze straat verdwenen. De "levende" octopus is nog wel redelijk populair. Hier moet ik wel zeggen dat de octopus technisch gesproken dood is: de tentakels worden in stukken gehakt, en die stukjes bewegen dan nog ongeveer een uur. Ander eten dat Nederlanders ongebruikelijk zullen vinden, zijn gekookte zijdenworm en een gefermenteerde rog. De gefermenteerde rog heeft een sterke ammoniaksmaak, en is een traditie uit het zuidwesten van Korea.
Het was verder tot ongeveer tien jaar geleden gebruikelijk om in een restaurant op de grond te zitten, maar dit aspect is inmiddels erg verwesterd. Er zijn nu in bijna alle restaurants tafels en stoelen. Uiterlijk speelt een veel grotere rol in Korea dan ik me van Nederland herinner. Er zijn vrijwel overal reclames over plastische chirurgie, zoals in de metro of in de lift van het flatgebouw waar ik woon.

Op de universiteit zijn de cultuurverschillen een stuk kleiner. Het lijkt erg op andere universiteiten: lesgeven, onderzoek en administratie. Alleen na een colloquium komen de verschillen boven water. Na het colloquiumdinner is er een tweede ronde die om half 9 start met bier en soju, een goedkope, maar vrij sterke drank, en dan vaak een derde ronde (tot middernacht) en soms zelfs een vierde ronde. Sommige collega's drinken veel, en ik heb een keer een dronken algebraïsche meetkundige naar huis moet slepen. Ik was alleen maar een student in Nederland, maar ik geloof dat dit daar niet vaak gebeurt.

Ik zal ook iets zeggen over Noord Korea, omdat mensen me daar vaak over vragen. Eigenlijk denken we hier in Zuid Korea niet zo

veel over Noord Korea: het speelt nauwelijks een rol in mijn dagelijks leven. De lange dienstplicht in Zuid Korea is het duidelijkste teken van Noord Korea. Deze was twee jaar en is nu nog anderhalf jaar, dus behoorlijk lang, en dat zou, denk ik, niet het geval zijn als de verhouding met Noord Korea een stuk beter was.

En dan nu iets over de universiteit hier. De studenten van de SNU zijn vaak erg goed, maar er zijn veel grotere onderlinge verschillen tussen de studenten dan in Nederland. Om dat uit te leggen, moet ik iets zeggen over het middelbare school systeem in Korea. Er zijn hier gewone en wetenschappelijke middelbare scholen (anders dan VWO). Op de wetenschappelijke middelbare scholen leren scholieren in de wiskundeklassen epsilon-delta bewijzen, machtreeksen, een beetje groepentheorie en nog veel meer. Van deze scholen komen ook altijd een paar scholieren die een gouden medaille winnen op de Internationale Wiskunde Olympiade. Met andere woorden, deze scholieren hebben al een prima wiskunde kennis voordat ze naar de universiteit komen.
Anderzijds is het wiskunde onderwijs veel zwakker op de reguliere middelbare scholen. Door onderwijshervormingen zullen scholieren op reguliere middelbare scholen vanaf 2028 niet meer leren wat vectoren en matrices zijn. Deze tweedeling tussen goed getrainde en veel zwakkere studenten maakt het lesgeven wat lastig op SNU. De beste studenten zouden eigenlijk meer moeten en kunnen leren tijdens hun studie, maar door de onderlinge verschillen zijn de college's relatief elementair.

Na hun studie gaan veel studenten werken. Vaak in de financiële sector, het onderwijs (het geven van bijles is bijhoorlijk lucratief), of in de software industrie. Een deel van de studenten wil promoveren in de wiskunde. De beste studenten die willen promoveren, onderbreken hun studie meestal voor militaire dienst voordat ze naar de Verenigde Staten gaan.
Andere studenten vervangen hun militaire dienst door in Korea het onderzoek in te gaan. Voor de SNU betekent dit dat elk jaar ongeveer 40 nieuwe wiskunde promovendi toegelaten worden. Die komen van verschillende universiteiten, en zijn meestal niet afkomstig van een wetenschappelijke middelbare school.

Helaas is de financiering van de promovendi aan de SNU niet zo goed geregeld. De universiteit ziet ze als studenten, dus moeten ze collegegeld betalen (ongeveer 2000 euro per semester, dus behoorlijk duur). De faculteit van natuurwetenschappen weet natuurlijk wel dat promovendi betaald moeten worden, en dit geld voor een basisbeurs komt van grants. Deze basisbeurs is niet voldoende, en in de praktijk moet de begeleider extra geld via meer grants regelen. De totale compensatie hangt dus sterk van de begeleider en de student af. Dit systeem is niet goed, maar ik zie het niet zo snel veranderen.

De universiteit is hier trouwens behoorlijk rijk. De campus is erg groot en mooi. De faciliteiten zijn erg goed en ik ben erg onder de indruk van studenten. Voor onderzoek is hier veel ruimte, hoewel ik sinds mijn promotie tot professor vrij veel administratie moet doen. En dat is waarschijnlijk hetzelfde als in Nederland.

Jop Briët
Centrum Wiskunde & Informatica (CWI)
Amsterdam
J.Briet@cwi.nl

De oplossing The solution

On the resolution of Marton's conjecture from additive combinatorics

In this article, Briët delves into the history and scope of Marton's conjecture, which is also known as the polynomial Freĭman-Ruzsa conjecture. This conjecture concerns set coverings by cosets of subgroups in case of small doubling in finite-field setting.

Already in 1927, Van der Waerden published an article about arithmetic progressions (APs) in this magazine. Via the conjecture by Erdős en Turán, an ergodic version by Furstenberg and proofs constructed via Fourier-analytic techniques and ergodic theory, Briët arrives at the proof of Marton's conjecture by Gowers, Green, Manners and Tao in 2023. This proof was achieved using information-theoretic tools, in particular, the entropic Ruzsa distance. Briët concludes with the importance of equivalent formulations for various fields and a brief outline.

Breakthroughs are supposed to be rare. Not so, it seems, for the relatively young field of additive combinatorics lately. Additive combinatorics is sometimes said to have its origins in a 1927 paper of van der Waerden published in this very journal [44]. Van der Waerden's theorem asserts that for any coloring of the integers $1, \ldots, n$ with r colors, there will be a k-term arithmetic progression (k-AP) whose terms all have the same color, provided n is big enough in terms of k and r.

The pigeonhole principle implies that one of the color classes has at least a $\frac{1}{r}$-fraction of $1, \ldots, n$. It was conjectured by Erdős and Turán [6] that this fact alone is sufficient, in other words, that dense sets of the integers always contain long arithmetic progressions. Erdős went even further and conjectured that any set $A \subseteq \mathbb{N}$ satisfying $\sum_{n \in A} \frac{1}{n} = \infty$ contains arithmetic progressions of arbitrary length. Perhaps the most important example of such a set is formed by the prime numbers.

The first progress towards the Erdős-Turán conjecture was made by Roth in 1953, who used Fourier analysis over $\mathbb{Z}/n\mathbb{Z}$ to prove that any set of size roughly $\frac{n}{\log\log n}$ contains a 3-AP [36]. Roth's methods turned out hard to generalize to deal with longer progressions, however. The next advance came from Szemerédi in 1975, who reproved Roth's theorem with combinatorial methods – introducing the now famous regularity lemma from graph theory – which he could generalize to prove the conjecture for arbitrary progression lengths [41].

A downside of Szemerédi's proof was that it gave extremely poor quantitative upper bounds on $r_k(n)$, the maximal size of a k-AP-free set in $\{1, \cdots, n\}$. In particular, Roth's proof gave far superior bounds on $r_3(n)$. This fact, in addition to the elegance of Roth's proof, motivated Gowers in the late 90's to search for suitable adaptations of Fourier analysis over $\mathbb{Z}/n\mathbb{Z}$ to reprove Szemerédi's theorem – not for a second, but a third time [10, 11]. A surprising new proof had already been discovered in the late 70's by Furstenburg by translating the theorem to an equivalent statement in ergodic theory [9]. The new ergodic theory proof gave no quantitative bounds on $r_k(n)$ at all, however, although it did give rise to powerful generalizations of van der Waerden's theorem and Szemerédi's theorem, such as a density version of the Hales-Jewett theorem and Szemerédi's theorem with polynomial progressions [8, 2]. Quantitative combinatorial and Fourier-analytic proofs for these results were developed only relatively recently [34, 35, 31].

Gowers's new proof of Szemerédi's theorem involves ingenious innovations of Fourier-analytic techniques, intitiating the new field of higher-order Fourier analysis [15, 43]. Building on these ideas, Green and Tao famously managed to prove that the primes indeed contain arbitrarily long arithmetic progressions [19].

A key tool in the (higher-order) Fourier-analytic proof of Szemerédi's theorem comes from the theory of set addition developed by Freĭman [7]. A main goal in this theory is to understand the structure of a finite subset A of an abelian group whose *doubling*, $A + A = \{a + b \mid a, b \in A\}$, is not much bigger than A itself. Cosets of subgroups are extreme examples where such set addition leads to no growth at all. Marton's conjecture concerns an inverse theorem for sets in finite vector spaces, asserting that if such a set has small doubling, then it can be covered by a few cosets of

a relatively small subgroup. Her motivation for posing the conjecture did not have to do with questions from additive combinatorics but rather originated from an information-theoretic source-coding problem [25]. However, the relevance of the conjecture to higher-order Fourier analysis is the reason for most of the attention it received in the last couple of decades.

Finite-field models

The finite-field setting of Marton's conjecture comes about in a heuristic that is often considered in additive combinatorics where the integers are replaced by finite vector spaces. A variant of Roth's theorem was proved by Meshulam in 1995 and shows that any set $A \subseteq \mathbb{F}_3^n$ (the n-dimensional vector space over the field of three elements) of size about $\frac{3^n}{n}$ contains a 3-term arithmetic progression (or equivalently, an affine line) [30]. Meshulam's theorem can be proved in much the same way as Roth's theorem, now using Fourier analysis over $\mathbb{F}_3^n$. Remarkably, the resulting proof is much cleaner and yields comparatively better bounds. Such finite-field models have proved to be a valuable testing grounds for problems over the integers or cyclic groups [14, 45, 32]. The relevance of finite vector spaces in theoretical computer science, in particular $\mathbb{F}_2^n$, also led to an ever-continuing process of cross fertilization between disciplines [29].

Many prior spectacular results notwithstanding, recent years have witnessed a surprising number of major strides in additive combinatorics. These include for instance the resolution of the cap set conjecture by Ellenberg and Gijswijt, showing that $r_3(\mathbb{F}_3^n) \leq 3^{cn}$ for some absolute constant $c < 1$ [5]; a proof of the above-mentioned Erdős conjecture for 3-APs by Bloom and Sisask [4]; and a further strong quantitative improvement on $r_3(n)$ by Kelley and Meka [24], which gets tantalizingly close to a lower bound due to Behrend from 1946 [1]. In the words of mathematician and popular math-blogger Gil Kalai, the most recent breakthrough is due to a veritable A-Team of mathematics. In November of 2023, Tim Gowers, Ben Green, Freddie Manners and Terence Tao posted an arXiv preprint [12] in which they settled Marton's conjecture, widely known in the literature as the polynomial Freĭman-Ruzsa conjecture.

Marton's conjecture


Marton

Let G be an abelian group. For a pair of finite subsets $A,B \subseteq G$, define their sum and difference sets by $A \pm B = \{a \pm b \mid a \in A, b \in B\}$. The key quantity of interest is the *doubling parameter* of A, which is defined by $\sigma(A) = \frac{|A+A|}{|A|}$ This parameter is easily seen to be bounded by $1 \leq \sigma(A) \leq \frac{1}{2}(|A|+1)$. Sets that attain the upper bound, known as Sidon sets, have the property that all sums of pairs from A are distinct. A basic example of a Sidon set is the set of standard basis vectors in $\mathbb{F}_3^n$. Of interest to Marton's conjecture, however, is the lower end of the spectrum, where the doubling parameter turns out to be a proxy for algebraic structure. To see why, it is instructive to first consider the extreme case.

Cosets of subgroups are easily seen to have doubling parameter 1. It turns out that the converse also holds.

Proposition 1 Let $A \subseteq G$ be a finite subset with doubling 1. Then A is a coset of a subgroup of G.

Proof: We may suppose that A contains 0 because for any $b \in A$, the translate $A - b = \{a - b \mid a \in A\}$ contains zero and has doubling $\sigma(A)$. If A contains 0, then $A \subseteq A + A$ and in fact equality $A = A + A$ holds because $\sigma(A) = 1$. Hence, A is closed under addition. This implies that for each $x \in A$, we have that $x + A = A$ as these two sets have equal size. Since $0 \in A$, we thus have that $-x \in A$.

A natural question that arises from this characterization is what can be said about sets with "small" doubling. As an example, if $H \subseteq G$ is a coset of subgroup and $A \subseteq H$ is any set that occupies an ε-proportion of H, then A has doubling at most $\frac{1}{\varepsilon}$ since $|A+A| \leq |H+H| = |H| \leq \frac{1}{\varepsilon}|A|$. In 1973, Freĭman slightly moved the scale and showed that these are the only examples if the doubling is not too much larger than 1 [7].

Theorem 2 (Freĭman) Let $A \subseteq G$ be a finite subset with doubling parameter at most $\frac{3}{2}$. Then $A - A$ is subgroup of G.

A result of Plünnecke implies that for any finite set $B \subseteq G$, the size of its difference set is related to its doubling parameter by $|B - B| \leq \sigma(B)^2 |B|$ [33]. Therefore, by translating $A - A$ by an arbitrary element of A, we ensure that it contains A and arrive at the following corollary.

Corollary 3 Let $A \subseteq G$ be a finite subset with doubling parameter at most $\frac{3}{2}$. Then, there is a subgroup $H \subseteq G$ and $x \in G$ such that $A \subseteq H + x$ and $|H| \leq \frac{9}{4}|A|$.

Does such a statement still hold if the scale is moved further? In the paper that first explicitly recorded Marton's conjecture, Ruzsa [7] proved that it does with the following finite-field analog of another celebrated result of Freĭman over the integers [17][46].

Theorem 4 (Freĭman–Ruzsa theorem) Let p be a prime number and let $A \subseteq \mathbb{F}_p^n$ be a set with doubling parameter K. Then, there is an affine subspace $H \subseteq \mathbb{F}_p^n$ of size $|H| \leq K^2 p^{K^4} |A|$ such that $A \subseteq H$.

Marton's conjecture concerns the dependence of the ratio $|H|/|A|$ on the doubling parameter K. An improvement on this dependence was obtained by Green and Ruzsa, who showed that the exponent K^4 could be reduced to $\lfloor 2K^2 - 2 \rfloor$ [17]. As stated, however, Theorem 4 cannot admit a better function than p^{K^c} for some constant $c > 0$, as the following example shows. Let $V \subseteq \mathbb{F}_2^n$ be the subspace spanned by the last $n - k$ standard basis vectors and let $A = \{e_1, \cdots, e_k\} + V$. Since A consists of k pairwise disjoint cosets of V, it has size $k2^{n-k}$. Due to the standard basis vectors, A has doubling about $k/2$ and any affine subspace containing A must have size at least $2^{n-1} = \frac{1}{k}2^{k-1}|A|$. In light of this, to what extent could one hope to improve on Theorem 4?

An important observation to make about the above example is that it contains a subspace V of size at most $|A|$ such that A is covered by only about K translates of V. Ruzsa attributed to Marton the conjecture that this fact points to a general economic description of small-doubling sets by subspaces. More precisely, Marton's conjecture, or polynomial Freĭman-Ruzsa conjecture, states that there is a subspace H of size at most $|A|$ such that A can be covered using K^c translates of H for some absolute constant $c > 0$ (see [37]).

Major progress towards this conjecture was obtained in 2012 by Sanders [39], who used sophisticated Fourier-analytic methods to show that a quasi-polynomial in K number of translates suffice. With similar methods, Konyagin shortly after showed a slightly better but still quasi-polynomial bound (see [40]). Remarkably, with only one more big leap the conjecture was recently settled in full [12].

Theorem 5 (Gowers, Green, Manners and Tao (2023)) If $A \subseteq \mathbb{F}_2^n$ has doubling parameter K, then there is a subspace H of size $|H| \leq |A|$ such that A can be covered by at most $2K^C$ translates of H, where $C > 0$ is an absolute constant.

The original proof gave the result with $C = 12$ but not long after it appeared this was improved to $C = 9$ by Liao [26]. Subsequently, it was shown by the same original authors that their result holds more generally over finite fields of larger characteristic [13]. A few words will be devoted to the ideas behind the proof of this result here, but it is worthwhile to first highlight a couple of intriguing equivalent formulations (for more formulations, see [23] and [12]). One example is of fundamental importance to the field of algebraic property testing [38].

Corollary 6 (Linearity testing) There are absolute constants $c, C > 0$ such that the following holds. Suppose $f: \mathbb{F}_2^m \to \mathbb{F}_2^n$ is a function such that if x, y are uniformly distributed over $\mathbb{F}_2^m$, we have

$$\Pr\big[f(x+y) = f(x) + f(y)\big] \geq \frac{1}{K}.$$

Then, there exists a linear map $g: \mathbb{F}_2^m \to \mathbb{F}_2^n$ such that

$$\Pr\big[f(x) = g(x)\big] \geq \frac{c}{K^C}$$

Another formulation lies at the heart of higher-order Fourier analysis and concerns inverse theorems for the Gowers uniformity norms.

Gowers Inverse Theorems

The uniformity norms measure how much a function behaves like a polynomial by looking at how much it oscillates after a certain derivative operation has been applied a number of times. Given a function $f: G \to \mathbb{C}$, its *multiplicative derivative* in direction $h \in G$ is given by the function $\Delta_h f: G \to \mathbb{C}$ defined by

$$\Delta_h f(x) = f(x+h)\overline{f(x)}.$$

An example to keep in mind to make sense of the terminology is a *polynomial phase function* $f(x) = \omega^{P(x)}$, where p is a prime, $\omega = e^{2\pi i/p}$ and $P(x) \in \mathbb{F}_p[x_1, \cdots, x_n]$ is an n-variate polynomial over $\mathbb{F}_p$. Then,

$$\Delta_h f(x) = \omega^{P(h+x)-P(x)}.$$

The exponent $P(h+x) - P(x)$ is the standard discrete derivative of $P(x)$ in direction h and if P has degree d, then this derivative has degree $d-1$. So, after applying the multiplicative derivative $d+1$ times to f, for any choice of directions, one is left with the constant-1 function, which exhibits no oscillation at all.

Definition 7 (Uniformity norms) For a finite abelian group G, positive integer k and $f: G \to \mathbb{C}$, the *Gowers k-uniformity norm* of f is defined by

$$\|f\|_{U^k} = \big(\mathbb{E}_{x, h_1, \ldots, h_k \in G} \Delta_{h_k} \cdots \Delta_{h_1} f(x)\big)^{\frac{1}{2^k}},$$

where the expectation is taken over independent uniformly distributed random elements from G.

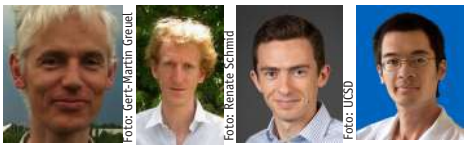
It is easily verified that the 1-uniformity norm is simply the absolute value of the average of f. This means that the 1-uniformity norm is in fact a semi-norm as it can be zero for nonzero f. For larger k, however, the uniformity norms are indeed norms.

To get some intuition for these norms, consider a linear phase function given by a character $\chi(x) = \omega^{\langle x, a \rangle}$ of $\mathbb{F}_p^n$ for a nonzero $a \in \mathbb{F}_p^n$. A single derivative in direction h turns this into the function $\chi(h)$, which is independent of x. Orthogonality of the characters implies that averaging over h causes such oscillation that the whole average cancels to zero. But a second derivative yields the constant-1 function. Linear phases thus attain the maximum-possible U^2-norm of 1. It is a routine exercise to show that these are the only such examples. Moreover, functions whose U^2-norm is bounded away from zero are closely related to linear phases. Using basic Fourier-analytic tools such as Parseval's identity and the Cauchy-Schwarz inequality, it is also not hard to show that if $\|f\|_{U^2} \geq \varepsilon$, then f correlates with some character χ, in the sense that

$$\big|\langle f, \chi \rangle\big| = \big|\mathbb{E}_{x \in \mathbb{F}_p^n} f(x)\,\overline{\chi(x)}\big| \geq \varepsilon^2.$$

This basic fact is a key step in a standard proof of Roth's theorem and Meshulam's version over finite vector spaces, as one can use the U^2-norm to count 3-APs in sets $A \subseteq G$. For a similar reason, Gowers introduced the U^k-norms to count $(k+1)$-APs.

The intuition one should have for the higher-order uniformity norms is that if $|f| \leq 1$ and f has large U^k-norm, then f correlates with a polynomial phase of degree at most $k-1$. This intuition turns out to be approximately correct for functions on cyclic groups and finite vector spaces, as



From left to right: Gowers, Green, Manners and Tao

was established in a series of highly nontrivial works on inverse theorems for the uniformity norms [10, 38, 20, 3 , 43, 22]. Quantitative aspects of these inverse theorems are important for their role in proofs of Szemerédi's theorem, where they are used to show that if a set deviates in the number of APs expected from a random set of equal size, then a balanced version of its indicator function must correlate with a structured function in the form of a polynomial phase. Such correlation can be leveraged to a density increment of the set in a large structured set such as an arithmetic progression or affine subspace. This argument can then be iterated in a so-called density increment strategy to show that AP-free sets of a given density only exist when the ambient group is not too big.

