

Inhoud | Contents

Artikelen | Features

Onderwijs | Education

- 163 **Bespreking examen vwo wiskunde B 2014**
Wim Caspers

De oplossing | The Solution

- 167 **The latest designs**
Ross Kang

Onderzoek | Research

De vernieuwingsimpuls

Onder redactie van Petra de Bont en Lex Zandee

- 169 **Vernieuwingsimpuls en wiskunde: 14 jaar ervaring**
Lex Zandee, Petra de Bont
- 173 **Kwantumcomputers**
Ronald de Wolf
- 176 **De macroscoop**
Bert Zwart
- 180 **Stochastische integratie in Banachruimten**
Jan van Neerven
- 188 **Differentiaalmeetkunde in de getaltheorie**
Gunther Cornelissen
- 192 **Aritmetische meetkunde**
Bas Edixhoven
- 198 **Longe range stochastic dynamics**
Ronald Meester

Ken uw klassieken | Classic Article

- 208 **Wiskunde en fysica**
Herman de Lang

Geschiedenis | History

- 211 **The Weil conjectures**
Frans Oort

Voorpublicatie | Book Preview

- 220 **Waarom zou je?**
Ionica Smeets

Rubrieken | Departments

- 155 **Redactioneel** *Petra de Bont, Lex Zandee*

- 156 **Servicepagina**

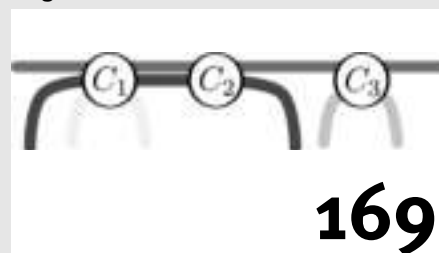
- 157 **Agenda** *Patrick Hafkenscheid*

- 159 **Nieuws** *Patrick Hafkenscheid*

- 206 **Het keerpunt van Paul van Meenen**
Ionica Smeets

- 222 **Problemen**

Uitgelicht



Vanaf pagina 169 veel aandacht voor de Vernieuwingsimpuls van NWO, met een inleiding van Lex Zandee en Petra de Bont.



In de nieuwe rubriek 'Ken uw klassieken' bespreekt Herman de Lang een klassiek artikel van Eugene Wigner.

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 een ieder 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
tel. 020-5924288
redactie@nieuwarchief.nl
www.nieuwarchief.nl

Hoofredactie

Barry Koren (b.koren@tue.nl)
Jan van Neerven (j.m.a.m.vanneerven@tudelft.nl)

Eindredactie/Bladmanager

Fred Drissen (fred@nieuwarchief.nl)

Redactie

Patrick Hafkenscheid (p.hafkenscheid@vu.nl)
Mark Timmer (timmer@cs.utwente.nl)

Bureau redactie

Gianni van den Braak
Lætitia Diemer

Medewerkers

Johan Bosman (IEM Essen), Hans Cuyper (TU/e), Gabriele Dalla Torre (UL), Christophe Debry (KU Leuven), Geertje Hek (UvA), Jinbi Jin (UL), Teun Koetsier (VU), Derk Pik (JSG Maimonides), Sjoerd Rienstra (TU/e), Hans Sterk (TU/e), Marco Streng (VU), Jan Ten Thijs Boonkamp (TU/e), Wouter Zomervrucht (UL)

Illustraties

Ryu Tajiri, Amsterdam

Advertenties

advertenties@nieuwarchief.nl

Abonnementen/Subscriptions

Abonnementenservice NAW
Postbus 2238, 5600 CE Eindhoven
admin@wiskgenoot.nl, tel. 088-2265256

Abonnementsperiode/Subscription period

Een abonnement gaat in op de dag dat uw aanmelding ontvangen wordt. De opzegtermijn is twee maanden vóór het verstrijken van de abonnementsperiode.