One of the main recent motivations for studying Marton's conjecture is due to its equivalence to the following polynomial version of the inverse theorem for the 3-uniformity norms over finite vector spaces [27, 21].

Corollary 8 (Polynomial inverse theorem for the U^3-norm) There exists an absolute constant $c > 0$ such that the following holds. For any function $f: \mathbb{F}_p^n \to [-1, 1]$, there exists a quadratic phase function $\phi: \mathbb{F}_p^n \to \mathbb{C}$ such that

$$\big|\langle f, \phi \rangle\big| \geq \|f\|_{U^3}^c.$$

Entropy version of PFR

We will only briefly touch upon some of the ideas behind the proof of Theorem 5. A streamlined and abridged version of it may also be found on Tao's blog [42]. The rough idea behind the proof of Theorem 5 is to follow a "doubling decrement" strategy. Given a set $A \subseteq \mathbb{F}_2^n$ with doubling K, the idea is to show that there is a set A' that is in some way related to A and that has doubling at most $K^{0.99}$. Iterating this process, one quickly ends up in the purview of Freĭman's $\frac{3}{2}$-theorem (Corollary 3), which gives an affine subgroup with which one might hope to cover A using only few translates. Due to certain difficulties of working with the doubling constant di-

rectly, Gowers et al. apply a strategy of this type instead to a smoother but equivalent information-theoretic setting where subsets are replaced by $\mathbb{F}_2^n$-valued random variables [16].

A subset A is then represented by a uniform random variable over A, denoted U_A. A key role is played by the *Shannon entropy* of finitely supported random variables X,

$$H[X] = -\mathbb{E}\big[\log_2(\Pr[X=x])\big].$$

The Shannon entropy serves as a measure of size, as $\mathrm{H}[\mathrm{U_A}] = \log_2|\mathrm{A}|$. For two finitely supported independent random variables X, Y taking values in an additive group G, define their *entropic Ruzsa distance* by

$$d[X;Y] = H[X-Y] - \tfrac{1}{2}H[X] - \tfrac{1}{2}H[Y].$$

This quantity is referred to as a distance, but it has the odd property that a random variable can have nonzero distance to itself. It is still useful in the context of doubling parameters, however, due to the fact that

$$\mathrm{d}[\mathrm{U_A}, \mathrm{U_A}] = \log_2 \mathrm{K}.$$

As one might expect in light of Proposition 1, it holds that $d[X,X] = 0$ if and only if X is uniformly distributed over an affine subspace. Another useful feature, also the main reason why this function is referred to as a distance, is that it obeys the triangle inequality.

Lemma 9 (Ruzsa triangle inequality) Let X, Y, Z be finitely supported random variables over an additive group G. Then,

$$d[X;Y] \le d[X;Z] + d[Y;Z].$$

This is a main tool in the entropic doubling decrement proof. It is used, very roughly speaking, to sequentially find certain improvements of the original distribution U_A to obtain distributions that are on the one hand closer to themselves in entropic Ruzsa distance (thereby moving towards a uniform distribution on an affine subspace), while on the other hand not moving too far away from U_A so as to still give an approximation of it. This results in the following version of Theorem 5.

Theorem 10 (The entropic polynomial Freĭman–Ruzsa theorem) Let X, Y be $\mathbb{F}_2^n$-valued random variables such that $d[X,Y] \le \varkappa$. Then, there is a subspace $H \subseteq \mathbb{F}_2^n$ such that

$$d[X;U_H] + d[Y;U_H] \le 11\varkappa,$$

When one replaces X and Y with U_A, then the resulting statement turns out to be equivalent to Theorem 5. In a large online collaboration, the proof of Theorem 10 was formalized in the automated proof assistant Lean4 (see https://teorth.github.io/pfr/).

What's next?

The proof of Marton's conjecture settled a major open problem in the field of additive combinatorics. It shows that any set $A \subseteq \mathbb{F}_2^n$ with doubling K can be covered by at most $2K^9$ cosets of a subspace of size at most A. There is a close connection between this type of statement and results on containment of a large affine subspace in iterated sum sets of A. Indeed, Theorem 5 also has the following corollary [12].

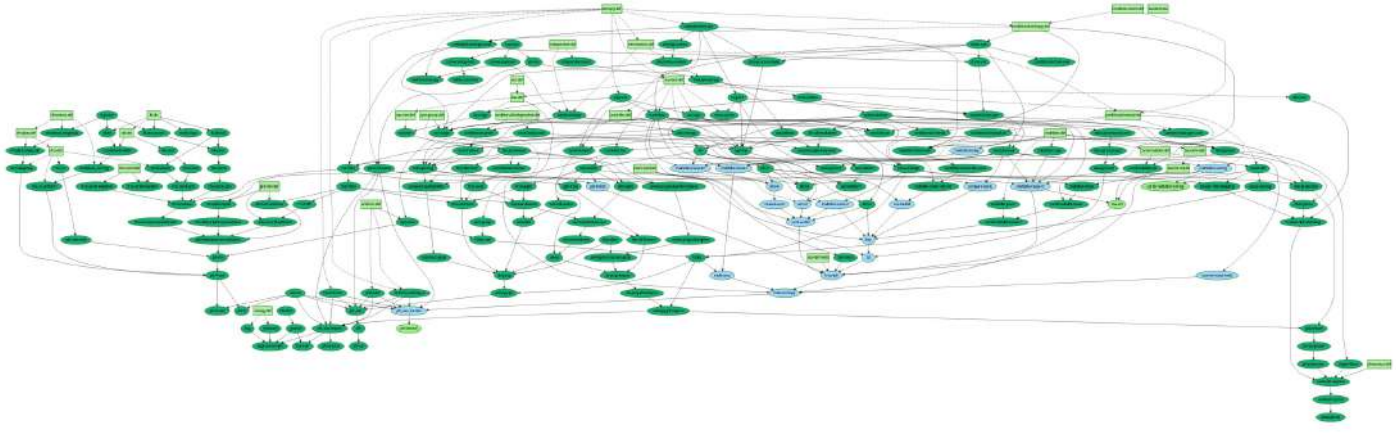
Corollary 11 There is an absolute constant $C > 0$ such that the following holds. Suppose $A \subseteq \mathbb{F}_2^n$ is a nonempty subset with doubling parameter K. Then, the m-fold iterated sum set $A + \cdots + A$ contains a subspace of size at least $K^{-C}|A|$ for some $m \le \log(K+2)^C$.

The relevance of this result is that it may be viewed as a weak version of the so-called *polynomial Bogulyubov conjecture*, posed by Lovett [28].

Conjecture 12 (Polynomial Bogulyubov conjecture) There is an absolute constant $C > 0$ such that the following holds. Suppose $A \subseteq \mathbb{F}_2^n$ is a nonempty subset with doubling parameter K. Then, $A+A+A+A$ contains a subspace of size at least $K^{-C}|A|$.

The best available result of this type, involving four-fold sum sets, is quasi-polynomial in K. It was proved by Sanders in the work that essentially established the previous best version of Theorem 5, showing that $4A$ contains a subspace of size at least $\exp\big(-\log(K+2)^C\big)|A|$ [39].

So while a major hurdle has just been overcome, a next milestone is already in clear view.



Bron: From https://teorth.github.io/pfr/blueprint/dep_graph_document.html

Figure 1 Dependency graph of the formalized proof of Marton's conjecture in proof assistant Lean4.

References and notes

1 F. A. Behrend. On sets of integers which contain no three terms in arithmetical progression. *Proc. Nat. Acad. Sci. U. S. A.*, 32:331–332, 1946.

2 V. Bergelson and A. Leibman. Polynomial extensions of van der Waerden's and Szemerédi's theorems. *J. Amer. Math. Soc.*, 9(3):725–753, 1996. doi:10. 1090/S0894-0347-96-00194-4.

3 Vitaly Bergelson, Terence Tao, and Tamar Ziegler. An inverse theorem for the uniformity seminorms associated with the action of F∞ p . *Geom. Funct. Anal.*, 19(6):1539–1596, 2010. doi:10.1007/s00039-010-0051-1.

4 Thomas F Bloom and Olof Sisask. Breaking the logarithmic barrier in Roth's theorem on arithmetic progressions. *arXiv preprint arXiv:2007.03528, 2020*.

5 Jordan S Ellenberg and Dion Gijswijt. On large subsets of with no three-term arithmetic progression. *Annals of Mathematics*, pages 339–343, 2017.

6 Paul Erdős and Paul Turán. On some sequences of integers. *Journal of the London Mathematical Society*, s1-11(4):261–264, 1936.

7 Grigory A. Freĭman. Foundations of a structural theory of set addition. *American Mathematical Society*, 1973.

8 H. Furstenberg and Y. Katznelson. A density version of the Hales-Jewett theorem. *J. Anal. Math.*, 57:64–119, 1991. doi:10.1007/BF03041066.

9 Harry Furstenberg. Ergodic behavior of diagonal measures and a theorem of Szemerédi on arithmetic progressions. *J. Analyse Math.*, 31:204–256, 1977.

10 W. T. Gowers. A new proof of Szemerédi's theorem for arithmetic progressions of length four. *Geom. Funct. Anal.*, 8(3):529–551, 1998.

11 W. T. Gowers. A new proof of Szemerédi's theorem. *Geom. Funct. Anal.*, 11(3):465–588, 2001.

12 W. T. Gowers, Ben Green, Freddie Manners, and Terence Tao. On a conjecture of Marton, 2023. arXiv:2311.05762.

13 W. T. Gowers, Ben Green, Freddie Manners, and Terence Tao. Marton's con- jecture in abelian groups with bounded torsion, 2024. arXiv:2404.02244.

14 Ben Green. Finite field models in additive combinatorics. In Surveys in combi- natorics 2005, volume 327 of London Math. Soc. Lecture Note Ser., pages 1–27. Cambridge Univ. Press, Cambridge, 2005. doi:10.1017/CBO9780511734885. 002.

15 Ben Green. Montréal notes on quadratic Fourier analysis. In Additive combi- natorics, volume 43 of CRM Proc. Lecture Notes, pages 69–102. *Amer. Math. Soc.*, Providence, RI, 2007.

16 Ben Green, Freddie Manners, and Terence Tao. Sumsets and entropy revisited, 2023. URL: https://arxiv.org/abs/2306.13403, arXiv:2306.13403.

17 Ben Green and Imre Z. Ruzsa. Sets with small sumset and rectification. Bull. *London Math. Soc.*, 38(1):43–52, 2006. doi:10.1112/S0024609305018102.

18 Ben Green and Imre Z. Ruzsa. Freiman's theorem in an arbitrary abelian group. *J. Lond. Math. Soc.* (2), 75(1):163–175, 2007. doi:10.1112/jlms/ jdl021.

19 Ben Green and Terence Tao. The primes contain arbitrarily long arithmetic progressions. *Ann. of Math.* (2), 167(2):481–547, 2008. doi:10.4007/annals. 2008.167.481.

20 Ben Green and Terence Tao. The distribution of polynomials over finite fields, with applications to the Gowers norms. Contrib. *Discrete Math.*, 4(2):1–36, 2009.

21 Ben Green and Terence Tao. An equivalence between inverse sumset theorems and inverse conjectures for the U 3 norm. *Math. Proc. Cambridge Philos. Soc.*, 149(1):1–19, 2010. doi:10.1017/S0305004110000186.

22 Ben Green, Terence Tao, and Tamar Ziegler. An inverse theorem for the Gowers U s+1[N]-norm. *Ann. of Math.* (2), 176(2):1231–1372, 2012. doi: 10.4007/annals.2012.176.2.11.

23 Benjamin J. Green. Notes on the Polynomial Freĭman- Ruzsa Conjecture. expository note. Available at http://people.maths.ox.ac.uk/greenbj/papers/PFR.pdf.

24 Zander Kelley and Raghu Meka. Strong bounds for 3-progressions, 2024. arXiv:2302.05537.

25 J. Korner and K. Marton. How to encode the modulo-two sum of binary sources (corresp.). *IEEE Transactions on Information Theory*, 25(2):219–221, 1979. doi:10.1109/TIT.1979.1056022.

26 Jyun-Jie Liao. Improved exponent for Marton's conjecture in Fn 2, 2024. URL: https://arxiv.org/abs/2404.09639, arXiv:2404.09639.

27 Sachar Lovett. Equivalence of polynomial conjectures in additive combinatorics. *Combinatorica*, 32:607–618, 2012. doi:doi.org/10.1007/ s00493-012-2714-z.

28 Shachar Lovett. An Exposition of Sanders' Quasi-Polynomial Freiman-Ruzsa Theorem. Number 6 in Graduate Surveys. Theory of Computing Library, 2015. URL: http://www.theoryofcomputing.org/library.html, doi:10.4086/toc.gs.2015.006.

29 Shachar Lovett. Additive Combinatorics and its Applications in Theoretical Computer Science. Number 8 in Graduate Surveys. Theory of Computing Library, 2017. URL: http://www.theoryofcomputing.org/library.html, doi:10.4086/toc.gs.2017.008.

30 Roy Meshulam. On subsets of finite abelian groups with no 3-term arithmetic progressions. *Journal of Combinatorial Theory, Series A*, 71(1):168–172, 1995.

31 Sarah Peluse. On the polynomial Szemerédi theorem in finite fields. *Duke Math. J.*, 168(5):749–774, 2019. doi:10.1215/00127094-2018-0051.

32 Sarah Peluse. Finite field models in arithmetic combinatorics – twenty years on, 2023. URL: https://arxiv.org/abs/2312.08100, arXiv:2312.08100.

33 Helmut Plünnecke. Eigenschaften und Abschätzungen von Wirkungsfunktionen. Number 22. Gesellschaft für Mathematik und Datenverarbeitung, 1961.

34 DHJ Polymath. A new proof of the density Hales-Jewett theorem. *Annals of Mathematics*, pages 1283–1327, 2012.

35 Sean Prendiville. Quantitative bounds in the polynomial Szemerédi theorem: the homogeneous case. *Discrete Anal., pages* Paper No. 5, 34, 2017. doi: 10.19086/da.1282.

36 Klaus F Roth. On certain sets of integers. *Journal of the London Mathematical Society*, 1(1):104–109, 1953.

37 Imre Ruzsa. An analog of Freiman's theorem in groups. *Astérisque*, 258(199):323–326, 1999.

38 Alex Samorodnitsky. Low-degree tests at large distances. In STOC'07— *Proceedings of the 39th Annual ACM Symposium on Theory of Computing, pages 506–515. ACM, New York, 2007*. Available at arXiv: 0604353.

39 Tom Sanders. On the Bogolyubov-Ruzsa lemma. *Anal. PDE*, 5(3):627–655, 2012. doi:10.2140/apde.2012.5.627.

40 Tom Sanders. The structure theory of set addition revisited. *Bull. Amer. Math. Soc. (N.S.),* 50(1):93–127, 2013. doi:10.1090/S0273-0979-2012-01392-7.

41 Endre Szemerédi. On sets of integers containing no k elements in arithmetic progression. *Acta Arith*, 27(299-345):21, 1975.

42 Terence Tao. URL: https://terrytao.wordpress.com/2024/06/22/ an-abridged-proof-of-martons-conjecture/.

43 Terence Tao and Tamar Ziegler. The inverse conjecture for the Gowers norm over finite fields in low characteristic. *Annals of Combinatorics*, 16(1):121–188, 2012.

44 Bartel Leendert van der Waerden. Beweis einer Baudetschen vermutung. *Nieuw Archief voor Wiskunde*, 15:212–216, 1927.

45 J. Wolf. Finite field models in arithmetic combinatorics—ten years on. *Finite Fields* Appl., 32:233–274, 2015. doi:10.1016/j.ffa.2014.11.003.

46 Analogous results were proved for arbitrary abelian groups in [18].

Diletta Martinelli
Korteweg-de Vries Instituut voor Wiskunde
Universiteit van Amsterdam
d.martinelli@uva.nl

Przemysław Grabowski
Korteweg-de Vries Instituut voor Wiskunde
Universiteit van Amsterdam
p.grabowski@uva.nl

Proof by example Portraits of women in Dutch mathematics

Jo Ellis-Monaghan

Jo Ellis-Monaghan is a full professor in Discrete Mathematics at the Korteweg-de Vries Institute (KdVI) for Mathematics at the University of Amsterdam (UvA). After several years in different US institutions, Jo arrived in the Netherlands in 2020 when the new research programme on Discrete Mathematics and Quantum Information was established. She has recently become Head of Department at the KdVI Mathematics Institute at the UvA. She shared with us her interesting and unorthodox personal journey and some of her views on mathematics and art.

Let's start from the beginning. Could you tell us a bit about the journey that brought you to work in mathematics? Was it something you always wanted to do or was it a long process?
"It was a long process. I actually hated math growing up. I literally campaigned against it!"

Really? What did you do?
"I was very impatient with what was going on at school. I remember, it was probably second or third grade, being bored with the math book and not wanting to do it. The teacher said "Well, I am sorry, we have to go through this book" so I took it home and did the whole book over the weekend and I brought it back to her. So she said "Ok, you are done. You can use the math period as study time" so I was allowed to sit in a corner during math class and just read. Also, I thought that math at the time was a lot about memorization and that was really not for me. But then in high school I had a geometry class and then it was when the fun started! That's when I started to grasp mathematical beauty and it fired my imagination. Art was my thing. For me it was all about theater, art and creative writing classes. So the idea that mathematics had this beautiful creative side was really a novelty. And I saw it for the first time in geometry class: you didn't have to deal with numbers, you could see things! So it fed right into the artistic abilities, the abilities to visualize things. There was this math competition team, the Mathletes, and I was part of the team and one of the top scorers that year. But then the following year was trigonometry, and I actually failed the class, because again it was all about memorization."


Jo Ellis-Monaghan

And after high school what did you do?
"I went to art school. I was a dance and drama major when I first went to college. That's what I thought I was going to do with my life. But then, for a variety of reasons, I ended up switching over to visual arts: ceramics and paintings."

And how did math come back into the picture?
"Well, while I was in college you had to do some distribution of courses. It was an American liberal art education, so you had to take courses in different fields. I just took math courses to fulfill my distribution requirements and what ended up happening was that these math courses became a little bit of refuge for me. I think it was because the answer was final and objective. Like, the answer was square root of two, that's it. There was not someone sitting there and saying 'But why did you choose that shade of green there?' or 'Can you

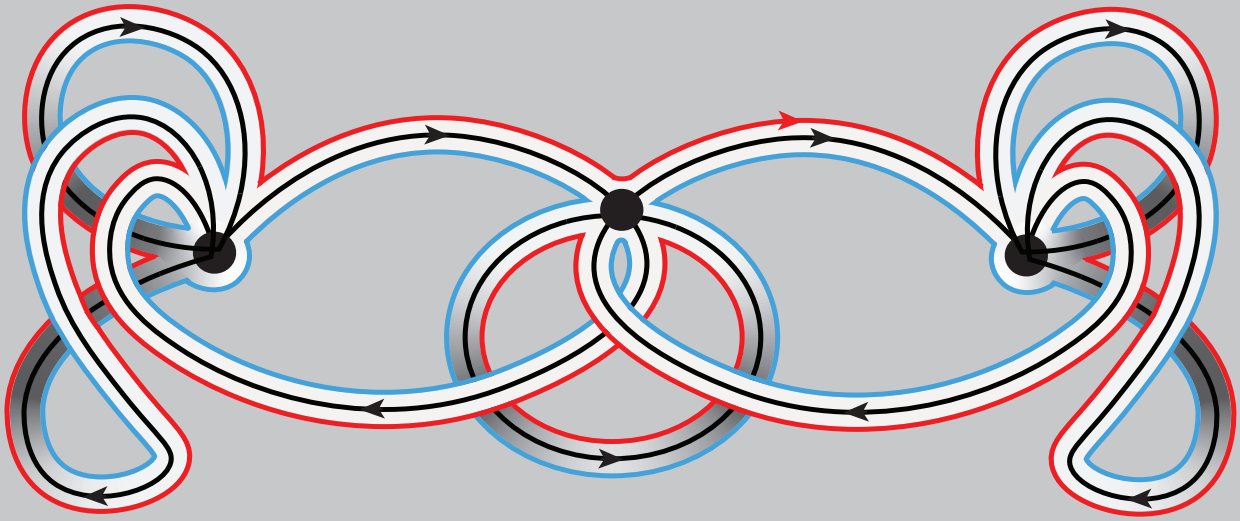


Figure 1 A ribbon graph representation of a graph embedded in a surface, which used artistic visualization and drawing skills. Sewing a disc into each of the red and blue curves reconstructs the surface.

emote a little more?'

There was only one full time math teacher (who was actually Dutch!), because it was more of an art school. I typically had just myself or one or two fellow students in my math courses. So they really noticed if you cut class. It also meant that we learned what he wanted to teach and we didn't learn other stuff. So I had a whole bunch of analysis and never had a linear algebra class! So it was really not a traditional education, but I enjoyed that the focus was always on creative thinking."

And what did you want to do after college?

"I wanted to continue with art school. However, the person I wanted to work with was at the University of Vermont which did not have a graduate programme in art. She was willing to serve as my mentor anyway, so I thought 'Ok I will go to Burlington, where the University of Vermont is, and do the starving-artist-thing. I'll wait tables and at least we'll be in the same town and I'll be able to work with her. And I will be an artist!'

My college mathematics teacher said 'But why should you do that? You should go to grad school'. 'But there is no grad school in art!' 'Just go to grad school in math!' He explained to me how the scholarship system worked and he convinced me that it was the best way to support myself and continue with my art ambitions. The idea that I could get paid while doing a master was completely new to me because it is not true in the humanities. I managed to get into the grad students' housing and in my dorm there was a ceramic studio in the basement that I could use for free, so it actually worked out perfectly for me!

But then, amazingly, I started to really enjoy the mathematics I was doing, and was quite good at it. The beginning of graduate school was a kind of tipping point: you had to pass from simply regurgitating what was in the book to producing your own creative mathematics. There were two very good professors in Algebra at the University of Vermont, Dave Dummit and Richard Foote, and I fell in love with Algebra. I learned that it had nothing to do with memorizing numbers but I could rather visualize structures in my head."

Do you think that your artistic training helped you in that?

"Definitely. It was a huge help throughout all of my career. The brain process of thinking about mathematics and art is for me exactly the same. And there was a moment when the creative energy started shifting from what I was doing in the ceramic studio to what I was doing in mathematics."

And then what happened?

"Well, at that point two life-things happened. The first one was that I got heavy metals poisoning from the art studio and that was a bit of a wake-up call that made me realize it was dangerous stuff. And the other thing that happened is that in the second year of my master, I fell in love with the man I am still married to. We got married and I had my first child.

I started to redirect my choices: I stayed at the University of Vermont as an instructor, I continued to do art, but I began to consider the idea of a PhD program in mathematics, that was unfortunately not available at the University of Vermont. There was not an easy solution for our young family. My husband was working at IBM as an engineer and they had a program that would support him to go to grad school. He didn't have to do it and he was not particularly interested in a PhD, but he suggested he could pursue this opportunity anyway, so that I could go to grad school as well. That's a measure of marital love: put yourself through a PhD program for no other reason than that your spouse could also do a PhD!"

Wow, that's love!

"So we literally sat down at the kitchen table with a map and two compasses and drew circles around the grad programs that could work for each of us and we looked where there was an overlap where we could live and go to the two schools. We ended up in the research triangle area in North Carolina: he went to North Carolina State University and I went to the University of North Carolina. And then, I

just flew! My PhD thesis was on Algebraic Combinatorics and Applied Graph Theory and my research line started.

What did you want to do after grad school?
"I wanted to continue doing research in mathematics. However, IBM had paid for my husband and me to go to grad school, so we then owed IBM a certain number of years, which meant that we had to go back to Vermont. The University of Vermont is the only research institution in the state and they did not have a tenure track hire in my field for many many years. So I went back to Vermont with research ambitions and nowhere to take them. Eventually I took a teaching position at Saint Michael's College, a small liberal art college which was focused on undergraduate education. We also became foster parents at the time, which meant that we were not allowed to leave the county, let alone the state. So I had no geographical mobility."

And how did you manage to keep your research active during the years?
"Both Saint Michael's and the University of Vermont (where I had a visiting position) were very supportive of my research activities. But it was a lot of personal determination and hard work. I grew up in Alaska and what remains with you is a sort of frontier spirit, this idea that you can just do things. Period. So if you don't have a research community, it means you have to create one for yourself. I took the lead in organizing seminar series, writing grants, and generally contributing to an active research community in the area."

Can you tell us a bit more about your decision to move to Amsterdam?
"The agreement with my family was that when my two younger sons were finished with high school I could move to a research institution and that is when the offer from Amsterdam came along, so the timing aligned kind of miraculously. This position was a dream job for me. There was a research group with interests closely aligned to my own and we were building combinatorics in the Netherlands so it was an incredibly exciting time."

You are so the only full time female Full Professor in our department. Do you feel an extra responsibility on your shoulders because of that?
"Yes, bluntly yes. It was actually a surprise when I moved to the Netherlands. It is such a socially liberal country that I simply assumed that there was a good gender balance across society and it was a shock to realize that in Dutch academia we are still far off from gender equality. It was very different from my expectations. I do feel obligations towards my gender because of that. I do feel the need to have more of a presence than I would otherwise if there were more female Full Professors".

To finish, we are curious to hear if you still have time to do art.
"Hold on a second."

Jo stands up in her house in Vermont, where she is while we are doing the interview on Zoom. She disappears for a moment. She comes back with her last artwork.

"I make icons, that's what I do these days. In the past I also did a lot of figurative paintings, but I don't have a lot of time recently. A lot of my art time has gone into learning Dutch, which has taken a phenomenal amount of time." [Jo is almost fluent in Dutch, attracting admiration and envy from the other international members of the department.]

Has now art become a refuge as math once was when you first were an art student?
"Actually it's kind of funny that you mentioned that. I never thought about that before. What happened is that mathematics has become less restful and more like the art. When you do research in mathematics you do make choices like you do in creating art. And a reviewer can come back and ask you to justify your particular choices as art critics do.

But going back to iconography: the composition and the thinking in iconography is very geometric so painting icons is a good mix of art and creative mathematical thinking. I grew up Greek orthodox so iconography also connects me with my heritage. And I do find a lot of rest and restoration in it. So yes, your question is spot-on, art became more of a restful place for me."

We really would like to thank Jo for her time and the very inspiring conversation. She is really an amazing role model for young mathematicians like us still struggling to find their own original path.

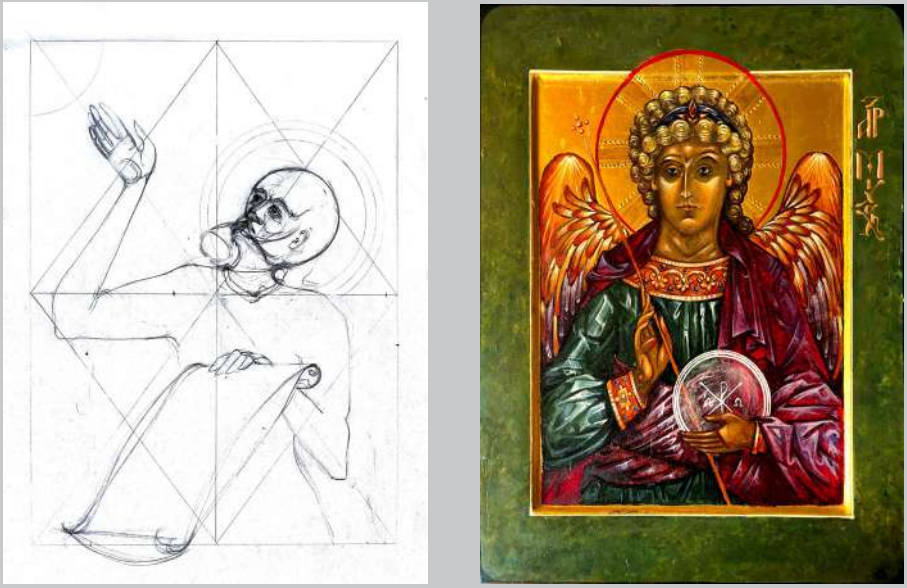
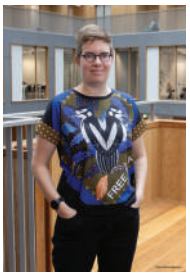


Figure 2
(l) A study for an icon of the Prophet Isaiah, with underlying geometry. (r) An icon of Saint Michael the Archangel, under master iconographer Dmitri Andreyev of the Prosopon School of Iconography.

Rianne de Heide
Department of Applied Mathematics
University of Twente
r.deheide@utwente.nl



Column Rianne takes her chance

Mental health and doing a PhD

Rianne de Heide regularly writes a column on everyday statistical topics in this magazine.

Is doing a PhD detrimental for your mental health? Is doing a PhD worse for your mental health than losing a parent? It appears so, one would conclude, if one read the many posts about this topic on social media in the past month, all linking to a Nature article [5] – that is, not a peer-reviewed publication, but an article in the magazine – titled *The huge toll of PhDs on mental health: data reveal stark effects*. The occasion for this article is a preprint about a longitudinal population study among Swedish PhD students [1].

I find it remarkable that such a magazine article with bold statements is written before the peer-review has been completed. As is often the case, the article itself is much more nuanced than the headline in the magazine, let alone the social media posts. Of course this is a topic that concerns us all in academia, many of us have some personal experience with it, we are all doing / have completed a PhD ourselves, and many of us are supervising students. While I see a lot of attention for this topic, it is mostly limited to accounts of personal experiences, which is of course valuable in itself, but I feel I am missing the bigger picture of whether it is just that, or a more pervasive problem. The preprint [1] provides a good attempt to investigate this (it is not the first one: see e.g. [2] and [3]).

The data included in the study by Bergvall et al. comprised all individuals enrolling in PhD education in Sweden between 2006 and 2017 – it seems therefore to provide a more representative picture than many self-reporting surveys that have been performed previously (see [4] for a meta-analysis). They investigate the use of psychiatric prescription medication and hospitalisation among this population, compared with the general population, and compared with a matched sample of individuals with a corresponding master's degree who are not pursuing a PhD. The authors conclude: "*We provide evidence that PhD studies are associated with a substantial increase in mental health care uptake*". That sounds a lot more nuanced than the newspaper headlines! One observation that made the headlines too, is that this increase is bigger than the increase after the unexpected death of a parent.

Correlation or causation?

News articles are prone to confusing correlation with causation. I'm always suspicious when I read something about a causal effect, and if I'm really interested in the topic, I download the underlying paper. In their paper [1], the authors compare a number of different events in different groups to investigate confounding of the hypothesis that doing a PhD is *causing* the increase in mental health uptake. One confounding factor that I thought of right away, is that the typical age for starting a PhD is around 22, and a typical onset age for several (severe) psychiatric disorders is about the same. But in the paper, the authors compare the group doing a PhD to matched samples of persons with the same master's degrees who are not pursuing a PhD, so that convinced me that there might be more going on (in the PhD, that is). One other hypothesis that I thought of is: but what if those who are inclined to start a PhD, are more predisposed for mental health issues than the population of those not wanting to do a PhD? The authors acknowledge that possibility in the paper: "our analysis cannot exclude that individuals who start PhD studies have, on average, a higher propensity for mental health problems than the control group". This thus remains a question.

Some personal experience

My reading about these topics is also coloured by personal experience. To start with, I see many neurodiverse people around me, I believe there is a higher prevalence among academics, than in the general population. I think academia can be a great place for them, if the conditions are right. There are many accounts of toxic working environments in academia — if one follows the university newspapers it seems to be endless — we all should take responsibility to change that, and to be kind and supportive to each other, and in particular to our PhD students. I was lucky to find a great place to do my PhD, despite my mental health problems, and I believe doing the PhD made it much better, not worse. I missed a role model though. I'm happy that I'm now mentoring several PhD students with similar issues. Feel free to reach out if you want to have a chat about it too.

Referenties

1 Bergvall, S., Fernström, C., Ranehill, E., & Sandberg, A. (2024). The Impact of PhD Studies on Mental Health-A Longitudinal Population Study. Available at SSRN 4920527.

2 Evans, T. M., Bira, L., Gastelum, J. B., Weiss, L. T., & Vanderford, N. L. (2018). Evidence for a mental health crisis in graduate education. Nature biotechnology, 36(3), 282-284.

3 Keloharju, M., Knüpfer, S., Müller, D., & Tåg, J. (2024). PhD studies hurt mental health, but less than previously feared. Research Policy, 53(8), 105078.

4 Satinsky, Emily N., Tomoki Kimura, Mathew V. Kiang, Rediet Abebe, Scott Cunningham, Hedwig Lee, Xiaofei Lin, et al. 2021. "Systematic Review and Meta-Analysis of Depression, Anxiety, and Suicidal Ideation among Ph.D. Students." Scientific Reports 11 (1): 14370. https://doi.org/10.1038/s41598-021-93687-7.

5 Schwaller, F. (2024). The huge toll of PhDs on mental health: data reveal stark effects. Nature, 634(8033), 277-278.

Nelly Litvak
Department of Mathematics and Computer Science
Eindhoven University of Technology
n.v.litvak@tue.nl

Noela Müller
Department of Mathematics and Computer Science
Eindhoven University of Technology
n.s.muller@tue.nl

Column Better than blackboard

Competency-based grading

***`Will this be on the exam?'*** **Over the years, I have noticed that my endeavors to make courses more interactive and engaging ultimately came up against the traditional grading system, with students' understandable but counterproductive fixation on the final exam. The main message of today's `Better than blackboard' issue is: It doesn't have to be that way! My co-author for this edition is Noela Müller, an assistant professor at Eindhoven University of Technology. In 2023/24, Noela and I implemented a new grading system in a probability course for 300 Computer Science students. In this column, we will tell you what we did and how it worked out, our story brightened up by cheerful illustrations of the student artist Mara Chelărescu.**

The course *Probability and Statistics for Computer Science* at TU/e enrolls 300 first-year students. It had a long history, but now its position in the curriculum changed, and revision was due.

In 2023, Noela was assigned to teach this course. In discussion with the Computer Science faculty at TU/e, she removed old and added new topics, and made an effort to use more Computer Science-related examples in her slides and exercises. However, she was also not happy with the existing grading system: 4 intermediate tests and one final exam. Students of previous years said that the intermediate tests were demotivating rather than helpful. But then, how to make sure that the students keep up with the course?

Nelly joined this course as an instructor. By a happy coincidence, in the summer of 2023, she had read the book `*Grading for Growth*' by Clark and Talbert [1] and was highly inspired by the concept of alternative grading: It is well developed, well studied, widely-used, comes in many forms, and is suitable for testing of any kind.

One approach described in [1] – standard-based, or, competency-based grading – sounded very suitable for basic mathematics courses, and we decided to give it a try. We believe it worked well, and we are happy to share what we have done, as well as our and our students' experiences.

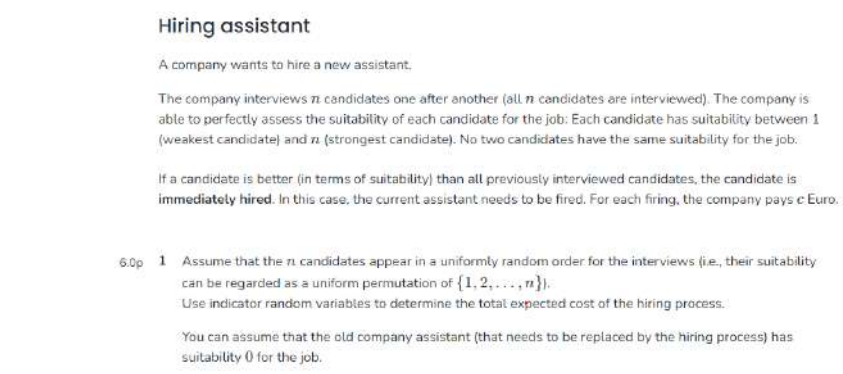
16 competencies

First, from the course content, we identified 16 competencies that we wanted our students to develop. You can see these competencies, called C1-C16, in the first two columns of Table 1.

Following [1], we formulated the competencies in an actionable form: `I can…' . One may say, we could have equivalently formulated them in terms of topics, but we daresay it's not the same. Indeed, take the topic of C14 – `Confidence intervals'. What should a student do to demonstrate understanding of this topic? This is left up to students' interpretation. The actionable `I can…' answers this question, and hence makes the requirements of the course

#	Competency	ANS Test	When
1	I can understand and apply the rules of probability.	Num+MC	week2, week3, exam, resit
2	I can understand and apply conditional probabilities.	Num+MC	week2, week3, exam, resit
3	I can understand and apply the basic theory of discrete random variables.	Num+MC	week3, week4, exam, resit
4	I can choose and apply an appropriate discrete distribution in context.	Num+MC	week3, week4, exam, resit
5	I can understand and apply the basic theory of continuous random variables.	Num+MC	week4, week5, exam, resit
6	I can choose and apply an appropriate continuous distribution in context.	Num+MC	week4, week5, exam, resit
7	I can derive the expected running time of simple algorithms using linear functions of random variables.	Open Q	week5, week6, exam, resit
8	I can understand and apply the Central Limit Theorem.	Num+MC	week5, week6, exam, resit
9	I can understand and construct Markov chain models in the context of computer science.	Open Q	week6, week7, exam, resit
10	I can understand and apply the basic theory of Markov chains.	Num+MC	week6, week7, exam, resit
11	I can compute and interpret descriptive statistics.	Num+MC	week7, week8, exam, resit
12	I can understand and carry out the basic analysis of statistical estimators.	Num+MC	week7, week8, exam, resit
13	I can derive parameter estimators using the method of maximum likelihood.	Open Q	week8, exam, resit
14	I can compute and interpret basic confidence intervals.	Num+MC	week8, exam, resit
15	I can understand the basic theory of hypothesis testing and carry out simple tests.	Num+MC	exam, resit
16	I can understand and apply the basic theory of Bayesian estimation and hypothesis testing.	Num+MC	exam, resit

Table 1 An open question on C7.



Hiring assistant

A company wants to hire a new assistant.

The company interviews n candidates one after another (all n candidates are interviewed). The company is able to perfectly assess the suitability of each candidate for the job: Each candidate has suitability between 1 (weakest candidate) and n (strongest candidate). No two candidates have the same suitability for the job.

If a candidate is better (in terms of suitability) than all previously interviewed candidates, the candidate is **immediately hired**. In this case, the current assistant needs to be fired. For each firing, the company pays c Euro.

6.0p 1 Assume that the n candidates appear in a uniformly random order for the interviews (i.e., their suitability can be regarded as a uniform permutation of $\{1, 2, \ldots, n\}$).
Use indicator random variables to determine the total expected cost of the hiring process.

You can assume that the old company assistant (that needs to be replaced by the hiring process) has suitability 0 for the job.

Figure 1 An open question on C7.

clear and explicit.

Competency quizzes

We assessed each competency separately using a small quiz. All quizzes were conducted in ANS software. The competencies that are marked red in Table 1 were tested with an open question (a written test). The remaining competencies were tested digitally, with one multiple choice and one numerical question. Below, we describe the questions in more detail.

Multiple attempts For most competencies (except the last 4), there were 4 opportunities to take a quiz: 2 during the course, 1 at the exam, and 1 at the resit, see the last column of Table 1. Students made quizzes in class, during tutorials/instructions, for 45 minutes. In week n, 4 quizzes were open, on the competencies covered in weeks n-1 and n-2. Usually, 45 minutes were too short to make all 4 quizzes, so the students chose which quizzes to attempt. During the exam and the resit all 16 quizzes were open for 3 hours.

Looking up is allowed In ANS, we have provided a Statistics compendium that summarized most formulas, and the lecture slides. We did this because in a real-life situation, if students look for material online, they will usually look up formulas and summaries similar to those in compendium and slides. The quiz problems were never the ones on the slides, therefore we believe it was adequate to allow the use of these materials.

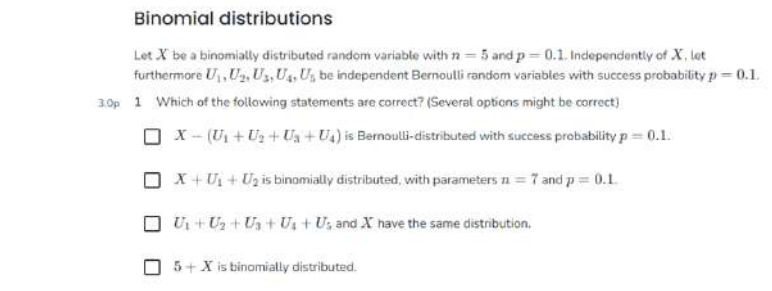
Open, multiple choice, and numerical questions

As mentioned before, the 'red' competencies in Table 1 were tested using open questions, for which we required a detailed write-up. These written competencies were chosen because they truly require probabilistic reasoning and due to their relevance for computer scientists, for instance:

> C7: I can derive the expected running time of simple algorithms using linear functions of random variables.

An example of a an open question on C7 is given in Figure 1.

We restricted the open questions to only three competencies because grading open questions takes a lot of time, and is not always useful. For instance, competency C14 - *I can compute and interpret confidence intervals*, is largely procedural, and can be tested very adequately with numerical and multiple choice questions, with the great advantage of automated grading and immediate feedback.



Binomial distributions

Let X be a binomially distributed random variable with $n = 5$ and $p = 0.1$. Independently of X, let furthermore U_1, U_2, U_3, U_4, U_5 be independent Bernoulli random variables with success probability $p = 0.1$.

3.0p 1 Which of the following statements are correct? (Several options might be correct)

- ☐ $X - (U_1 + U_2 + U_3 + U_4)$ is Bernoulli-distributed with success probability $p = 0.1$.
- ☐ $X + U_1 + U_2$ is binomially distributed, with parameters $n = 7$ and $p = 0.1$.
- ☐ $U_1 + U_2 + U_3 + U_4 + U_5$ and X have the same distribution.
- ☐ $5 + X$ is binomially distributed.