The subscription starts on the day that your application is received. The term of notice is two months before the end of the current subscription period.

Exchange subscriptions

Koninklijk Wiskundig Genootschap Library
Centrum voor Wiskunde en Informatica
Postbus 94079, NL-1090 GB Amsterdam
KWG-exchange@cw.nl, fax +31 20 5924026

Vormgeving

Kitty Molenaar (ontwerp)
Susanne Laws (omslag, begeleiding binnenwerk)
Programmatuur (CONTEX)
Hans Hagen, PRAGMA-ADE, Hasselt (Overijssel)
Druk
Drukkerij Ten Brink, Meppel

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.

De contributie voor gewone leden bedraagt €80 per jaar. Voor gepensioneerden en werklozen €40. Voor studenten aio's en oio's van een Nederlandse universiteit of hbo-opleiding €30. Studenten en pas afgestudeerden kunnen een jaar lang gratis lid worden. Voor leden van de wiskundige vakverenigingen VVS, NVvW en NVORWO geldt het gereduceerd tarief van €60. Leden die het Nieuw Archief voor Wiskunde niet willen ontvangen, betalen slechts €40 contributie. Losse nummers zijn te bestellen voor €20.

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 €60 instead of the full membership fee of €80 a year. Conversely, these foreign societies, as well as the VVS 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.

Instituten in Nederland en buitenland kunnen zich abonneren op het Nieuw Archief voor Wiskunde voor €100 (Nederland), €110 (Europa) of €112,50 (buiten Europa).

Website: www.wiskgenoot.nl

Ledenadministratie

Abonnementenservice NAW
Postbus 2238, 5600 CE Eindhoven
admin@wiskgenoot.nl, tel. 088-2265256
Bestuur (wiskgenoot@wiskgenoot.nl)

Geurt Jongbloed (TUD, voorzitter), Fetsje Bijma (VU, penningmeester), Joke Blom (CWI, secretaris), Onno van Gaans (UL), Jenneke Krüger (SLO), André Ran (VU), Herman te Riele (CWI), Arjen Sevenster, Mark Veraar (TUD)

Informatie voor auteurs

Kopij

Het Nieuw Archief voor Wiskunde is een geredigeerd tijdschrift. Kopij dient elektronisch te worden aangeboden aan de hoofdredactie. Uitgebreide informatie en auteursinstructies kunt u vinden op www.nieuwarchief.nl.

Reprints

Auteurs ontvangen een elektronische reprint in pdf-formaat.

Volgende nummers

nummer	verschijningsdatum	deadline kopij
4	01-12-2014	verstreken
1	02-03-2015	01-11-2014
2	01-06-2015	01-02-2015
3	07-09-2015	01-05-2015

Instituutsleden

De publicaties van het Koninklijk Wiskundig Genootschap worden mede mogelijk gemaakt door de bijdragen van de volgende instituten.



Centrum Wiskunde
& Informatica



Rijksuniversiteit Groningen



Universiteit van Amsterdam



Universiteit Leiden



Vrije Universiteit



Universiteit Utrecht



Technische Universiteit
Eindhoven



Eurandom



Technische Universiteit Delft



Universiteit Twente



Radboud Universiteit
Nijmegen

FIsme

Freudenthal Instituut

Op het omslag

In dit nummer aandacht voor wiskundeonderzoek dat gefinancierd is vanuit de Vernieuwingsimpuls van NWO. Lees over het Vidi-project van Ronald de Wolf over kwantummechanische technieken in de informatica op pagina 173. (Foto: Erik Lucero, Martinis Group, Santa Barbara, CA.)

De Vernieuwingsimpuls

Deze editie van het *Nieuw Archief voor Wiskunde* is grotendeels gewijd aan de Vernieuwingsimpuls van NWO. U zult er een beschrijving van diverse gehonoreerde wiskundeprojecten in aantreffen en ook achtergrondinformatie over dit subsidieprogramma, gefocust op de discipline wiskunde.