Figure 2 Example of a multiple choice question on competency C4 - *I can choose and apply an appropriate discrete distribution in context*.

All other competencies were tested with a digital test of two questions: a multiple choice question on understanding the theory, and a numerical question on executing procedures.

We believe that multiple choice questions work very well, see also our previous column [2]. When students are confronted with a yes/no question: `Is this statement right or wrong?', they cannot talk their way around it, as sometimes they can in an open question. See the example in Figure 2 for competency C4 - *I can choose and apply an appropriate discrete distribution in context*.

Our numerical questions were standard, akin to a usual exam, and we often used randomized numbers, so that different students had different correct answers. See an example in Figure 3.

Marks for the quizzes

Following [1], instead of numerical grades for quizzes, we gave only three marks to `indicate progress':

S = Success
G = Getting there
N = Not yet.

In a digital quiz (multiple choice + numerical question) we gave S if both answers were answered 100% correctly, G if one of the answers (numerical or multiple choice) was answered 100% correctly, and N otherwise.

In multiple choice questions, we didn't give partial scores to minimize the chances of success by a random guess.

In numerical questions, we counted only correct answers, with a margin to account for rounding errors. We made it clear to the students that by `I can execute a procedure' we mean: bringing calculations to the correct answer. As a consequence, there were no partial points, but this was amply compensated by the enormous advantage of immediate grading and feedback, and revision opportunities.

Open questions were graded manually. Since it was only one question per competency, and not all students chose to make the quiz in that week, we always could grade within a week.

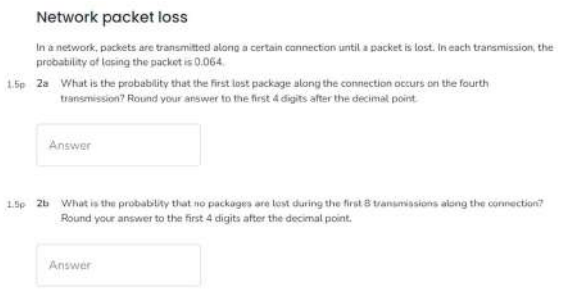


Figure 3 Example of a numerical question on competency C4 - *I can choose and apply an appropriate discrete distribution in context*.

We used 3 criteria:

1. The solution is correct.
2. All variables are defined.
3. All steps are explained.

We gave S if all three criteria were met; G if 2 out of there criteria were met; N otherwise. We always gave a detailed feedback that students could use when retrying the quiz. We gave S even if there were slight flaws in a write-up, as long as the student confidently demonstrated understanding and ability to explain. Looking back, the three criteria and grading rules were not very convenient because often a student met all three criteria partially. In these cases, we struggled to communicate which criteria were met and why we gave G or N.

Altogether, the quizzes had high requirements: 100% correct answers, correct procedures, good write-up. But we also offered a high support with immediate feedback and multiple attempts. We were happy to learn that this is exactly the right principle in mentoring young people: *high standards - high support* [3].

Final grade

Number of S's and G's The final grade was defined by the number of S's and G's that the student has obtained on the competency quizzes. Here, we had the conversion rule that S in 1 competence = G in 2 competencies.

Open question requirement For passing the course, we required at least one S in an open question, and the number was higher for a higher grade (see below). This gave the competencies with open question a higher weight. We found this fair because these competencies are important for Computer Scientists, and because writing a probabilistic argument is an important skill.

Quizzes at home don't count Technically, any student could access weekly quizzes on ANS, also at home. However, we registered attendance, and quizzes made at home didn't count for the grade.

Exam requirement At the exam, we used STEP sticks that locked student's browsers. During weekly tests, we didn't have this facility. After a discussion with the examination board, we imposed an additional requirement: S in at least 4 competencies during one exam session (either at the exam or at the resit). Again, S in one competency could be replaced by G in two competencies. Importantly, for the exam requirement, students could redo the competencies where they already had S or G before. If they did so, they did not improve their grade, but this gave them a choice to meet the exam requirement more securely. It was up to the students how many new S's and G's they tried to score during the exam.

Computing final grade To summarize, here are our requirements for each grade, across weekly quizzes, the exam, and the resit:

- Grade 6: S in 8 competencies in total; S in 1 competency with an open question; S in 4 competencies at the exam or resit.
- Grade 7: S in 10 competencies in total; S in 1 competency with an open question; S in 4 competencies at the exam or resit.
- Grade 8: S in 12 competencies in total; S in 1 competency and G in 1 competency with an open question; S in 4 competencies at the exam or resit.
- Grade 9: S in 13 competencies and G in 1 competency in total; S in 2 competencies with an open question; S in 4 competencies at the exam or resit.
- Grade 10: S in 15 competencies in total; S in 2 competencies and G in 1 competency with an open question; S in 4 competencies at the exam or resit.

In Figure 4, we made a hypothetical example of a student with final grade 7. In the last column, in yellow, are S's and G's scored at the exam. This student did very well on the new competencies C14, 15, but they also retook familiar competencies C1, 3, 4. Quizzes made at home in week 7 don't count for the grade.

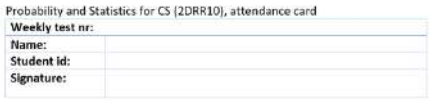
Creating quizzes

For each competency, we made 6 quiz-

Example: Grade=7

Competency #	week2	week3	week4	week5	week6	week7	week8	Exam	Resit	Total
1	S	no attempt						S		S
2	G									G
3			S					S		S
4			S					S		S
5			G	N						G
6			N	G						G
7				N	S					S
8					S					S
9						at home				
10										
11							S			S
12							S			S
13							N			
14								S		S
15								G		G
16										

Figure 4 Results of a hypothetical student, final grade 7. Attempts at home don't count. At the exam, the student may attempt quizzes for new competencies, or repeat the ones they passed before.


Probability and Statistics for CS (2DRR10), attendance card

Weekly test nr:	
Name:	
Student id:	
Signature:	

Figure 5 Attendance slip.

zes: 2 practice quizzes, 2 weekly quizzes, 1 exam, and 1 resit. Altogether, 16×6=96 quizzes. This is a lot of work, even if we had some question banks already available. Since the course had 300 students, we had 4 instructors. We have divided the competencies, four per instructor: C1-4, C5-8, C9-12, C13-16. Each instructor made 24 quizzes, 6 per assigned competency. It is still a lot, but definitely doable.

Grading

Only the competencies with an open question had to be graded, which was done by the four instructors. Each instructor had a group of about 75 students, and they graded their own group.

Altogether, it was not a lot of grading. Indeed, there were only three competencies with exactly one open question. In the weekly quizzes, not all students attempted these open questions, and the quizzes were spread over the weeks, so we could always grade within a week. Also, students chose to attempt the competency themselves, so even wrong and badly written solutions were still meaningful, and we were happy to engage with students' work and give feedback. Plus, we also knew that our feedback was useful because the students could retry. This made grading easier and more satisfying.

It was very helpful that we gave only three marks. Usually it was very clear which mark to give. This saved us a lot of exhausting decision making of traditional grading: to give or not to give those 0.5 points? As we mentioned before, possibly the criteria for open questions can be improved to make the grading even easier.

Organization and Logistics

We hired five teaching assistants (TA's): one per instructor, and one for administration.

At the beginning of each quiz, we distributed attendance slips on paper (see Figure 5). Then a TA collected the slips and marked the attendance in a shared Excel file.

During the quiz, the instructors and the TA's were walking around to make sure that the students had only ANS on their screens.

After the quiz, one of the instructors (Nelly) downloaded the results and saved them in a folder shared with the TA responsible for the grade administration. This TA combined the quiz results with attendance, and posted the results (S,G,N) on Canvas, together with a preliminary grade (provided the student will meet the exam requirement). Already around week 5-6, the students who consistently did well on quizzes starting seeing their preliminary grade turn into a 6 or higher.

We were lucky with an especially talented TA for grade administration who has even created a manual, which we can now use in the next editions of the course.

The four pillars of alternative grading

The book [1] describes the four pillars of alternative grading: clear standards, helpful feedback, marks indicating progress, and revisions without penalty. Altogether, these pillars uphold the feedback loop, vehicle of any learning process. Here is how we experienced the four pillars.

Clear standards These were our 16 competencies. We believe that this worked very well. Here are some quotes from the students:

> "[...] I appreciate this system, because it is completely transparent what is asked from us [...]"

> "The competency system is very useful in helping the student understand their shortcomings and strengths"

This is exactly what we wanted to achieve!

Besides, we believe it is very valuable that the students know exactly which competencies they mastered and which they skipped. This structures their prior knowledge of probability in subsequent courses (see our previous column on the prior knowledge problem [4]). For instance, suppose a later course on randomized algorithms uses Markov chains. Naturally, the teacher will expect this prior knowledge from our course. But if a student consciously skipped competencies C9 and C10, they have no illusion of their prior knowledge. They know they must revise that material.

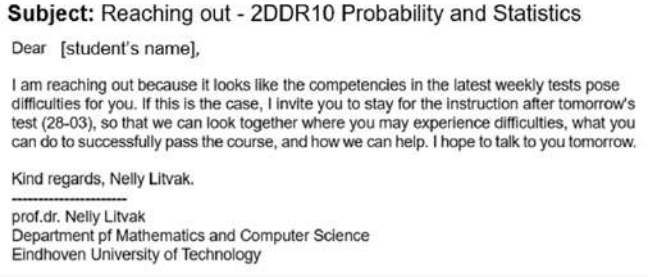
Helpful feedback Digital quizzing software gave immediate feedback on numerical and multiple choice questions. Instructors gave timely feedback on open questions. We believe that the most helpful part was that the students could use the feedback to redo the quizzes in the same competency, on which they received the feedback.

One the other hand, we also observed that even in this new grading system, students often saw feedback mostly as criticism. For instance, this was a quote from evaluations:

> "[..] grading [of open questions] is really particular about `notation' and showing all work"

Clearly, this student didn't find our feedback very helpful. We are now looking into new insights and ideas on how to give helpful and motivating feedback to young people [3]. We hope to report more on this in future issues of the column.

Marks indicating progress It helped us to have only three marks, the grading was easy. However, having letters or phrases instead of grades didn't make much difference to the students. Mentally, the students still perceived S, G and N as a grade, not as an indication of progress. Students are very used to the idea that high grade is good and low grade is bad. We noticed


Subject: Reaching out - 2DDR10 Probability and Statistics

Dear [student's name],

I am reaching out because it looks like the competencies in the latest weekly tests pose difficulties for you. If this is the case, I invite you to stay for the instruction after tomorrow's test (28-03), so that we can look together where you may experience difficulties, what you can do to successfully pass the course, and how we can help. I hope to talk to you tomorrow.

Kind regards, Nelly Litvak.

---

prof.dr. Nelly Litvak
Department pf Mathematics and Computer Science
Eindhoven University of Technology

Figure 6 Reaching out to struggling students.

Illustration: Mara Chelărescu

Figure 7 The four pillars of alternative grading.

that renaming grades did not help much. However, according to [3], another approach could be helpful: constantly repeat to the students what the grade means. An N for a competency doesn't mean that you are not-smart-enough or failing. It is just a current status in that particular competency. We will try to communicate this better next year.

Revision without penalty Along with *Clear standards*, this was a huge advantage of alternative grading. Students liked this a lot, here are some quotes:

> "[.. .] we do not have to stress about lacking in one or two competencies as we can easily make up for it [...]"

> "I really liked the new examination system [...]. It made it a lot less stressful as we had multiple tries per competency."

> "I like that not everything comes down to the final exam [...] ."

Multiple attempts felt very natural to us. We believe that revisions without penalty are simply fair!

Better learning

In our previous column [5] we wrote what is needed for learning: engagement, inconsequential error feedback, and spacing.

Engagement means actively working with the material. *Spacing* means that students work on the course regularly. We have achieved engagement and spacing because 100% of the students were present every week for the quizzes. Here are some testimonies of engagement:

> "The weekly tests are nice and make you actively learn the material"

> "[...] the weekly tests forced us to actively learn the course material, which I think will help the knowledge stick longer.''

About 10% of the students came to the resit to take some more quizzes and improve their grade, although they already passed the course. We did not mind that they chose to work on the course some more!

Inconsequential error feedback is exactly what we did: error feedback and revision without penalty.

In addition, students found the new system less stressful, which is also good for learning.

At the end, almost 80% students passed the course, and the most common grade was 7. While this is higher than with a standard exam, we cannot conclude much on the basis of this result, because grades commonly are higher with alternative grading [1]. We believe, however, that our grades adequately match the abilities and the interests of this group.

Students in control

One crucial advantage of alternative grading is that the students are in control of their results. They know exactly what to do to get a desired grade. We believe the students experienced this exactly as intended. For example, at the tests, we often saw students strategically choosing which quizzes to try. Many students liked having their results under control:

> "I love the grading scheme! It removes so much randomness in the grade - grades don't depend on a single random exam."

Some students even expressed doubts that they had too much control:

> "It's great, but for first year students, I believe, there is too much freedom."

> "[..] learning harder competencies properly is sort of discouraged as succeeding at easier ones is much much easier.''

Answering these doubts, we trust that students are mature enough to choose what grade they want. As for focusing on simpler material, students commonly do this in the traditional grading as well, maybe unconsciously. We believe that no system can eliminate such slacking completely, but the advantage of our system is that the slacking is a transparent and conscious choice.

Reaching out to struggling students

While the course was running, David Clark, a co-author of [1], published blogpost [6] about how alternative grading helps to support struggling students. It was just on time, because we were approaching the last week of the course!

Inspired by [6], each instructor looked at their group and identified students who started out well, but were getting all N's

Illustration: Mara Chelărescu

Figure 8 Students in control: catching a 9.

lately. In Nelly's group there were 7 such students out of 75. We wrote an e-mail to them, see Figure 6. Importantly, the subject said `Reaching out' so that our intention to help was immediately clear. Not all students replied, but some did, and some came to the instruction for help. To those who responded, we suggested to make practice quizzes and gave them feedback. Students appreciated this. Here is what one student wrote:

> "[...] thanks a million for the feedback, if I do pass the quiz tomorrow, and the course in general it is not lost on me that this correspondence has been instrumental for it."

This student was just one G short of passing after the exam, and has passed the course after the resit.

What we will improve next year

Better explanation of the system. A common complaint of the students was that the new system was hard to understand:

> "I think the structure with the competencies and weekly tests S and G system is very confusing for 1st year students to understand.''

> "[...] this system with competencies was more than confusing for the vast majority of students, I saw questions being asked even on week 8."

At some point, even a study advisor wrote to us asking for explanations! In week 8, right before exam, the most common question was: `For the exam requirement, can I retake quizzes where I already have an S?' (The answer is, yes!)

We now have a lot of feedback from the study advisor and the students, and we will pay special attention to explain the system better next year.

Revising competencies Students experienced that C1-4 were too easy, and C7 was far too hard. Also, students often felt that the emphasis on open questions was too strong:

> "[...] the written tests take disproportionally more time, which makes taking them extra stressful.''

Students also didn't like that there was no weekly quiz on C15, 16, as this material was offered in the last week.

Next year we will combine some competencies and split others to make them more equal in difficulty. We will also reduce the number of competencies from 16 to 14 so that we can give quizzes on the last 2 competencies in week 8.

Larger question bank At the moment, we have exactly the minimal number of questions to fill all quizzes. We want to extend the question bank, and possibly choose questions at random from the question bank.

Humane alternative grading

Traditional exams bring upon us, teachers, the uninspired `will-it-be-on-the-exam' questions and dreadful grading.

But students suffer even more! They feel that their entire future depends on a `random exam'. Only two weeks ago, in another course, Nelly observed a student who was explaining each problem, bright and clear, to their friends. But at the intermediate test, speeding through 8 problems in 45 minutes, they read two questions incorrectly, and scored only 6/8. It was soul crashing for the young person. There is no good reason why this student couldn't try again.

The new system felt as a great relief because we could set high standards (good write-up; 100% correct answers), and yet be more relaxed and sympathetic to our 300 anxious first-year students.

We were especially happy to read this very rewarding testimony:

> "Thanks for being human. I wish that other courses would treat us in the same way as we were treated in this course.''

Acknowledgement

Last, but not least, we want to thank all the wonderful people that have made the course a success. First, we thank the remaining three instructors Vinay Kumar Bindiganavile Ramadas, Fabian Burghart and Florian Henning, who have created all digital tests with Nelly. We are also very grateful for the enthusiastic and reliable student assistants of the course, Pascal Otjens, Andrei Pătularu, Diego Rivera Garrido, Floortje van Santen, Georgi Tsonkov. Finally, we would like to thank our colleagues from the computer science domain as well as the course support at TU/e, who have provided invaluable help and support throughout the course.

References

1 Clark, D., & Talbert, R. (2023). *Grading for Growth: A Guide to Alternative Grading Practices that Promote Authentic Learning and Student Engagement in Higher Education*. Taylor & Francis.

2 Litvak, N., & Weedage, L. (2023). Do we teach what we preach? *Nieuw Archief voor Wiskunde*, December 2023, pp. 233-238.

3 Yeager, D. (2024). 10 to 25: The Science of Motivating Young People. *Random House*.

4 Litvak, N., & Kula, F. (2023). The prior knowledge problem. *Nieuw Archief voor Wiskunde*, September 2024, pp. 161-166.

5 Litvak, N (2024). How students learn. *Nieuw Archief voor Wiskunde*, June 2024, pp. 112-116 .

6 Clark, D. (2024) How alternative grading helps me support struggling students (*gradingforgrowth.com*).

7 Haidt, J. (2024). *The anxious generation: How the great rewiring of childhood is causing an epidemic of mental illness*. Random House.

Wil Schilders
Mathematics and Computer Science
Eindhoven University of Technology
w.h.a.schilders@tue.nl

Event Workshop Simons Foundation, New York, 12-13 September 2024

Workshop on Perspectives on Electronic Information & Communication in the Mathematical Sciences

The Mathematics & Physical Sciences division of the Simons Foundation hosted a Workshop in New York, September 12-13, concerning Perspectives on Electronic Information & Communication in the Mathematical Sciences, organized by the IMU Committee on Electronic Information and Communication (CEIC). Many aspects were discussed, including an important joint statement by IMU and ICIAM on the challenges of citation cartels and predatory publishers. Wil Schilders was invited as president of ICIAM, here is an account of his impressions.

Introduction

The Committee on Electronic Information and Communication (CEIC) is a standing committee of the International Mathematical Union (IMU), whose mandate is to review the development of electronic information, communication, publication, instruction, and archiving in the Mathematical Sciences and to represent the IMU accordingly at an international level. It serves the mathematical community as a whole by providing advice, endorsing standards, articulating best practice recommendations, and by the development of electronic infrastructure. Ilka Agricola of the Philipps-Universität Marburg in Germany is the chair of the CEIC, she was the main organizer of the workshop which brought together leading mathematicians, researchers, librarians and professionals who are interested in an interdisciplinary exchange of ideas that aligns with the CEIC's goals. Topics covered included:

1. The future of mathematical archiving and research data infrastructure
2. Steps towards a Global Digital Math Library
3. The challenges of citation cartels and predatory publishers
4. Open access and copyright strategies
5. New challenges: what is the impact of AI and formal proof assistants on mathematical publishing?

The meeting surveyed progress in these fields with an alternation of short presentations and discussion sessions. The third topic was especially of interest to us, as early in 2024 ICIAM and IMU started to discuss a joint statement as a reaction to the decision of the organization Clarivate in November 2023 to ban all mathematicians in their list of highly cited researchers. We used the workshop to further discuss this joint statement. More on this below.

The workshop was held in the premises of the Simons Foundation on 5th Avenue, New York, a splendid location. At 160 5th Avenue, there is the main meeting area for workshops, very well equipped, modern, and the catering was really fantastic, starting with a luxurious breakfast each morning. Visitors are very well treated! On the other side of the street, 162 5th Avenue, the Flatiron building, is the building where many employees are working. Every two floors have their own theme: 3rd and 4th floor host the CCM (Centre for Computational Mathematics), other floors then host also topic areas starting with CC: Centre for Computational Quantum, Centre for Computational Biology, etc. Again, everything looks very modern, and I am sure that the people working here feel very comfortable. For more information, see for example the website of CCM [1]. The Simons Foundation also provides funding [2].

The future of mathematical archiving and research data infrastructure

As more and more journals are becoming digital – with several being exclusively available in digital format – it is increasingly important to establish viable means for ensuring free access to back issues of mathematical journals. For the mathematics community, it would be optimal to have the shortest possible window before open access. On the other hand, a short window would put financial pressure on learned societies and make it difficult to reach a broad agreement. The IMU Executive Committee (EC) – on the advice of the IMU CEIC

– created in 2021 an ad hoc Committee on Permissions with the task of preparing a report regarding the following:

- A recommendation for IMU policy on the time frame for making papers freely available after publication, together with technical details such as licenses.
- A concrete proposal for how to implement this recommendation, for example by outreach to publishers, with the particular goal of negotiating access to existing back issues.
- Any additional considerations that may affect the availability of past papers, such as the demise of publishing companies or issues with archiving.

The Committee on Permissions met from 2021 to 2024 and submitted its final report to the IMU EC in August 2024. This final report has been endorsed by the IMU EC. The report can be found at [3]. The main recommendation is that all mathematical journals should make their articles freely available within five years of publication. The discussion then concentrated on the question: What next steps can we take towards a GDML based on the report, and how to organise / fund it? Should the IMU formulate „best practice recommendations for authors"? For example, allowing the deposit of Author Accepted Manuscripts on personal websites and in public repositories with limited embargo periods. There was also much discussion on how to publish: Green Open Access, Gold Open Access, Diamond Open Access. The majority was in favour of Diamond Open Access, and this is interesting in the context of a contest that has been launched recently by the committee on Publications within PWN (and the organisation ''Mathematics in Open Access'')[4]. It also turned out during the discussion that the Simons Foundation has provided 5 million US$ to modernize the software of ArXiv; a representative of the latter organisation was also present at the meeting.

Steps towards a Global Digital Math Library

This topic was introduced by Marie Farge (CNRS-INSMI and ENS Paris), who is leading a working group that will look for a universal legal framework which would be better suited to electronic publishing, and able to protect the interests of both researchers and of the academic institutions that support them, not forgetting the taxpayers (citizens and companies) who fund public research independently of their original country. The working group will also propose that the exclusive transfer of copyright to the publisher should become non-exclusive, to take into account the contractual asymmetry between publishers and researchers (publishers require authors to submit their articles electronically in camera-ready layout and, when they are accepted after peer-review, to transfer their copyrights to them for free). The working group will look for a way to provide legal advice to researchers before they sign the contracts required by publishers, and to defend themselves if a publisher refuses to publish their article accepted by the editors. We will also examine the licenses currently used to publish research articles, analyse the recommendations published in 2024 by the IMU Committee on Permissions (see above), and consider advice that could be given to mathematicians wishing to publish in open access.

The challenges of citation cartels and predatory publishers

This topic was of the most interest to us, as ICIAM and IMU have been working together since the start of 2024 on a joint statement as a reaction to Clarivate's decision to ban all mathematicians from their list of highly cited researchers. Clarivate is a global company that provides data-driven insights and analytics for businesses and researchers. It specializes in intellectual property, scientific research, and innovation, offering tools like Web of Science, Cortellis, and Derwent for patent research, drug development, and academic performance tracking. These tools help universities, researchers, and funding agencies evaluate research productivity, collaboration networks, and the influence of academic work globally. Clarivate's annual Highly Cited Researchers (HCR) list identifies scientists and social scientists who have demonstrated significant influence in their fields through the publication of multiple highly cited papers. These researchers are recognized for being in the top 1% of citations for their respective subjects, based on data from the Web of Science.

In a Science paper [5] published January 2024, entitled ''Citation cartels help some mathematicians—and their universities—climb the rankings'', Michele Catanzaro states that widespread citation manipulation has led the entire field of math to be excluded from an influential list of top researchers (namely Clarivate's HCR list). Quoting from the paper: ''Cliques of mathematicians at institutions in China, Saudi Arabia, and elsewhere have been artificially boosting their colleagues' citation counts by churning out low-quality papers that repeatedly reference their work, according to an unpublished analysis seen by Science. As a result, their universities—some of which do not appear to have math departments—now produce a greater number of highly cited math papers each year than schools with a strong track record in the field, such as Stanford and Princeton universities.''

The paper in Science led IMU and ICIAM to start writing a joint document, arguing that current practices, such as citation counts and impact factors, are unsuitable for assessing the quality of mathematical work due to the discipline's unique publishing culture. Mathematicians tend to publish fewer papers and receive fewer citations compared to other scientific fields, making them vulnerable to bibliometric manipulation. The document discusses broader issues of fraudulent publishing, including citation cartels, paper mills, and predatory journals, which distort the academic landscape across disciplines. It advocates for the mathematical community to take control of how its research is evaluated and proposes guidelines to mitigate malicious behaviours. Finally, the statement offers practical recommendations for recognizing and combatting fraudulent publishing practices in mathematics.

As an example, see Table 1 where we list the affiliations of the 89 mathematicians that appeared in Clarivate's HCR list in 2019. Stunning fact is that the top university in this list has no mathematics department. The list also reveals problems

University Comments	# of HCRs
China Medical University Taiwan, Taiwan	11
King Abdulaziz University, Saudi Arabia	5
Queensland University of Technology (QUT)	3
Stanford University	3
University of California Los Angeles, US	3
Shandong Univ. of Science and Technology, China	2
Beijing Normal University, China	2
University of Minnesota – Twin Cities	2
University of Milano-Bicocca, Italy	2
University of Urbino, Italy	2
Amirkabir University of Technology, Iran	2
University of Michigan, US	2
University of Electronic Science and Technology of China	2

Table 1: Most frequent primary affiliations of the 89 HCRs in math (2019).

with affiliations, several of the universities listed have mathematicians on board that have many different affiliations.

Interesting is also the website [6] of retracted papers in journals. Restricted to mathematics, we observed that quite a few retracted papers can be traced back to mathematicians that were listed in the Clarivate 2019 list of HCRs. Furthermore, the database reveals that several publishers have high numbers of retracted papers in mathematics, with certain journals topping the list. Reassuring is that SIAM, which has many journals in applied mathematics, does not have any papers listed, probably due to the fact that they have excellent editorial boards.

Topics 4 and 5

The last two topics discussed, Open access and copyright strategies and New challenges: what is the impact of AI and formal proof assistants on mathematical publishing, were interesting in itself, but led to less discussion. Topic 4 concentrated on recommendations how to recognise and how to deal with the phenomenon, as author, editor, reviewer, evaluator, dean... Topic 5 was aiming at questions like: How will AI and computer proof assistants change mathematical publishing? What will be an ''original'' article? What can we do to fight AI generated fake science? Will AI be able to generate mathematical proofs in a few years? Some think this will be the case in some 5 years.

Conclusion

The workshop was very interesting, and it is good to see that the IMU is very active in the field of publication, electronic information and communication, representing the interests of mathematicians. ICIAM is also getting involved with respect to the problem of misuse and fraud with respect to bibliometrics, as a business is developing that makes use of the vulnerability of mathematics in this respect. The joint IMU-ICIAM statement will be available at the end of 2024, and we will pay attention to this in the newsletter of Platform Wiskunde Nederland as soon as it has appeared.

Types of Open Access

- Diamond Open Access: Journals that do not charge fees for authors or readers. These community-driven initiatives support academic publishing without commercial interests and cater to diverse scholarly communities. Diamond journals are typically multilingual and operate on a small scale.
- Gold Open Access: Journals offering immediate Open Access to published articles. Various business models exist, some charging article processing fees (APCs) to authors. A directory of peer-reviewed Open Access journals is available via the Directory of Open Access Journals (DOAJ).
- Green Open Access: Also known as self-archiving. Authors can publish in any journal and deposit a version of the article (often the post-print) in an Open Access repository. Some publishers enforce an embargo period before public release.

Notes

1 https://www.simonsfoundation.org/flatiron/center-for-computational-mathematics/
2 https://www.simonsfoundation.org/funding-opportunities/
3 https://www.mathunion.org/fileadmin/IMU/Report/2024-IMU_Committee_on_Permissions-FinalReport.pdf
4 https://www.mathoa.org/diamond-open-access-stimulus-fund/
5 https://www.science.org/content/article/citation-cartels-help-some-mathematicians-and-their-universities-climb-rankings
6 http://retractiondatabase.org/

Paul Drijvers
Expertisepunt Rekenen-Wiskunde
Universiteit Utrecht
p.drijvers@uu.nl

Anne Heemskerk
Expertisepunt Rekenen-Wiskunde
Universiteit Utrecht
a.g.a.heemskerk@uu.nl

Onderwijs Education

BLIK OP DE BASIS: BASISVAARDIGHEDEN REKENEN-WISKUNDE IN DE LITERATUUR

In het onderwijsveld, de politiek en de media is veel te doen over prestaties van leerlingen op het gebied van taal en rekenen. De resultaten van internationale vergelijkende studies en nationale peilingsonderzoeken laten te wensen over en lijken een dalende trend te vertonen. Als reactie hierop lanceerde het ministerie van OC&W het Masterplan Basisvaardigheden. Naast taal, burgerschap en digitale geletterdheid is rekenen-wiskunde een van de basisvaardigheden. Maar wat zijn die basisvaardigheden voor rekenen en wiskunde? Hoe wordt daar tegenaan gekeken? Om deze vraag te beantwoorden voerden Anne Heemskerk en Paul Drijvers vanuit het Expertisepunt Rekenen-Wiskunde [1] een internationale literatuurstudie uit [2]. Hieronder vatten ze de bevindingen samen. Gecijferdheid is in de gevonden literatuur de meestvoorkomende interpretatie van basisvaardigheid rekenen-wiskunde.

De basis, dat klinkt fundamenteel en vaardigheid is natuurlijk ook altijd goed. Het lijkt vanzelfsprekend dat basisvaardigheden belangrijk zijn. Hoewel er discussie is over de vraag in hoeverre de prestaties bij rekenen-wiskunde inderdaad een dalende trend vertonen, verdient de beheersing van basisvaardigheden daarom constante aandacht. Maar wat verstaan we daar eigenlijk onder, als het gaat om rekenen-wiskunde? Daarover zijn de ministeriële stukken niet zo duidelijk. Daarom vroegen we ons af: welke interpretaties van basisvaardigheden rekenen-wiskunde komen we tegen in de internationale onderzoeksliteratuur? Om deze vraag te beantwoorden hebben we een literatuurstudie uitgevoerd. In het kader 'Aanpak van het onderzoek' lees je meer over de manier waarop dit is gedaan.

Overzicht van de gevonden literatuur

Het literatuuronderzoek leidde tot een selectie van 49 artikelen, die we in vier categorieën hebben ingedeeld die elk een verschillende blik op basisvaardigheid bieden:

1. Basisvaardigheden als procedurele operaties
Dit betreft de kijk op basisvaardigheden als procedurele en geautomatiseerde basisbewerkingen. Dit is de opvatting die van oudsher het denken over basisvaardigheden overheerst.

2. Basisvaardigheden van hogere orde
Dit betreft de kijk op basisvaardigheden als hogere-orde vaardigheden zoals probleemoplossen, modelleren, interpreteren en redeneren, ingegeven door het idee dat de tegenwoordige tijd vanwege de technologische ontwikkelingen beroep doet op een ander type basisvaardigheden.

3. Basisvaardigheden als combinatie van procedurele en conceptuele kennis
Dit betreft de kijk op basisvaardigheden als het samengaan van procedurele en conceptuele kennis, die elkaar nodig hebben en versterken. Daarmee verbindt dit perspectief de eerste twee categorieën met elkaar.

4. Basisvaardigheden als gecijferdheid
Dit betreft de kijk op basisvaardigheden als de vaardigheden die burgers nodig hebben om te functioneren in de maatschappij, in het vervolgonderwijs en in

Perspectief	Frequentie
Basisvaardigheden als procedurele operaties	2
Basisvaardigheden van hogere orde	3
Basisvaardigheden als combinatie van procedurele en conceptuele kennis	14
Basisvaardigheden als gecijferdheid	30
Totaal	49

Tabel 1 Aantal artikelen per perspectief

een beroep. Het gaat om procedurele en conceptuele kennis die voorbereidt op de concrete situaties waarin ze kunnen worden toegepast. Hiervoor wordt ook de term wiskundige geletterdheid gebruikt.

Tabel 1 geeft een overzicht van de frequenties per perspectief. Slechts enkele van de gevonden publicaties focussen op basisvaardigheden als procedurele operaties en hetzelfde geldt voor de basisvaardigheden van hogere orde. De nadruk in de gevonden literatuur ligt sterk op gecijferdheid als basisvaardigheid. Dit wordt mede veroorzaakt door de internationale vergelijkende PISA-studies van OECD, die wiskundige geletterdheid nadrukkelijk tot uitgangspunt hebben gekozen. Globaal gesproken zijn de bronnen over procedurele operaties ouder dan die over hogere-orde vaardigheden en over de procedurele en conceptuele kennis. De publicaties over gecijferdheid zijn overwegend van recentere datum. De artikelen komen uit het hele bereik van hoogaangeschreven wetenschappelijke tijdschriften tot praktijkgeörienteerde tijdschriften voor leraren. De geografische herkomst van de publicaties is divers, al zijn de VS sterk vertegenwoordigd.

Basisvaardigheden als procedurele operaties

We lopen deze vier perspectieven langs. In het eerste, meest voor de hand liggende perspectief worden basisvaardigheden wiskunde gezien als de vaardigheden om basisbewerkingen te kunnen uitvoeren zoals optellen, aftrekken, delen en vermenigvuldigen. Later in de leerlijn komen daar algebraïsche procedures bij zoals haakjes wegwerken en formules vereenvoudigen. Deze basisbewerkingen moeten vlot, routinematig en geautomatiseerd met pen en papier of uit het hoofd worden beheerst. Ook feitenkennis, bijvoorbeeld het memoriseren van de tafels voor vermenigvuldiging, speelt een rol. In deze optiek zijn basisvaardigheden wiskunde dus de vaardigheid om procedures uit te voeren. Dat vraagt om de nodige oefening.

Opvallend genoeg heeft de literatuurstudie slechts twee artikelen opgeleverd waarin procedurele vaardigheid de hoofdrol speelt, die beide niet recent zijn. De eerste, de studie van Denmark en Kepner [4], betreft een vragenlijstonderzoek onder ruim 1200 wiskundeleraren in de V.S. De centrale vraag was wat deze docenten onder basisvaardigheden verstaan. Behalve elementaire rekenoperaties worden hier ook complexere operaties genoemd. Kennelijk was er ook toen al ruimte voor een bredere interpretatie van het begrip basisvaardigheid. Saillant detail is dat 53% van de respondenten stelt dat de leerlingen de basisvaardigheden minder goed beheersen dan vroeger. Dat geluid is dus niet uniek voor de huidige tijd. Het tweede artikel over procedurele kennis (Newport, [10]) is eveneens sceptisch over het niveau van beheersing van basisvaardigheden. Waarom er zo weinig is gepubliceerd over basisvaardigheden als procedurele kennis weten we niet. Is het onderwerp academisch gezien niet interessant? Zijn andere aspecten van basisvaardigheid van groter belang? Mogelijk is de wereldwijde trend om basisvaardigheden in toenemende mate te zien als meeromvattend dan procedurele kennis hier debet aan. Daarom gaan we in de volgende paragraaf nader in op basisvaardigheden van hogere orde.

Basisvaardigheden van hogere orde

Het perspectief van basisvaardigheden van hogere orde gaat ervan uit dat functioneren in samenleving en beroep niet zozeer vraagt om procedurele vaardigheid, waarvoor we immers digitaal gereedschap hebben, maar eerder om weten wanneer en waarvoor je welke basisbewerkingen kunt gebruiken en wat de resultaten betekenen. Vanuit dit perspectief maken de technologische ontwikkelingen dat het doel van reken-wiskundeonderwijs het hogere-orde denken is. Denk aan vaardigheden zoals probleemoplossen, modelleren, toepassen en abstraheren. Het gaat om kennis die je flexibel kunt inzetten voor taken die het uitvoeren van procedures ontstijgen. In dit perspectief zijn de basisvaardigheden van morgen van hogere orde dan die van gisteren.

In de literatuur zien we dit perspectief onder andere terug in de vorm van competentiemodellen. Een van de bekendste is het model van Kilpatrick et al. [8] dat vijf componenten van wiskundige bekwaamheid beschrijft:

Conceptueel inzicht – begrip van wiskundige concepten, operaties en relaties. Een leerling ziet bijvoorbeeld meteen in dat je bij een korting van 20% de oude prijs door 5 moet delen om de korting te berekenen.

Procedurele vlotheid – vaardigheid om procedures flexibel, accuraat, efficiënt en in geschikte situaties uit te voeren. Een leerling kent bijvoorbeeld de tafels voor vermenigvuldigen uit het hoofd en kan een uitdrukking als $3x + 2y - x + 5y$ snel en foutloos herschrijven tot $2x + 7y$.

Strategisch vermogen – competentie om problemen wiskundig te formuleren, te representeren en op te lossen. Een leerling ziet bijvoorbeeld hoe een verhoudingstabel kan worden gebruikt om een recept voor vier personen aan te passen voor zeven personen.

Adaptief redeneren – vermogen tot logisch denken, reflecteren, uitleggen en verantwoorden. Een leerling krijgt 640 m² als antwoord bij het berekenen van de oppervlakte van een appartement en realiseert zich dat dat onwaarschijnlijk groot is. Dit is aanleiding om alles toch nog eens na te rekenen.

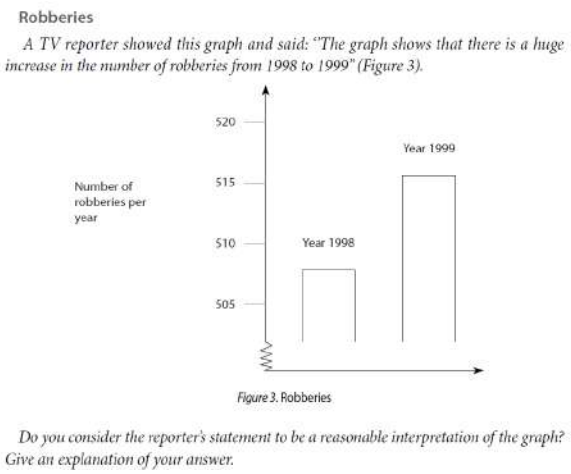
Productieve dispositie – neiging om wiskunde te zien als betekenisvol, nuttig en waardevol, met een vertrouwen in volharding en eigen doeltreffendheid. De leerling heeft bijvoorbeeld het gevoel dat vaardigheid in rekenen-wiskunde van pas komt en heeft het vertrouwen om een onbekende opgave aan te pakken.

De procedurele basisvaardigheden die in de vorige paragraaf aan de orde zijn gekomen vallen in de tweede component. Nieuw is echter de nadruk op het wiskundig denken van hogere orde in de eerste, derde en vierde component. De vijfde component heeft betrekking op de attitude ten aanzien van rekenen-wiskunde. Kilpatrick en collega's benadrukken dat deze vijf sterk met elkaar verweven zijn. Ze vormen samen de 'strengen van de kabel' van

Figuur 1 Het model voor wiskundige bekwaamheid van Kilpatrick et al.[8]

wiskundige bekwaamheid (zie figuur 1). In de nieuwe concept-kerndoelen en concept-examenprogramma's in Nederland zien we de laatste drie strengen terug als denk-werkwijzen, wiskundige (denk)activiteiten en wiskundige attitude.

Ook in landen zoals Denemarken en Duitsland zien we dergelijke modellen die de inrichting van de wiskundecurricula sturen. Dit perspectief op basisvaardigeheden als hogere-orde overstijgende competenties, met probleemoplossen als meest genoemde voorbeeld, zien we in sterkere mate terug in curriculumdocumenten die geen deel uitmaken van het literatuurcorpus. Deze interpretatie van basisvaardigheden wijkt af van de eerste interpretatie van basisoperaties en procedurele vlotheid.



Figuur 3 PISA-item in Markovic et al. [9]

Basisvaardigheden als combinatie van procedurele en conceptuele kennis

Het derde perspectief benadert de relatie tussen procedurele en conceptuele kennis en vaardigheid. In verschillende toonaangevende publicaties (Hiebert & Lefevre [6]; Rittle-Johnson [11]; Star [12]) wordt benadrukt dat de procedurele vaardigheid en conceptuele kennis geen tegenpolen zijn maar elkaar nodig hebben en versterken. Bovendien is het onderscheid soms slecht te maken. Een voorbeeld vinden we bij Kieran [7] (niet in de literatuurselectie). Ze bekritiseert hoe de linker opgave in figuur 2 wordt gelabeld als conceptuele kennis en de rechter als procedurele, terwijl het in beide gevallen gaat om inzicht in de globale structuur van de vergelijkingen.

Uit de literatuur blijkt dus dat procedurele en conceptuele kennis en vaardigheden twee kanten van de medaille van wiskundige competentie zijn. Het is niet *skills versus understanding* maar *skills and understanding*. Procedurele vaardigheid is niet per se oppervlakkig en conceptuele kennis is niet per definitie diep. Over de beste didactische aanpak wat betreft de volgorde, *skills-first* of *concepts-first*, is er geen consensus in de literatuur. Gepleit wordt voor een iteratieve aanpak, waarin beide vaardigheden elkaar afwisselen en elkaar bevorderen en waarbij begonnen wordt met een conceptuele insteek (Rittle-Johnson [11]).

Conceptual Knowledge	Procedural Flexibility
Here are two equations: $98 = 21x$ $98 + 2(x+1) = 21x + 2(x+1)$ (a) Look at this pair of equations. Without solving the equations, decide if these equations are equivalent (have the same answer), (b) Explain your reasoning.	$5(x+3) + 6 = 5(x+3) + 2x$ $6 = 2x$ (a) What step did the student use to get from the first line to the second line? (b) Do you think that this is a good way to start this problem? (c) Explain your reasoning.