Heel wat wiskundigen, en niet alleen wiskundigen, fronsten de wenkbrauwen toen NWO in 2000 het nieuwe subsidieprogramma Vernieuwingsimpuls introduceerde. Deze nieuwe pot geld was bestemd voor “jonge, dwarse, onorthodoxe onderzoekers. Kenmerkend voor de onderzoekvoorstellen is dat ze risicovol moeten zijn en dat succes in het onderzoek niet verzekerd is.” Dat waren bepaald geen criteria die eerdere beoordelingscommissies bij NWO hanteerden. Ze riepen nogal wat vraagtekens op. De selectie van de kandidaten vond mede plaats op basis van een interview. Wat de wiskundigen betreft waren die interviewsessies meestal gezamenlijk met de astronomen en informatici. Dit benauwde sommige wiskundigen, bevreesd dat het niet mogelijk was een wiskundeonderzoeksvorstel begrijpelijk aan een multidisciplinaire commissie uit te leggen. Hoe zouden wiskundigen ooit succesvol kunnen opboksen tegen de indrukwekkende visuele technieken die astronomen hanteren in hun voordrachten?

Wel, nu, ruim tien jaar later, kunnen we stellen dat die Vernieuwingsimpuls, ook voor wiskundigen, en ondanks de teleur-

stellend lage honoreringspercentages, een belangrijk subsidie-instrument is. Qua honoreringspercentage blijken wiskundigen bovendien grofweg net zo succesvol als de andere twee disciplines binnen het gebied Exacte Wetenschappen. De honorering in de Vernieuwingsimpuls gaf heel wat wiskundigen de kans hun universitaire carrière te ontwikkelen. Een aantal van hen laten we in dit nummer aan het woord. De oorspronkelijke beschrijving van de doelgroep is in de loop der jaren wel aangepast en luidt nu: “excellente onderzoekers met een opvallend en origineel talent en een grote fascinatie voor het doen van uitdagend en grensverleggend onderzoek”. Dat is waar NWO altijd al naar op zoek is geweest en niet speciaal alleen in de Vernieuwingsimpuls.

Op dit moment wordt er binnen NWO gewerkt aan de nieuwe strategie voor de komende vier jaar. Het is onze verwachting dat de Vernieuwingsimpuls daar nog steeds een prominente plaats in zal nemen. Het definitieve antwoord hierop zal uiteindelijk in het najaar van 2014 bekend zijn. Excellent onderzoek en uitzonderlijke talenten zullen altijd onlosmakelijk met elkaar verbonden zijn. Een goed financieringsinstrument blijft hiervoor noodzakelijk. 

Petra de Bont en Lex Zandee, gastredacteuren
NWO, Den Haag

Servicepagina

| Service page

Koninklijk Wiskundig Genootschap

□ Secretariaat

Joke Blom, CWI
Postbus 94079, 1090 GB Amsterdam
wiskgenoot@wiskgenoot.nl
www.wiskgenoot.nl

□ Verhoging lidmaatschapstarieven

Zoals vastgesteld in de Algemene Ledenvergadering van 17 april zullen met ingang van 2015 de lidmaatschapstarieven verhoogd worden. De nieuwe tarieven kunt u vinden op www.wiskgenoot.nl/wordlid/tarieven.html.

□ Stieltjesprijs 2013

Benjamin Sanderse en Pavel Zorin-Kranich hebben ex aequo de Stieltjesprijs voor het beste wiskundeproefschrift van 2013 gewonnen. De Stieltjesprijs wordt vanaf 1996 jaarlijks toegekend. Tot 2009 stelde het Thomas Stieltjes Institute for Mathematics de prijs beschikbaar; vanaf 2010 wordt de prijs toegekend door WONDER. De prijs bedraagt 2500 euro, beschikbaar gesteld door Stichting Compositio Mathematica. De 2500 euro voor de extra prijs is beschikbaar gesteld door de Thomas Stieltjes Stichting.