Figuur 2 Conceptuele en procedurele kennis kunnen veel op elkaar lijken (Kieran, p. 168)[7]

Basisvaardigheden als gecijferdheid

De vierde en laatste kijk op basisvaardigheden, die van gecijferdheid of wiskundige geletterdheid, stelt de procedurele en conceptuele kennis van het derde perspectief nadrukkelijk in dienst van het functioneren in de samenleving. In ons literatuurcorpus komt dit perspectief frequent naar voren: 30 van de 49 publicaties hebben gecijferdheid als thema en met name in de recente jaren is deze interpretatie de gangbare. Een zeer actueel onderwerp dus in de onderzoeksliteratuur.

Uitgangspunt bij de opvatting van gecijferdheid als basisvaardigheid is dat de wereld waarin we leven rijk is aan kwantitatieve en wiskundige aspecten. Denk aan getallen en berekeningen, maar ook aan grafieken, diagrammen, statistische uitspraken, ruimtelijke oriëntatie en logische redeneringen. Daarmee hebben we te maken in dagelijks leven, vervolgonderwijs en beroepspraktijk. Gecijferd gaat dan ook om de kwantitatieve vaardigheden die een mens nodig heeft om in de samenleving te kunnen functioneren. Het omvat zowel procedurele als conceptuele kennis, maar beide worden geconcretiseerd voor functioneel gebruik in toepassingssituaties in het leven. In verschillende landen, zoals Australië en de Verenigde Staten, heeft gecijferdheid een grote plaats in curricula gekregen.

In de literatuur worden gecijferdheid en wiskundige geletterdheid breed opgevat. Er zijn verschillende definities. Geiger en collega's omschrijven gecijferdheid als

> … the knowledge and capabilities required to accommodate the mathematical demands of private and public life and to participate in society as informed, reflective, and contributing citizens (Geiger et al., p. 531)[5].

De internationale vergelijkende PISA-toetsen richten zich op wiskundige geletterdheid. Figuur 3 geeft een voorbeeldopgave, die gaat over het inzicht dat de schaling van de verticale as grote invloed heeft op de indruk die een statistische grafiek wekt.

In de gevonden literatuur is gecijferdheid of wiskundige geletterdheid de dominante interpretatie van basisvaardigheid rekenen-wiskunde. Het omvat de vaardigheden die je nodig hebt om te functioneren als burger in een samenleving die in toenemende mate doordrenkt is van wiskundige aspecten waartoe je je moet verhouden. Het hangt samen met andere vaardigheden zoals statistische geletterdheid en digitale geletterdheid. In de literatuur komt nauwelijks of niet aan de orde hoe leerlijnen voor onderwijs in gecijferdheid eruitzien die recht doen aan factoren zoals de leeftijd van de leerlingen en het schooltype.

Conclusie

Uit deze literatuurstudie concluderen we

Aanpak van het onderzoek

Op basis van een oriënterend vragenlijstonderzoek onder 48 internationale experts zijn zoektermen opgesteld waarmee vier veelgebruikte literatuurdatabases zijn doorzocht: Scopus, Web of Science, ERIC en PsycInfo. De zoekopdracht luidde:

((“basic skill*”) OR (“basic compentenc*”) OR (“numeracy”) OR (“mathematical litera*”) OR (“basic math*”) OR (“basic litera*”) OR (“math* skill*”) OR (“math* fluen*”) OR (“fundamental math*”) OR (“math* proficien*”) OR (“procedural know*”)) AND ((“math* education”) OR (“math* teaching”) OR (“math* learning”))

Dit leidde na deduplicatie tot 3279 artikelen. Daarin zijn we gaan selecteren met behulp van het AI-programma ASReview [3]. Dat resulteerde in een corpus van 49 artikelen, gepubliceerd in de jaren 1979 – 2023. Na een eerste lezing en vanuit onze kennis van de literatuur hebben we deze artikelen ingedeeld in vier perspectieven: basisvaardigheden als procedurele operaties, basisvaardigheden van hogere orde, basisvaardigheden als combinatie van procedurele en conceptuele kennis en basisvaardigheid als gecijferdheid. Deze indeling vormt de leidraad van de analyse en van dit artikel.

ten eerste dat de perspectieven van basisvaardigheden als procedurele operaties, basisvaardigheden van hogere orde, basisvaardigheden als combinatie van procedurele en conceptuele kennis en basisvaardigheden als gecijferdheid alle vier naar voren komen in de gevonden literatuur. Deze globale indeling geeft de verschillende perspectieven weer. Wel is de verdeling over deze categorieën scheef en zijn er weinig publicaties die primair over procedurele operaties of over hogere-orde vaardigheden gaan.

Ten tweede zien we consensus over het feit dat basisvaardigheden een subtiel en gebalanceerd samenspel zijn tussen procedurele vlotheid en conceptueel inzicht van hogere orde. De derde en belangrijkste conclusie is dat gecijferdheid – of wiskundige geletterdheid – verreweg de meeste aandacht krijgt in de onderzoeksliteratuur rond basisvaardigheden rekenen-wiskunde. Kennelijk wordt dit beschouwd als de belangrijkste basisvaardigheid bij rekenen-wiskunde.

Ons advies aan het ministerie is dan ook om deze internationale trend te volgen en in te zetten op gecijferdheid als belangrijkste basisvaardigheid rekenen-wiskunde. De uitdaging voor het onderwijs in basisvaardigheden rekenen-wiskunde is dan vooral om leerlijnen te ontwerpen die de gecijferdheid bevorderen van leerlingen van verschillende leeftijden en schooltypen als voorbereiding op vervolgonderwijs, beroep en functioneren in de samenleving.

Referenties en noten

1 Het Expertisepunt Rekenen-Wiskunde (https://exprw.nl/) is door OCW ingesteld om de kwaliteit van het reken-wiskundeonderwijs in Nederland te bevorderen. Het expertisepunt ondersteunt het onderwijsveld bij het implementeren van nieuwe ontwikkelingen in reken-wiskundeonderwijs rond basisvaardigheden, kerndoelen en curriculumvernieuwingen.

2 Dit artikel is gebaseerd op een rapport voor het ministerie van OC&W met dezelfde titel. Het volledige rapport is te vinden op https://exprw.nl/basisvaardigheden/. Met dank aan Peter Boon (UU), Johan Brons (SLO), Jacco-line Klein (SLO), Peter Kop (RUL), Filip Moons (UU), en Marc van Zanten (SLO) voor het meedenken, meelezen en meecoderen van de literatuur.

3 https://asreview.nl/

4 Denmark, T., & Kepner, H. S., Jr. (1980). Basic Skills in Mathematics: A Survey. *Journal for Research in Mathematics Education*, 11(2), 104-123. https://doi.org/10.2307/748903

5 Geiger, V., Goos, M., & Forgasz, H. (2015). A rich interpretation of numeracy for the 21st century: a survey of the state of the field. *ZDM - Mathematics Education*, 47(4), 531-548. https://doi.org/10.1007/s11858-015-0708-1

6 Hiebert, J., & Lefevre, P. (1986). Conceptual and procedural knowledge in mathematics: An introductory analysis. In J. Hiebert (Ed.), *Conceptual and procedural knowledge: The case of mathematics*. (pp. 1-27). Lawrence Erlbaum Associates, Inc. https://doi.org/https://doi.org/10.4324/9780203063538

7 Kieran, C. (2013). The False Dichotomy in Mathematics Education Between Conceptual Understanding and Procedural Skills: An Example from Algebra. In K. R. Leatham (Ed.), *Vital Directions for Mathematics Education Research* (pp. 153-171). Springer New York. https://doi.org/10.1007/978-1-4614-6977-3_7

8 Kilpatrick, J., Swafford, J., & Findell, B. (2001). *Adding it Up. Helping Children Learn Mathematics*. National Academies Press.

9 Markovic, O., Pikula, M., & Zubac, M. (2019). A critical analysis of the PISA mathematics tasks. *Croatian Journal of Education*, 21(1), 233-274. https://doi.org/10.15516/cje.v21i1.3245

10 Newport, J. F. (1979). Why the Decline in Student Achievement of the Basic Skills? School Science and Mathematics, 79(2), 122-124. https://doi.org/10.1111/j.1949-8594.1979.tb09461.x

11 Rittle-Johnson, B. (2019). Iterative development of conceptual and procedural knowledge in mathematics learning and instruction. In J. Dunlosky & K. Rawson (Eds.), *The Cambridge Handbook of Cognition and Education* (pp. 124-147). Cambridge University Press. https://doi.org/10.1017/9781108235631.007

12 Star, J. R. (2005). Reconceptualizing procedural knowledge. *Journal for Research in Mathematics Education*, 36(5), 404-411.

Open podium

Brieven van lezers
brieven@nieuwarchief.nl

Mijnenveld

"Onderwijsramp door realistisch rekenen", zo luidt de kop van een nieuwsbericht in het *Nieuw Archief voor Wiskunde* van juni 2024. Er is geen bewijs voor deze stelling. De KNAW-commissie die vijftien jaar geleden het rekenonderwijs op de basisschool onderzocht, constateerde dat bezorgdheid over de rekenvaardigheid van onze kinderen op zijn plaats is, maar dat er geen overtuigend verschil in het effect van de realistische en de traditionele didactiek is aangetoond. De sleutel tot verbetering werd gezocht in het niveau van de leaar, want de opleiding en nascholing waren in ernstige mate geërodeerd. Aldus het KNAW-advies [2].

Er blijft onverminderd reden tot bezorgdheid, niet alleen over de rekenvaardigheid op de basisschool, maar over het gehele niveau van het basis- en voortgezet onderwijs. De PISA-scores dalen, de Onderwijsinspectie trekt aan de bel, de instellingen voor hoger onderwijs zien een achteruitgang in de kennis en vaardigheden en ook in de werkhouding van hun eerstejaarsstudenten. Het funderend onderwijs staat voor nieuwe uitdagingen: oplopende lerarentekorten, een grotere variëteit in de maatschappelijke achtergrond van de leerlingen, afleiding door sociale media, nieuwe onderwerpen zoals burgerschap en digitale geletterdheid. En dat is maar een greep.

Nederland moet zich afvragen wat het van het onderwijs verwacht en hoe het dat voor elkaar gaat krijgen. Voor het vervolgonderwijs is hiertoe een aanzet gegeven in de vorm van een toekomstverkenning [1, 3]. Ik doe hier een oproep tot een onderzoek naar en een debat over het constructief doen, met de kracht van argument en evidentie. Hoe het niet moet, hebben we geleerd van het didactiekdebat, dat ontaardde in een geloofsstrijd met standpunten die uiteindelijk even extreem als onhoudbaar waren.

Bij de aanbieding van het KNAW-advies [2] aan staatssecretaris Marja van Bijsterveldt zei KNAW-president Robbert Dijkgraaf: "Ik heb de commissie een mijnenveld ingestuurd en ik ben blij dat ze heelhuids zijn teruggekeerd." Dat kwam omdat de mijnen aan de extremen van het strijdperk liggen. In het midden loopt een goed begaanbaar pad.

Jan Karel Lenstra
Centrum Wiskunde & Informatica, Amsterdam
jkl@cwi.nl

Referenties

1 T. Eimers (red.). *Vandaag is het 2040; toekomstverkenning voor middelbaar beroepsonderwijs, hoger onderwijs en wetenschap*. KBA Nijmegen & ResearchNed, Nijmegen; Andersson Elffers Felix, Utrecht; CHEPS, Enschede; Kohnstamm Instituut, Amsterdam. 2023.
2 KNAW. *Rekenonderwijs op de basisschool; analyse en sleutels tot verbetering*. 2009.
3 PWN-commissie Onderwijs. *Samenvatting van Vandaag is het 2040, de kamerbrief van de minister van OCW en de reactie van de Onderwijsraad*. 2024, https://platformwiskunde.nl/wp-content/uploads/2024/09/20240224-2040-samenvatting.pdf.

Nicos Starreveld
Korteweg-de Vries Institute for Mathematics
University of Amsterdam
Platform Wiskunde Nederland
n.j.starreveld@uva.nl

Interview Jan-Willem van Ittersum

Feeling like an explorer

On the 16th of October, mathematician Jan-Willem van Ittersum, who completed his PhD in 2021 at Utrecht University, was awarded the Christiaan Huygens Science Prize for his dissertation "Partitions and quasi-modular forms; variations on the Bloch-Okounkov theorem". He received the prize - consisting of an amount of ten thousand euros and a bronze sculpture of Christiaan Huygens - from Minister Bruins of Education, Culture and Science. This happened during a festive meeting in Voorburg. Mathematicians Rosa Schwartz and Lucas Slot were also nominated for the award and received an honorary distinction.

To celebrate the occasion, Nicos Starreveld interviewed Jan-Willem to discuss his research, his future ambitions, and the wonderful mathematics problems which keep him motivated and enthusiastic. Currently, Jan-Willem is doing a postdoc at the University of Cologne. Let us travel back in time and follow him in his mathematical steps that led him to his current position.

Jan-Willem, first, my congratulations on receiving this prestigious award. You received your PhD in 2021 on a topic with a very long history, namely partitions of integers. You have found a very special connection between partitions and modular forms, building upon the work of Bloch and Okounkov. Before we discuss the mathematics, I am curious to hear more about how you discovered mathematics. Why did you want to become a researcher?

"Thank you for the nice words, I really enjoyed the evening in Voorburg. The ceremony was very well organized and the atmosphere was great. From a young age I was fascinated by mathematics. I didn't know what I wanted to do when I would grow up, but I knew I wanted to do something with mathematics. This fascination grew stronger during my studies at Utrecht University. The first time I came in contact with research was during my bachelor thesis, in algebraic number theory.

My supervisor, Gunther Cornelissen, asked me to read an article because there was a sentence he did not understand. I found the article very interesting; I started experimenting and working out examples to understand the results better. At some point I also thought I had proven a theorem, but it turned out I misunderstood some concepts. But this is how it goes with research. At the end, I managed to prove a new result, which was very nice. This was my first encounter with research, and I knew that I wanted to keep doing it and keep exploring open questions."

Gunther was also your supervisor during your master thesis, and later also your promotor, together with Professor Don Zagier from the Max Planck Institute for Mathematics in Bonn. Could you say something about your collaboration?

"After my bachelor I already knew I wanted to continue as a researcher. When I was finishing my master Utrecht University gave the opportunity to students to submit their own research proposal for a PhD project, which was possible because the university had received a grant from NWO. This was a great opportunity.

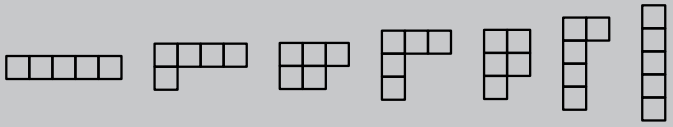
Advised by Gunther and Don, I found a very interesting problem to work on and I submitted a proposal, which was accepted.

The collaboration with Gunther was always very pleasant and motivating. Something I find unique in him is how he collaborates with students. He is very good in tailoring a project to the needs and level of a student. He recommended it would be useful to ask Don as the second supervisor for my research, since the topics I was interested in were related to research Don had done in the past.

The topic of my PhD was inspired by an article Don had written. The article was motivated by some problems from geometry. Don he made a translation to a problem about partitions, which he then related to modular forms. I found this relation of partitions and modular forms very interesting, and we decided to investigate it further."

Understanding partitions

Central to Jan-Willem's research is the concept of a partition of a number. A partition of an integer is a way to express the number as a sum of positive integers, where the order of the terms does not matter. For example, the partitions of 5 are given by 5, 4+1, 3+2, 3+1+1, 2+2+1, 2+1+1+1, and 1+1+1+1+1, which can be represented graphically by their Young diagrams as



Partitions of numbers have intrigued mathematicians since the 18th century. For instance, is there a systematic way to find all partitions of a natural number? Such questions quickly proved to be very challenging, even for today's most powerful computers. To get an idea: the number 100 has 190,569,292 partitions. If you try to find them all, then you are probably doomed to make a mistake or get exhausted and never want to do math again!

Mathematicians therefore had to be creative to better understand partitions. Leonard Euler was the first to use functions to study partitions. He developped a method to determine the number of partitions of a number by using power series. Euler proved that

$$\sum_{n=0}^{\infty} p(n)q^n = \prod_{j=1}^{\infty} \frac{1}{1-q^j}. \qquad (1)$$

To prove this formula, and to show why it is useful in understanding partitions, Euler had to work on it for many years. By working on the infinite product on the right he managed to prove a wonderful result, the Euler pentagonal theorem. This theorem gives a recursive expression to compute partitions, namely

$$p(n) = p(n-1) + p(n-2) - p(n-5) - p(n-7) - \cdots = \sum_{k \neq 0} (-1)^{k-1} p(n-g_k).$$

where the summation is over all nonzero integers k (positive and negative) and g_k is the k-th generalized pentagonal number. The infinite sum is in practice a finite sum, because $p(n) < 0$ for negative numbers. For many years this recursive formula was the only way to compute and work with partitions. Until 1918, when Hardy and Ramanujan proved the asymptotic expression

$$p(n) \sim \frac{1}{4n\sqrt{n}} \exp\left(\pi\sqrt{\frac{2n}{3}}\right).$$

You can experiment yourself with this formula and investigate how good it approximates $p(n)$. In Wolfram Alpha you can compute the approximation of the summation for rather high values of n. Ramanujan proved many results about partitions. A collection of his work relying on modular arithmetic bears the name "Ramanujan's congruences". Furthermore, in 1937 Hans Rademacher improved this asymptotic result of Hardy and Ramanujan by providing a convergent series expression for $p(n)$, which is considered up to today to be the best closed form expression possible.

Foto: Paul Voorham

Jan-Willem van Ittersum received the Christiaan Huygens Science Prize. Rosa Schwartz and Lucas Slot received an honorary distinction.

What is the motivation to study this bracket (see equation (2) on the next page)?

"From a mathematical perspective, you should interpret the q-bracket in the following sense: suppose you want to investigate a sequence of numbers. On most occasions, the best way to start is by using the generating series of the sequence, where the terms of the sequence are the coefficients of each term, like Euler did in computing the generating series of partitions, for example. Then you use the obtained results to deduce information about the sequence. What is very surprising and interesting is that only for very specific choices of weight-functions the q-bracket is a (quasi)modular form.

During my research I wanted to understand for which families of weight-functions the q-bracket will constitute a family of quasimodular forms. Bloch and Okounkov had proven this for shifted symmetric functions, I proved it also for other cases, for example symmetric functions. If there are more such families is still an open question.

Here in Cologne we are also interested in the modular properties of the q-bracket; for instance, we can use so-called mock-modular forms to prove some new results. Cologne is in some sense a center for research in modular forms, with two professors who are experts in this topic, Kathrin Bringmann and Sander Zwegers."

Did you feel well prepared to work on this topic when you started on your PhD?

"When I started, I found it very exciting and a little bit scary. But I had followed a course on Modular Forms by Sander Dahmen and Peter Bruin during my master, which triggered my interest on this topic. It also helped a lot that I could apply for the position by submitting my own proposal.
The process of working on this topic was very exciting and I enjoyed it a lot. From the first day, I tried to work out many examples to understand how it works. And understanding good examples turned out to be pivotal for my research. In the literature we could find various specific examples of functions which lead to quasimodular forms. But, besides the result of Bloch and Okounkov, it was not known whether you could find an algebra of functions which leads to an algebra of quasimodular forms. To build confidence and get insights on how this could work we had to work out many concrete examples. I remember that when I was still at school, one specific mathematics teacher stimulated me to participate in the first round of the Mathematical Olympiad. I performed well and I got invited to a series of trainings. There I learned how to approach mathematical problems where I had no idea how to start. These problem-solving skills are very important, also today in my research."

Which research direction did you choose after your PhD?

"Towards the end of my PhD, I was discussing with mathematicians at conferences about interesting topics to work on. One of these mathematicians was Henrik Bachmann, who got me interested in the so-called MacMahon's q-series, which are also related to partitions and modular forms.

In another conference I was discussing with Ken Ono about quasimodular forms and their properties, when we realized there was a very interesting connection between MacMahon's series and prime numbers. We got enthusiastic about it and decided to work on it further. This collaboration led to the recent publication "Integer partitions detect the primes", where we prove that certain equations involving MacMahon's partition functions can "detect" the primes. In this article we found infinitely many equations, which are linear combinations of MacMahon's parti-

Partitions in the 21st century

Back to today. Since the time of Euler and later Ramanujan mathematicians have been working on partitions and have developed new methods to understand them. From the results presented above, it is evident that heavy machinery is necessary to extract information about them. But there is a cost: the more you want to understand, the more advanced the methods become. There is no royal road to understanding them. The information about partitions is hidden within various other objects. Moreover, the kind of information you can extract about partitions also varies. Euler proved a recursive formula, while Ramanujan and Hardy obtained an asymptotic result. But we can also investigate deeper and more subtle properties of $\mathrm{p(n)}$, instead of its value. Mathematicians have found patterns and connections with other well understood mathematical concepts which can yield information about partitions.