Platform Wiskunde Nederland

□ Bureau PWN

Science Park 123, L013, 1098 XG Amsterdam
bureau@platformwiskunde.nl
pr@platformwiskunde.nl (publiciteit)
Tel: 020-5924006/06-51892525
www.platformwiskunde.nl

□ PWN Nieuwsbrief

PWN publiceert maandelijks een PWN Nieuwsbrief, die op de website te vinden is. Actuele PWN-informatie wordt zowel via de website

als via Twitter gegeven. Voor overig wiskundenuws: www.platformwiskunde.nl/newsfeed.

European Mathematical Society

□ EMS website

www.euro-math-soc.eu

□ Executive Committee EMS Council

Op de Council meeting van 28 juni 2014 zijn er drie nieuwe leden in het dagelijks bestuur van de EMS gekozen: President: Pavel Exner (Academy of Sciences of the Czech Republic), secretaris: *Sjoerd Verduyn Lunel* (Universiteit van Utrecht) en penningmeester: Mats Gyllenberg (University of Helsinki, Finland).

□ EMS Newsletter

Van de drie-maandelijks EMS Newsletter is de elektronische versie van de meest recente uitgave beschikbaar op de EMS publications website: www.ems-ph.org/publications.php.

International Mathematical Union

□ IMU website

www.mathunion.org

□ Fieldsmedailles 2014

Tijdens de opening van het ICM 2014 zijn op 13 augustus 2014 de Fieldsmedailles, de Nevanlinna Prize, de Gauss Prize en de Chern Medal Award uitgereikt. De winnaars van de Fieldsmedailles waren Maryam Mirzakhani (Stanford University, Riemannoppervlakken), Martin Hairer (University of Warwick, SPDEs), Manjul Bhargava (Princeton, getaltheorie) en Artur Avila (IMPA, Brazilië en CNRS, dynamische systemen).

□ IMU Newsletter

The twee-maandelijks IMU Newsletter is beschikbaar via www.mathunion.org/imu-net.

Recente publicaties van het KWG

□ **Indagationes Mathematicae** (www.elsevier.com/locate/indag, gratis toegang via 'View Articles')
Special issue 'Probability and Numbers', Frits Beukers, Frank den Hollander, Robbert Fokink, Cor Kraaikamp (eds.), Volume 25, issue 4, 2014.

Zaanen Centennial Special Issue, R. Kaashoek, B. de Pagter (eds.), Volume 25, Issue 2, 2014.

□ **Epsilon Uitgaven** (www.epsilon-uitgaven.nl)

77. *Hemelverschijnselen nabij de Horizon*, Henk Broer, €22, 2013.

76. *Inleiding in de Statistiek*, F. Bijma, M. Jonker en A. van der Vaart, €32, 2013.

75. *An Invitation to Functional Analysis*, B. de Pagter en A.C.M. van Rooij, €25, 2013.

□ **Zebra-reeks** (Epsilon Uitgaven)

40. *Kantelpunten en alternatieve evenwichten*, Lia Hemerik, Egbert van Nes en Theo-Jan van de Pol, €10, 2014.

39. *De juiste ondersteuning*, Dolf van den Hombergh en Leon van den Broek, €10, 2014.

38. *SpiroSporen*, Stephan Berendonk en Leon van den Broek, €10, 2013.

37. *Moiré-kunst met niveaulijnen*, Luc Van den Broeck, €10, 2013.

Manuscripten voor Epsilon Uitgaven kunt u mailen naar redactie@epsilon-uitgaven.nl.

Agenda

| Upcoming Events

September 2014

8–12 september 2014

Mathematical Facets of Crystallization

Workshop over de wiskundige theorie van kristallisatie, mede georganiseerd door Frank den Hollander en Markus Heydenreich (UL).

plaats Lorentz Center, Leiden

info lorentzcenter.nl

12 september 2014

Finale Nederlandse Wiskunde Olympiade

Finale van de nationale wiskundeolympiade in Eindhoven.

plaats TU Eindhoven

info wiskundeolympiade.nl

20 september 2014

Ig Nobel Night

Satelliet-evenement van de uitreiking van de Ig Nobelprijs.

plaats Stadsgehoorzaal, Leiden

info ignobelnight.nl

21 september 2014

Waar komen kometen vandaan en waar gaan ze naar toe?

Wakker Worden Kinderlezing door sterrenkundige Henny Lamers over de banen van hemellichamen.

plaats NEMO, Amsterdam

info e-nemo.nl

22–25 september 2014

Statistical Inference for Lévy Processes

Workshop over Lévy-processen, mede georganiseerd door Shota Gugushvili, Aad van der Vaart (UL), Peter Spreij en Harry van Zanten (UvA).

plaats Lorentz Center, Leiden

info lorentzcenter.nl

26 september 2014

Wiskundetoernooi 2014

Jaarlijkse wiskundewedstrijd voor scholieren.

plaats RU, Nijmegen

info ru.nl/wiskundetoernooi

26–27 september 2014

In de ban van het griepvirus

Masterclass voor leerlingen van 5 en 6 vwo.

plaats Utrecht

info betasteunpunt-utrecht.nl

26–27 september 2014

Afscheidsevenement Johan van Benthem

Afscheidscolleges en receptie ter ere van het officiële pensioen van Johan van Benthem, met colleges over diverse onderwerpen in de logica.

plaats UvA, Amsterdam

info <http://illc.uva.nl/J65>

27 september 2014

Discovery Festival

Uitgaansnacht-met-inhoud, waarin wetenschap samengaat met muziek, kunst en inspiratie.

plaats Amsterdam, Rotterdam en Eindhoven

info discoveryfestival.nl

Oktober 2014

4 oktober 2014

CWI Open Dag

Op de open dag van het Amsterdam Science Park opent ook het CWI zijn deuren voor publiek.

plaats CWI, Amsterdam

info cwi.nl

6 oktober 2014

Dag van de leraar

Dag van de leraar met onder andere de verkiezing van de Leraar van het Jaar 2014.

plaats overal

info dagvandeleraar.nl

8–10 oktober 2014

39ste Woudschotenconferentie

39ste editie van de conferentie over Scientific Computing, dit jaar zijn de thema's 'domein decomposities' en 'sterk oscillerend gedrag'.

plaats Woudschoten conferentieoord, Zeist

info wsc.project.cwi.nl/woudschoten/2014/conferentieN.php

Suggesties voor deze agenda zijn welkom.

Redacteur: Patrick Hafkenscheid

agenda@nieuwarchief.nl

9 oktober 2014

Van Dantzig Seminar

Landelijke serie seminars in de statistiek.

plaats VU, Amsterdam**info** few.vu.nl/~bkk320/vandantzig

31 oktober 2014

Wiskundeleraar voor één dag

Masterclass voor leerlingen van 4 en 5 havo met interesse in het onderwijs.

plaats Utrecht**info** betasteunpunt-utrecht.nl

31 oktober 2014

Netwerkbijeenkomst Wiskunde B-dag

Netwerkbijeenkomst ter voorbereiding van de jaarlijkse Wiskunde B-dag.

plaats Utrecht**info** fi.uu.nl/wisbdag**November 2014**

8 november 2014

Jaarvergadering NVvW

Jaarlijkse vergadering van de Nederlandse Vereniging van Wiskundeleraren.

plaats Ichthus College, Veenendaal**info** nvww.nl

14 november 2014

Voorronde A-lympiade

Voorronde van de jaarlijkse wedstrijd waarin Wiskunde A centraal staat, voor leerlingen van 5 havo en 5/6 vwo.

plaats eigen school**info** fisme.science.uu.nl/alympiade

14 november 2014

Wiskunde B-dag

Jaarlijkse wedstrijd waarin Wiskunde B centraal staat, voor leerlingen van 5 havo en 5/6 vwo.

plaats eigen school**info** fi.uu.nl/wisbdag

16 november 2014

Hoe klein kan je zien?