The theorem of Bloch-Okounkov is such an example: it provides a connection between partitions and modular forms. This connection between partitions and modular forms was observed before. Namely, the product Euler found in (1) is, up to a factor of $\mathrm{q}^{1/24}$, equal to the modular Dedekind eta-function. This relation was important in the work of Hardy and Ramanujan to prove the asymptotic expression for $\mathrm{p(n)}$. But the Bloch-Okounkov theorem pushes this framework further.
A modern technique to study partitions, which is also central in Jan-Willem's research relies on the q-bracket, defined as

$$< f >_q = \frac{\sum_{\lambda \in p} f(\lambda)\, q^{|\lambda|}}{\sum_{\lambda \in p} q^{|\lambda|}}. \qquad (2)$$

where $\mathscr{P}$ is the collection of all partitions. You can view the sum in the numerator as the infinite sum

$$\sum_{n=1}^{\infty} \sum_{\lambda \vdash n} f(\lambda)\, q^{|\lambda|}.$$

We are interested in the functions f for which $< f >_q$ is a nice function with good algebraic properties. We can notice that the denominator in the definition of $< f >_q$ is exactly the power series in (1), which is known by the work of Euler. In his dissertation Jan-Willem proved that for the family of symmetric functions the q-bracket is a quasimodular form. Which means that it inherits many nice properties and symmetries that these well understood mathematical objects have.
For a more mathematical and detailed overview of Jan-Willem's work we refer the reader to the nice overview he wrote for the Nieuw Archief voor Wiskunde in 2022 [1].

tion functions, which are zero if and only if you plug in a prime number. This was a surprising result, because there is no evident reason why partitions should be related to the prime numbers! Partitions are related to addition, while prime numbers are related to multiplication and factorization. It is very interesting that there is a connection between them."

From your experiences until now, which are the important open questions in your field at the moment?

"Modular forms are very well understood. Most open problems about modular forms concern their relations to other mathematical objects, for example in the Langlands program. An open question which I am very interested in concerns families of functions which are not exactly modular, but look like such forms. There are nowadays various types of modularity, for example quasi-, mock or quantum modular forms. I am quite interested in such variations of modularity, in particular for series for which the precise modularity is not yet understood."

Is mathematics something you do on your own or working together in a team?

"I think you need to find a balance, between understanding the topic on your own and collaborating or discussing with colleagues. Being in a team also helps when you get stuck, which naturally occurs in research. Often it helps a lot to push yourself to gather your ideas, organise them, and explain them to someone else. When you work independently you get stuck in your own ideas sometimes. Discussing with other mathematicians helps gain new insights and ideas. If I reflect on my previous projects, the projects where I collaborated with other mathematicians are those I enjoyed the most.

In general, I often feel like an explorer when I am investigating a new mathematical problem, similar to the analogy Andrew Wiles shared in the BBC Documentary about Fermat's Last Theorem [2]. He mentioned that when you start with a new problem, you feel like you are in a dark room and you don't see anything in it, but as you start exploring you start touching objects and it becomes clearer how the room looks like. Doing mathematics feels like this, like an explorer discovering new things which sometimes reveal a great beauty. Whether I do it on my own or with colleagues, this is always the part I enjoy the most, the feeling of being an explorer!"

References

1 Een recept voor quasimodulaire vormen, Jan Willem van Ittersum, *Nieuw Archief voor Wiskunde*, September 2022.

2 BBC, *Horizon*, 1995-1996, Fermat's Last Theorem.

3 Math Is Still Catching Up to the Mysterious Genius of Srinivasa Ramanujan, Jordana Cepelewicz, *Quanta Magazine*, October 2024.

Nieuws (vervolgd)

| News (continued)

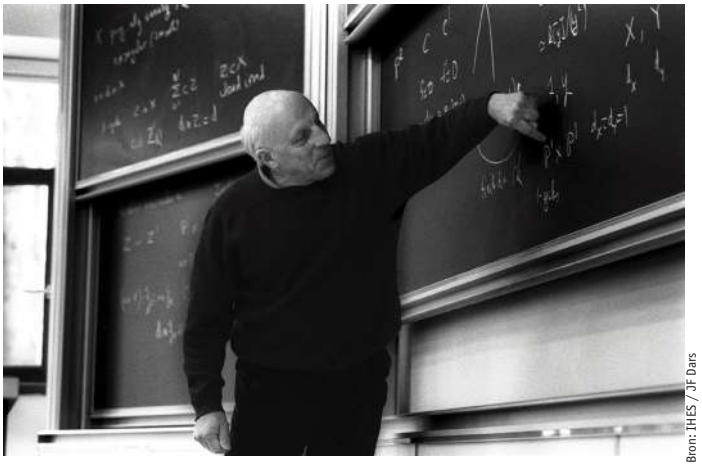
Nederlandse wint prijs voor beste proefschrift in Engeland

Serte Donderwinkel heeft met haar proefschrift *The structure of large random graphs* in oktober 2024 een prijs van de Royal Statistical Society gewonnen. Deze bekroont iedere twee jaar het beste in het Verenigd Koninkrijk geschreven proefschrift in de toegepaste waarschijnlijkheidsleer. Donderwinkel is in 2022 in Oxford bij Christina Goldschmidt gepromoveerd op toevalsgrafen en universaliteit en werkt momenteel als universitair docent aan de Rijksuniversiteit Groningen. De jury prees onder meer het allooi van haar bewijzen en de hoge kwaliteit van haar dissertatie.

Aernout van Enter

Franse meetkundige Pierre Cartier overleden

De gevierde wiskundige Pierre Cartier heeft op 17 augustus de geest gegeven. Hij is bekend van bijvoorbeeld de naar hem genoemde klasse divisoren in de algebraïsche meetkunde alsook Cartierdualiteit voor commutatieve groepenschema's en de Cartierbewerking voor differentiaalvormen op variëteiten in positieve karakteristiek. De Fransman is aan de École Normale Supérieure in Parijs gepromoveerd bij Henri Cartan en werd in 1955 lid van het genootschap Bourbaki. Na een korte verpozing in Princeton is hij achtereenvolgens professor geweest in Straatsburg en bij het IHES, het CNRS, de École Polytechnique en de École Normale Supérieure. Daarnaast was hij erg geïnteresseerd in de geschiedenis en filosofie van wiskunde en haar ontplooiing in ontwikkelingslanden. Cartier heeft de Prix Peccot en Ampère gewonnen en is 92 jaar geworden. *smf.emath.fr*

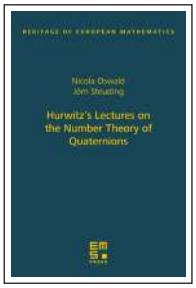


Bron: IHES / JF Dars

Pierre Cartier.

Boekbesprekingen

| Book Reviews



Nicola Oswald, Jörn Steuding

Hurwitz's Lectures on the Number Theory of Quaternions

Heritage of European Mathematics
EMS Press, 2023
xviii + 293 p., prijs $ 85.00
ISBN 9783985470112

Adolf Hurwitz schrijft op 15 september 1919 in zijn dagboek dat hij van zijn arts een brief heeft gekregen waarin staat dat hij sinds jaren te maken heeft met hartproblemen en een nierziekte; dit attest is nodig om vrijgesteld te worden van het geven van colleges in het komende wintersemester. Een seminarie wil hij nog wel geven. Hij woont dan in Zürich. De notitie over dit attest staat temidden van uitvoerige aantekeningen over het thema *Die Zahlentheorie der Quaternionen im Gauss'schen Zahlkörper*. Na het overlijden van Hurwitz op 18 november 1919 stuurt zijn vriend Hilbert een brief aan Hurwitz' weduwe Ida Samuel, waaruit op te maken valt dat Hurwitz zich alleen nog goed voelde als hij morfine gebruikte. Ondanks zijn tanende gezondheid voltooit Hurwitz toch nog een boek over quaternionen en hij gebruikt daarvoor als basis een beknopt artikel uit 1896: *Über die Zahlentheorie der Quaternionen* in de *Göttinger Nachrichten (1896), 313-340*. Hij stuurt een aantal exemplaren van het boek aan vrienden en collega's. Het is in de herfst van 1919 uitgegeven bij Julius Springer met als titel *Vorlesungen über die Zahlentheorie der Quaternionen*. Het is een juweeltje van een boek en makkelijk als pdf op internet te vinden. Het is elementair maar daarom zeker niet eenvoudig; de bewijsvoering is vaak heel slim, subtiel en vindingrijk. Dit boek van Hurwitz is in Engelse vertaling en voorzien van commentaar opgenomen in het hier te bespreken boek van Nicola Oswald en Jörn Steuding. Daarnaast is er nog een tweede primaire bron die een grote rol speelt in hun boek: de zogeheten *Mathematische Tagebücher*. Hurwitz is continu bezig met wiskunde en noteert allerlei thema's zeer uitgebreid en goed leesbaar in dikke schriften voorzien van een datum waarop hij met het thema bezig is. Deze dertig zogeheten *Mathematische Tagebücher* bestrijken de periode 1882 tot en met 1919; zeer indrukwekkend om te bekijken. Het totaal betreft circa 6000 pagina's. Ze zijn te vinden op www.e-manuscripta.ch. Als u meer wilt weten over wat er aan manuscripten van Hurwitz is bewaard, dan verwijs ik u naar de paragraaf *Über den handschriftlichen Nachlass* in band II van de uitgave van zijn verzameld werk.

Het boek van Nicola Oswald en Jörn Steuding bestaat uit zeven hoofdstukken. Het is goed leesbaar, mooi uitgevoerd en zeker te gebruiken om meer te weten te komen over de quaternionentheorie van Hurwitz en ook over recentere ontwikkelingen. De zeer uitgebreide literatuurlijst is daarbij zeker behulpzaam. Er is veel werk verricht aan historisch onderzoek over Hurwitz. Hoofdstuk I schetst in kort bestek de relevante historische ontwikkelingen, voornamelijk op het gebied van getaltheorie, die uitmonden in de quaternionen. Hurwitz' boek over quaternionen, bestaande uit 12 *Vorlesungen*, vormt de kern en is in een Engelse vertaling van de hand van Steuding opgenomen als hoofdstuk II. Per 'Vorlesung' zijn commentaren toegevoegd die soms wel en soms ook niet te maken hebben met quaternionen. Het is een terecht eerbetoon

Redactie: Hans Cuypers en Hans Sterk
Secretariaat: Enna van Dijk

Review Editors NAW - MF 5.092
Faculteit Wiskunde & Informatica
Technische Universiteit Eindhoven
Postbus 513
5600 MB Eindhoven

reviews@nieuwarchief.nl
www.win.tue.nl/wgreview

aan Hurwitz dat het boek verschijnt in de serie *Heritage of European Mathematics*.

Ik geef een kort overzicht van het quaternionenboek van Hurwitz. Hierin staat de verzameling J van de zogeheten *gehele* quaternionen centraal. Deze verzameling bestaat uit de quaternionen van de vorm $\frac{1}{2}(k_0+k_1i_1+k_2i_2+k_3i_3)$ met k_0,k_1,k_2 en k_3 geheel en alle oneven of alle even. Voor i_1,i_2,i_3 gelden de welbekende eigenschappen. De verzameling J_0 van de quaternionen van Lipschitz bestaat uit geheeltallige combinaties van $1,i_1,i_2,i_3$ en is bevat in de gehele quaternionen van Hurwitz. In J zijn de 24 eenheden voorhanden die Hurwitz nodig heeft om zogeheten priemquaternionen te kunnen definiëren. In J is het mogelijk een Euclidisch algoritme te definiëren, weliswaar linkszijdig of rechtszijdig want J is niet commutatief, maar in J_0 is dat niet mogelijk. Verdere onderwerpen die aan bod komen zijn: de permutaties van de gehele quaternionen, de grootste gemene deler en idealen van quaternionen, even en oneven quaternionen, geassocieerde en primaire quaternionen, en priemquaternionen. Veel aandacht wordt besteed aan het modulorekenen in J met de moduli 2, $1+i_1$, $2(1+i_1)$ en een oneven geheel getal m. Bij het modulorekenen naar een oneven geheel getal m wordt de zogeheten *Zuordnungssatz* bewezen die Hurwitz een van de opmerkelijkste stellingen uit de getaltheorie van de quaternionen noemt. Deze stelling komt erop neer dat je, alles modulo m rekenend, aan het quaternion $k=k_0+k_1i_1+k_2i_2+k_3i_3$ met k_0,k_1,k_2 en k_3 geheel, een 2 bij 2 matrix toekent van gehele getallen met de eigenschap dat die afbeelding een bijectie is die de optelling en vermenigvuldiging respecteert en dat de norm van het quaternion gelijk is aan de determinant van de matrix (weer modulo m).

Deze stelling is onder andere essentieel bij zijn bewijs later van de vier-kwadratenstelling van Lagrange. Als centrale stelling volgt dan de zogeheten *Zerlegungssatz* of *Ontbindingsstelling* waarin onderzocht wordt op welke manier de gehele quaternionen als product van priemquaternionen zijn te schrijven. Ten slotte bepaalt Hurwitz als toepassing van zijn theorie op hoeveel manieren een positief geheel getal te schrijven is als som van vier kwadraten, de vier-kwadratenstelling, en bepaalt hij een methode om magische vierkanten te bepalen; de aanleiding hiervoor is dat hij via Legendre een magisch vierkant kent waarover Euler in 1770 aan Lagrange heeft geschreven, en dat hij in de veronderstelling verkeert dat de theorie van Euler hierover nog niet gepubliceerd is. Die veronderstelling is overigens onjuist.

In hoofdstuk V is een artikel van Hurwitz opgenomen (eveneens in het Engels vertaald door Steuding) met de oorspronkelijke titel ‘Über die Komposition der quadratischen Formen’, *Math.Ann.* **88**, 1–25 (1922). Ook deze vertaling is voorzien van diverse commentaren. Ik denk toch dat het beter was geweest te blijven bij het thema quaternionen; in dagboek 30 zijn daarvoor zeker geschikte stukken te vinden. Ik vind de commentaren (van de hand van Jörn Steuding) zeker interessant, maar vaak iets te ver verwijderd van de quaternionentheorie zoals Hurwitz die behandelt. Ik zou liever gezien hebben dat Steuding een soort leeswijzer geschreven had bij het boek van Hurwitz.

In de hoofdstukken III en IV geeft Nicola Oswald historische achtergronden en zij doet dat steeds op een interessante en boeiende manier. Oswald had zich al eerder verdiept in Hurwitz. In haar proefschrift met de titel *Hurwitz’s Complex Continued Fractions, A Historical Approach and Modern Perspectives* kunt u onder andere nog veel meer biografisch materiaal over Adolf Hurwitz vinden, zeer lezenswaardig allemaal. In hoofdstuk III schrijft zij over de inhoud en ontstaanswijze van het boekje van Hurwitz. Zij kadert dit in in de ontwikkeling van de algebraïsche getaltheorie in de negentiende eeuw. Ze geeft van Hurwitz en Lipschitz een biografische schets en evalueert beider aanpak van de quaternionentheorie met de nadruk op de algebraïsche gehelen, die een centrale rol spelen in hun rekenwijze. Ten slotte gaat ze na welke rol boeken zoals het boekje van Hurwitz speelden in het onderwijs en het onderzoek van die tijd. Hoofdstuk IV richt zich op de *Mathematische Tagebücher* en in het bijzonder op het gedeelte dat te maken heeft met quaternionen. Zij vermeldt onder andere in welke dagboeken Hurwitz bezig was met het bestuderen van quaternionen, het begint al in zijn dagboek van 1896. Zij gaat nader in op deze dagboeken en na beschrijving van de dagboeken 14, 15 en 25 gaat ze speciaal in op dagboek 30, het volgens haar meest interessante voor wat betreft quaternionen. Het hoofdstuk is rijkelijk voorzien van foto’s van de dagboeken, vaak ook nog met een Engelse vertaling. Zoals al vermeld, de dagboeken van Hurwitz zijn werkelijk indrukwekkend.

Ik vermeldde eerder al dat de commentaren van Steuding soms wijdlopig zijn en ga er op een paar gedetailleerd in. Een voorbeeld betreft Vorlesung 11, waar Hurwitz Lagrange’s vier-kwadratenstelling bewijst. Steuding besteedt in zijn commentaar zeven bladzijden aan de zèta-functie, terwijl het verhaal van Hurwitz twee bladzijden beslaat. Hij noemt een aantal personen die de stelling ook bewezen hebben en oordeelt, zonder onderbouwing overigens, dat het bewijs van Hurwitz het meest natuurlijke is. Bij Vorlesung 12, over magische vierkanten, gaat Steuding meer in op het werk van Euler dan dat van Hurwitz.

Op het einde van het boek van Hurwitz staan een 12-tal voetnoten. Steuding vertaalt die naar het Engels, maar doet er verder niets mee. Toch denk ik dat je daar op in moet gaan, want zo ontdek je best mooie boeken en iets over de genealogie van de ideeën van Hurwitz: onder andere boeken van Felix Klein en werk van Eduard Study waarin de relatie tussen quaternionen en de formules van Euler voor rotaties aan de orde komt. In Vorlesung 8 heeft Hurwitz het over de zogeheten *Zuordnungssatz*, die volgens hem een van de meest opmerkelijke stellingen uit de getaltheorie van quaternionen is. Als je dan het gedeelte van een boek van Klein-Fricke bekijkt waar Hurwitz naar verwijst, dan herken je veel van wat Hurwitz in Vorlesung 8 doet. Felix Klein was zijn leermeester, bij wie hij op zijn 18-de in de leer ging; Klein eiste veel van hem en dat leidde tot een geestelijke uitputting met alle gevolgen van dien conform een schrijven van zijn echtgenote Ida Samuel. U kunt daarover lezen in het proefschrift van Nicola Oswald.

In hoofdstuk VI schetst Steuding hoe de quaternionentheorie na Hurwitz verder gegeneraliseerd is; hij gaat in op het werk van Grassmann, Clifford, Frobenius, Study, Du Pasquier (een leerling van Hurwitz) en Dickson, steeds voorzien van literatuurverwijzingen. Het boek van Dickson, *Algebras and their arithmetics*, uit 1923 krijgt aparte aandacht. Dickson schrijft in zijn voorwoord dat het vanzelfsprekend is dat men eerst zijn aandacht richtte op de *arithmetic of quaternions* zoals gedaan door Lipschitz en Hurwitz en dat daarna pas, ofschoon verbazingwekkend langzaam, de theorie van de *arithmetic of algebras* evolueerde. Dit boek is als een van de eerste Engelstalige wiskundeboeken op initiatief van Andreas Speiser vertaald naar het Duits met als titel *Algebren und*

ihre Zahlentheorie (1927). Het argument was dat wiskundigen rond Emmy Noether, Emil Artin en Helmut Hasse er ook kennis van wilden opdoen. Steuding schrijft nog dat in het geweld van die generalisaties en abstracties het oorspronkelijke werk van Hurwitz nu bijna vergeten is; maar ook dat zonder dit fundamentele werk een algemene theorie van algebra's ondenkbaar zou zijn. Voor wat betreft de klassenlichamentheorie beschouwt Steuding deze theorie als een generalisatie van Fermat's twee-kwadraten stelling omdat dat bewijs steunt op de rekenkunde van $\mathbf{Z}[i]$.

Hoofdstuk VII, het laatste hoofdstuk, heeft een filosofisch karakter. Nadat de meningen van Poincaré, Dickson en Weil over het belang en de rol van de quaternionen in de wiskunde zijn vermeld, stellen Oswald en Steuding zich de vragen: *Wat maakt een bewijs een nieuw bewijs en wat maakt een theorie een nieuwe theorie?* De eerste vraag wordt gerelateerd aan de bewijzen van de vier-kwadratenstelling van Lagrange; in dit hoofdstuk wordt nog een bewijs van Euler geschetst dat gebruikmaakt van Fermat's methode van de oneindige afdaling. De vraag die de auteurs zich daarbij stellen is: welk bewijs is het meest natuurlijke? Bij de tweede vraag gaat het om alle ontwikkelingen die te maken hebben met de vier-kwadratenstelling van Lagrange die wellicht op enig moment als geheel een theorie genoemd kunnen worden. Het hoofdstuk eindigt met een brief van Hurwitz aan George Pólya van 31 augustus 1919 waarin hij schrijft dat hij, als zijn gezondheid het toelaat, nog van plan is om thema's aan zijn boek toe te voegen die door doctoraalstudenten en promovendi uitgewerkt kunnen worden. Kortom, Hurwitz wil nog veel toevoegen aan zijn quaternionentheorie.

Tot slot, het boek van Nicola Oswald en Jörn Steuding samen met de twee voornoemde primaire bronnen biedt een mooie toegang tot het werk van Adolf Hurwitz.

In 2015 hebben zij al iets soortgelijks gedaan, maar dan vanuit het perspectief van de zèta-functie waarin Hurwitz zijn leven lang al geïnteresseerd is geweest. Hun artikel is getiteld: *Aspects of zèta-function theory in the mathematical works of Adolf Hurwitz* (arXiv). In dit artikel vindt men ook interessant biografisch materiaal over Hurwitz. Kortom, het boek zet Hurwitz in de schijnwerper en maakt je enthousiast om zijn *Mathematische Tagebücher* nader te bekijken. *Math Dicker*

Hans Fischer

Signaalanalyse en Digitale Signaalverwerking

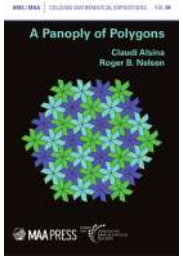
Fouriertheorie, systeemtheorie en theorie van digitale filters

Epsilon Uitgaven, 2024
xv + 375 p., prijs € 32,00
ISBN 9789050412025

In de serie Epsilon Uitgaven is onlangs verschenen *Signaalanalyse en Digitale Signaalverwerking* van Hans Fischer. Het boek is qua opzet en formaat vergelijkbaar met *Digitale Signaalbewerking* van Van den Enden en Verhoeckx dat niet meer leverbaar is. Het ingangsniveau is vwo met wiskunde D en het boek is geschreven voor studenten, docenten, professionals en geïnteresseerden in wiskunde, informatica, natuurwetenschappen en techniek. Het eerste deel is voorbereidend waarbij de benodigde wiskunde wordt opgefrist, zoals basiskennis van Fourierreeksen, Fouriertransformatie en convolutie. Dit beslaat ongeveer het eerste derde deel van het boek. Vervolgens worden lineaire tijdcontinue systemen, de discrete Fouriertransformatie en de Fast Fourier transform, de z-transformatie en lineaire tijddiscrete systemen behandeld, wat ongeveer het tweede derde deel van het boek beslaat. In het laatste derde deel komen digitale filters ter sprake. Elk hoofdstuk begint met een korte inleiding en eindigt met opgaven, waarvan de antwoorden achterin het boek gegeven zijn.

Het boek ziet er aantrekkelijk uit met veel figuren en veel voorbeelden; de belangrijke formules zijn omkaderd en afleidingen worden met vele kleine stappen gegeven. Zoals de ondertitel laat weten, betreft het alleen de theorie; toepassingen van digitale signaalverwerking worden niet genoemd, evenmin onderwerpen als wavelets, adaptieve filters, kwantisatie, en effecten van eindige woordlengte en samplerate conversie. In de literatuurlijst zijn alleen geraadpleegde bronnen opgenomen; klassiekers als de boeken van Rabiner & Gold, Schafer, Lyons, Roberts & Mullis, en andere meer recente boeken ontbreken.

Voor hen die willen beginnen met het bestuderen van de theorie van digitale signaalverwerking, is het goed geschreven en prettig leesbare boek van Fischer een aanrader. *Ronald Aarts*



Claudi Alsina, Roger B. Nelsen

A Panoply of Polygons

AMS/MAA Press, 2023
xi + 267 p., prijs $ 65.00
ISBN 9781470471842

Heel goed passend in de reeks recent uitgekomen (en in dit prachtblad besproken) boeken over driehoeken (*The Secrets of Triangles*), over vierhoeken (*A Cornucopia of Quadrilaterals*) en over vijfhoeken (*Pentagons and Pentagrams*), is er nu *A Panoply of Polygons*, een zeer rijk, maar ook rijk (helaas in zwart-wit) geïllustreerd boek over veelhoeken met vijf of meer zijden. De reden dat de auteurs Alsina en Nelsen (al dan niet samenwerkend, met zijn tweeën in totaal reeds goed voor 13 voorgaande MAA-AMS-publicaties) zich beperken zal duidelijk zijn, er is heel veel te vinden over drie- en vierhoeken.

De acht hoofdstukken hebben enigszins saaie en voorspelbare titels (Polygon Basics, Pentagons t/m Octagons, Many-sided Polygons, Miscellaneous Classes of Polygons en Polygonal Numbers), maar de inhoud vergoedt veel, heel veel. Dit zeer compact en effectief geschreven boek bevat per hoofdstuk ongeveer een tiental doenbare *challenges* (93 in totaal) die achterin volledig en helder worden uitgewerkt (zo hoort het ook) en geeft een mooi overzicht van wat je allemaal zou kunnen uitzoeken op het gebied van veel-

hoeken. Ook de ervaren lezer wordt regelmatig verrast met of weggezakte, maar heel vaak relatief onbekende zaken. Dat begint wat mij betreft al met een voor mij onbekende definitie van *convex* (een veelhoek waar geen twee zijden elkaar snijden is convex als die veelhoek in zijn geheel aan één kant ligt van elke lijn die een zijde bevat) en toch ook van *concaaf* (niet convex uiteraard, maar dan moet er minstens één lijn die veelhoek in minstens vier punten snijden). Vele fraaie tot verpletterende stellingen komen voorbij zoals: Als een koordenveelhoek wordt opgedeeld in driehoeken door diagonalen (dat kan uiteraard op meerdere manieren), dan is de som van de stralen van de ingeschreven cirkels van die driehoeken constant! En kende u de Nederlandse wiskundige Frans van Schooten (1615-1660)? Waarschijnlijk wel zijn charmante lemma: Als P een punt is op de omgeschreven cirkel van gelijkzijdige driehoek ABC dan is de langste van de drie afstanden PA, PB en PC gelijk aan de som van de kleinste twee.

De basis van veel andere mooie - ook weer minder bekende - uitspraken voor punten op omgeschreven cirkels van hogere regelmatige veelhoeken. Of de stelling (en het bewijs) dat in een regelmatige zevenhoek met zijde a en diagonalen b en c geldt dat $1/a = 1/b + 1/c$. Waarlijk schitterend is het bewijs (gebaseerd op de formule van Heron en de Stelling van Pick) van de sowieso al intrigerende uitspraak dat een roosterdriehoek (een driehoek met roosterpunten als hoekpunten) nooit gelijkzijdig kan zijn. Helemaal ingenieus (de kracht van inductie) is het minuscule bewijs dat een schaakbord van n bij n kan worden betegeld met een L-triomino mits n een macht van 2 is. Ook aardig is hoe je met een winkelhaak een hoek in drie gelijke delen kan verdelen. Dissecties komen voorbij (zie voor veel en veel meer op dit terrein het sublieme werk van de grootmeester op dit gebied Greg Frederickson) en in het bijzonder de ongelofelijke en zeer fundamentele Stelling van Wallace-Bolyai-Gerwien die zegt dat voor elk tweetal veelhoeken met dezelfde oppervlakte geldt dat de ene veelhoek kan worden verdeeld in een eindig aantal kleinere veelhoeken waarmee je die andere veelhoek kan maken.

Ook de paragraaf over de lange zoektocht naar alle verschillende types betegelingen met convexe vijfhoeken (in 1918 gestart door Karl Reinhardt, in 1975 door Martin Gardner vervolgd in een artikel in de *Scientific American*, langzaam uitgebreid onder andere door de bijdragen van huisvrouw en amateurwiskundige Marjorie Rice en de vondst in 2015 van het 15e geval en pas in 2017 besloten met het met behulp van een computer gevonden bewijs dat er precies 15 van die types zijn) is - nog steeds - interessant.

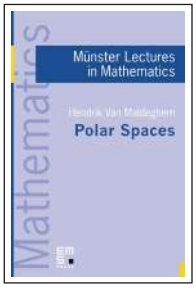
Verder wilde ik graag vermelden de door Richard Feynman zo gewaardeerde stelling, namelijk *Morrie's Law,* die stelt dat $\cos(20^\circ)\cos(40^\circ)\cos(80^\circ) = 1/8$. Het boek biedt ook een mooi overzicht van de historische ontwikkeling van het aantal bekende decimalen van het getal pi (dankzij de bekende inbedding tussen twee regelmatige veelhoeken). Meest praktische en verrassende toepassing van de vijfhoek is de afsluiting van de brandbluskraan zoals gebruikt door de brandweer, die alleen door de brandweer kan worden geopend. Ten slotte de stelling over de zogenaamde *calissons* (een Frans snoepje in de vorm van een ruit, die bestaat uit twee gelijkzijdige driehoeken). Een regelmatige zeshoek is te vullen met deze calissons in drie oriëntaties en nu geldt dat de drie aantallen van de in een van de drie oriëntaties gebruikte snoepjes gelijk zijn. Het gegeven meta-bewijs is waarlijk elegant. Je kunt blijven citeren.

Voor de gezegende docent die een klasje wiskunde D (waar meetkunde gelukkig nog op het programma staat en ook het zo belangrijke bewijzen nog de aandacht krijgt die het verdient) mag lesgeven, is dit boek een schatkamer van leuke en fascinerende weetjes en stellingen om achteloos rond te strooien ter lering ende vermaak. Als men dan nog niet massaal wiskunde gaat studeren, weet ik het niet meer. Het boek is zonder meer te volgen voor de B-leerling vanaf 5 vwo.

De schrijvers maken vele uitstapjes naar de realiteit, door vele foto's te plaatsen van gebouwen (bijvoorbeeld een hexagonale snackbar in Eindhoven), planten, betegelingen, munten en verkeersborden en geven een wel heel uitgebreide bibliografie van de gebruikte bronnen. Ondanks de weer ouderwets hoge prijs (het blijft jammer dat de AMS vooral dit soort meer populaire boeken niet makkelijker en dus goedkoper beschikbaar stelt) en de vele bekende zaken die voorbijkomen (maar dat is niet te vermijden als je deze opzet kiest) zou ik dit boek zeer willen aanbevelen.

Joop van der Vaart

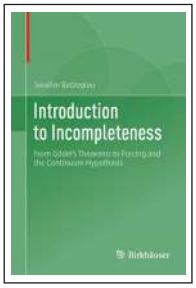
Recent verschenen publicaties. Als u een van deze boeken wilt bespreken of als u suggesties heeft voor andere boeken voor deze rubriek, laat dit dan per e-mail weten aan reviews@nieuwarchief.nl.



Hendrik Van Maldeghem

Polar Spaces

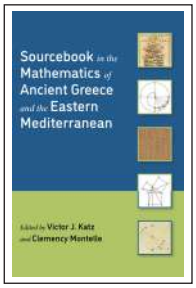
EMS Press, 2024
ISBN 9783985470808
https://ems.press/books/mlm/295



Serafim Batzoglou

Introduction to Incompleteness
From Gödel's Theorem to Forcing and the Continuum Hypothesis

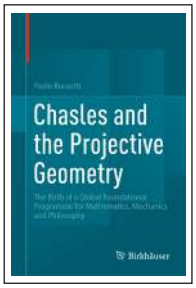
Springer, 2024
ISBN 9783031642173
https://link.springer.com/book/10.1007/978-3-031-64217-3



Victor J. Katz, Clemency Montelle (Eds.)

Sourcebook in the Mathematics of Ancient Greece and the Eastern Mediterranean

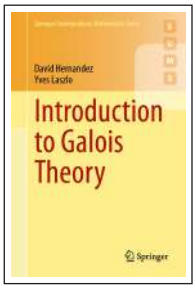
Princeton University Press, 2024
ISBN 9780691202815
https://press.princeton.edu/books/hardcover/9780691202815/sourcebook-in-the-mathematics-of-ancient-greece-and-the-eastern



Paolo Bussotti

Chasles and the Projective Geometry
The Birth of a Global Foundational Programme for Mathematics, Mechanics and Philosophy

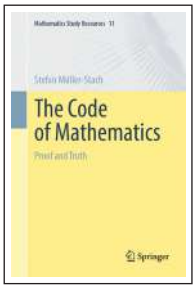
Springer, 2024
ISBN 9783031542657
https://link.springer.com/book/10.1007/978-3-031-54266-4



David Hernandez, Yves Laszlo

Introduction to Galois Theory

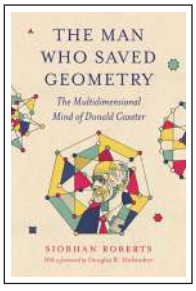
Springer, 2024
ISBN 9783031661815
https://link.springer.com/book/10.1007/978-3-031-66182-2



Stefan Müller-Stach

The Code of Mathematics
Proof and Truth

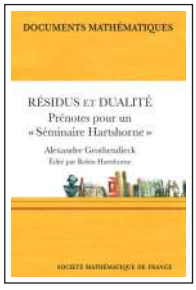
Springer, 2024
ISBN 9783662694824
https://link.springer.com/book/10.1007/978-3-662-69483-1



Siobhan Roberts

The Man Who Saved Geometry
The Multidimensional Mind of Donald Coxeter

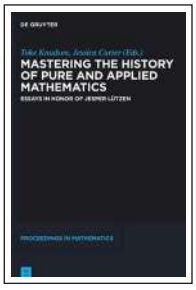
Princeton University Press, 2024
ISBN 9780691264745
https://press.princeton.edu/books/paperback/9780691264745/the-man-who-saved-geometry



Robin Hartshorne (Ed.)

Alexandre Grothendieck, Résidus et Dualité: Prénotes pur un ``Seminaire Hartshorne"

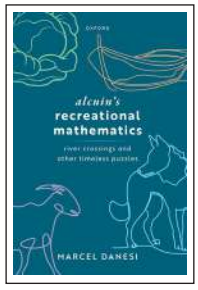
Société Mathématique de France, 2024
ISBN 9782856299838
https://smf.emath.fr/publications/residus-et-dualite-prenotes-pour-un-seminaire-hartshorne



Toke Knudsen, Jessica Carter (Eds.)

Mastering the History of Pure and Applied Mathematics
Essays in Honor of Jesper Lützen

De Gruyter, 2024
ISBN 9783110769906
https://www.degruyter.com/document/doi/10.1515/9783110769968



Marcel Danesi

Alcuin's Recreational Mathematics
River Crossings and other Timeless Puzzles

Oxford University Press, 2024
ISBN 9780198925309
https://academic.oup.com/book/58853

Problemen

| Problem Section

This Problem Section is open to everyone; everybody is encouraged to send in solutions and propose problems. Group contributions are welcome. We will select the most elegant solutions for publication. For this, solutions should be received before **15 January 2025**. The solutions of the problems in this issue will appear in one of the subsequent issues.

Problem A (proposed by Hendrik Lenstra)

Let r,k,n be integers with $0<k<n-1$ such that the set of remainders of $r,2r,\cdots,kr$ upon division by n equals the set $\{1,\cdots,k\}$. Prove that $r\equiv 1 \bmod n$ or give a counterexample.

Problem B (proposed by ...)

Let $n\geq 2$ be an integer, let $P\in\mathbb{R}[X]$ be a polynomial of degree $n-2$, and suppose that there exist $0\leq x_1<\cdots<x_n\leq n\pi$ with $P(x_i)=\sin(x_i)$ for all $i\in\{1,\cdots,n\}$. Prove that there exist distinct $i,j\in\{1,\cdots,n\}$ with $|x_i-x_j|<\pi$.

Problem C (proposed by Hendrik Lenstra)

Let $k,n>0$ be integers and let R be a commutative ring whose additive group is isomorphic to $\mathbb{Z}^n$. Let $a_1,\cdots,a_k\in R$. Prove that

$$S=\{f(a_1,\cdots,a_k)\mid f\in\mathbb{Z}[X_1,\cdots,X_k],\deg(f)<n\}$$

is a subring of R.

Edition 2024-3 We received solutions from Pieter de Groen and Carsten Dietzel

Problem 2024-1/A

Prove that for all three line segments of length 1 in a disc of radius 1 there are two of those line segments with distance at most 1.

Solution We received solutions from Pieter de Groen and Carsten Dietzel
Divide the disk into 6 equal closed pie slices. Any of the line segments contained within a slice intersects at least 3 slices: the segment either has to be a radius and thus contains the center point shared by all slices, or must be the chord between the sides of the slice and thus intersects (the boundary of) both neighboring slices. Consequently, each line segment intersects at least 2 slices. We may choose the orientation of the slices so that a given line segment intersects at least 3 slices, by placing one of the end points of the segment on the boundary of a slice. By the pigeonhole principle there is a slice with at least two line segments intersecting it, and these two segments then have distance at most 1.

Problem 2024-1/B (proposed by Hendrik Lenstra)

Let A be an abelian group and write $\mathrm{End}(A)$ for the ring of group homomorphisms from A to A. Show that A is free as $\mathrm{End}(A)$-module if and only if A admits a commutative ring structure so that the Cayley map $A\to\mathrm{End}(A)$ given by $x\mapsto(y\mapsto xy)$ is an A-module isomorphism. Show that for all subrings of $\mathbb{Q}$ and rings $\mathbb{Z}/p\mathbb{Z}$ with p a prime the Cayley map is an isomorphism, and give an example of an uncountable ring with this property.

Solution We received solutions from Carsten Dietzel
Suppose A is a commutative ring such that $\phi:\mathrm{End}(A)\to A$ given by $f\mapsto f(1)$, the in-

Redactie: Onno Berrevoets en Daan van Gent
problems@nieuwarchief.nl
www.nieuwarchief.nl/problems

Oplossingen | Solutions

verse of the Cayley map, is an A-module isomorphism. For $f,g \in \mathrm{End}(A)$ we have $\phi(fg) = f(g(1)) = f\phi(g)$, so ϕ is an $\mathrm{End}(A)$-module homomorphism. In particular, A is free as $\mathrm{End}(A)$-module.

Write $R = \mathrm{End}(A)$ and suppose we have an isomorphism $b: R^{(S)} \to A$ of (left) R-modules. Hence we have a isomorphism $R = \mathrm{End}(A) \to \mathrm{End}\big(R^{(S)}\big)$ of groups given by $f \mapsto b^{-1} \circ f \circ b$. For $f \in R$ and $g = (g_i)_i \in R^{(S)}$ we have

$$(b^{-1} \circ f \circ b)(g) = b^{-1} \circ (f \cdot b(g)) = b^{-1}(b(fg)) = fg = (fg_i)_i.$$

We may assume $A \neq 0$, hence $R \neq 0$ and $S \neq \emptyset$, otherwise all holds trivially. Choose $j \in S$ and let $x, y \in R$ be distinct. Consider the the element of $\varphi \in \mathrm{End}\big(R^{(S)}\big)$ that multiplies on the *right* by x at index j and by y elsewhere. Then by the previous there is some $f \in R$ such that φ is given by $(g_i)_i \mapsto (fg_i)_i$. At index j this gives $fg_j = g_j x$ for all $g_j \in R$, so in particular $f = x$ when taking $g_j = 1$, from which it then also follows that R is commutative. At any index different from j we have similarly that $f = y$, so $x = y$, which is a contradiction. Hence $\#S = 1$ and $b: R \to A$ is an isomorphism of R-modules. If we transport the ring structure of R along b to A, then the Cayley map is an A-module isomorphism.

Let R be a subring of $\mathbb{Q}$, or $\mathbb{Z}/p\mathbb{Z}$ for some prime p. For each $f \in \mathrm{End}(R)$ and $a, b \in \mathbb{Z}$ such that the image of a/b in R is well-defined, we have $bf(a/b) = f(a) = af(1)$, so $f(a/b) = f(1) \cdot (a/b)$. With $x = f(1) \in R$ we have $f = y \mapsto xy$, so indeed $R \to \mathrm{End}(R)$ is an isomorphism.

Consider $R = \prod_p (\mathbb{Z}/p\mathbb{Z})$ and note that it is uncountable. Then we have an isomorphism $\mathrm{End}(R) \cong \prod_p \mathrm{Hom}(R, \mathbb{Z}/p\mathbb{Z})$, where $\mathrm{Hom}(R, \mathbb{Z}/p\mathbb{Z})$ are the group homomorphisms from R to $\mathbb{Z}/p\mathbb{Z}$. It suffices to show that the natural injection $\varphi: \mathrm{End}(\mathbb{Z}/p\mathbb{Z}) = \mathrm{Hom}(\mathbb{Z}/p\mathbb{Z}, \mathbb{Z}/p\mathbb{Z}) \to \mathrm{Hom}(R, \mathbb{Z}/p\mathbb{Z})$ is surjective for all primes p. Suppose $f \in \mathrm{Hom}(R, \mathbb{Z}/p\mathbb{Z})$. For $x \in R$ we have $0 = pf(x) = f(px)$, so $\{(x_q)_q \in R : x_p = 0\} = pR \subseteq \ker(f)$. Hence f is in the image of φ.

Problem 2024-1/C (proposed by Albert Visser)

A *Gollum ring* is a ring that is isomorphic to the subring $\mathbb{Z} + 2R$ of a commutative ring R. Show that there is a sentence in first-order logic in the language of rings that is true in all Gollum rings, but not true in all commutative rings.

Solution We received solutions from Carsten Dietzel. Clarification: $\mathbb{Z}$ in $\mathbb{Z} + 2R$ refers to the image of $\mathbb{Z} \to R$.

Note that the statement $r \in 2R$ can be expressed as the proposition $\exists s \in R : 2s = r$. Let G be the Gollum ring with ambient ring R, i.e., $G = 2R + \mathbb{Z}$. An element $r \in G$ can be written as $r = 2s + m$ with $s \in R, m \in \mathbb{Z}$. As either $m \in 2\mathbb{Z}$ or $m - 1 \in 2\mathbb{Z}$, we see that either $r \in 2R$ or $r - 1 \in 2R$. Therefore, $r(r-1) \in 2R$. It follows that $r^2(r-1)^2 \in 4R = 2(2R) \subseteq 2G$, proving the following first-order formula:

$$\forall r \in G, \exists s \in G : r^2(r-1)^2 = 2s.$$

This formula does not hold in general! The ring $R = \mathbb{Z}[x]/(x^2(x-1)^2 - 1)$ is an integral extension of $\mathbb{Z}$. Then $r = \overline{x}$, the class of x, clearly satisfies the equation $r^2(r-1)^2 = 1$. An element s satisfying $2s = r^2(r-1)^2$ would therefore satisfy $2s - 1 = 0$ and can thus not be integral over $\mathbb{Z}$. The formula can therefore not hold in R.

In Problem 2023-2/C, the statement $c_{[p]} = \mathrm{gcd}\{s \in S : v_p(s) > 0\}$ is incorrect. Instead, one could prove $c_{[p]} \in \langle S \rangle$ inductively.