Wakker Worden Kinderlezing van Mark Hink, over de wereld onder de microscoop.

plaats NEMO, Amsterdam**info** e-nemo.nl

21 november 2014

Bartjens rekendictee

Finale van het jaarlijkse rekendictee.

plaats Windesheim, Zwolle**info** bartjensrekendictee.nl

27 november 2014

Van Dantzig Seminar

Landelijke serie seminars in de statistiek.

plaats TU Delft, Delft**info** few.vu.nl/~bkk320/vandantzig**December 2014**

14 december 2014

Waarom wiebelt een wolkenkrabber?

Wakker Worden Kinderlezing van bouwkundige Leo Wagemans over hoe hoge gebouwen buigen maar niet barsten.

plaats NEMO, Amsterdam**info** e-nemo.nl**Januari 2015**

12–16 januari 2015

Mathematical Modelling in Biology: Evaluating Auxin Transport Mechanisms

Workshop mathematische biologie, mede georganiseerd door Bert van Duijn, Sander Hille, Remko Offringa (UL) en Roeland Merks (CWI).

plaats Lorentz Center, Leiden**info** lorenzcenter.nl

26–30 januari 2015

Studiegroep Wiskunde met de Industrie

Jaarlijkse studiegroep waarin wiskunde en industrie samen problemen oplossen.

plaats Universiteit Utrecht**info** projects.science.uu.nl/swi2015

26–28 januari 2015

14th Winter School Mathematical Finance

Winterschool over financiële wiskunde met onder andere een minicursus van Damiano Brigo.

plaats De Werelt, Lunteren**info** staff.science.uva.nl/~spreij/winterschool/winterschool.html

30 januari 2015

Bijles geven in de bètavakken

Masterclass voor leerlingen uit de bovenbouw havo en vwo met interesse in onderwijs.

plaats Utrecht**info** betasteunpunt-utrecht.nl

30–31 januari 2015

Nationale Wiskunde Dagen

21ste editie van de tweedaagse conferentie voor wiskundeleraren.

plaats Noordwijkerhout**info** www.fi.uu.nl/nwd

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 van ± 350 woorden, zo mogelijk met illustratie. De redactie behoudt zich het recht voor berichten te weigeren of in te korten.

Redacteur: Patrick Hafkenscheid
 nieuws@nieuwarchief.nl

Nieuwe hoogleraren KdVI

Professor Jan van Mill (1951) is aangesteld als nieuwe hoogleraar in de topologie aan de Universiteit van Amsterdam. Hij zal gaan werken aan het Korteweg-de Vries Instituut. Van Mill heeft veel onderzoek gedaan in de topologie naar onder andere de topologie van oneindig-dimensionale variëteiten, dimensietheorie en topologische groepen. Van Mill is emeritus hoogleraar aan de Vrije Universiteit in Amsterdam, waar hij al sinds 1974 zit.

Ook Jasper Stokman is aangesteld als nieuwe hoogleraar aan het KdVI. Stokman zal hoogleraar Lie Theory worden, naar het vakgebied van de continue symmetrieën. Stokman is al sinds 2005 werkzaam aan de UvA als universitair docent, ook was hij al eerder bijzonder hoogleraar Integreerbare Systemen en Lie-theorie aan de Radboud Universiteit in Nijmegen.

science.uva.nl

Altruïsme leidt niet altijd tot betere uitkomsten in speltheorie

Nieuw wiskundig onderzoek toont aan dat rekening houden met anderen niet altijd tot de beste uitkomst leidt — tenminste, in de speltheorie. Dit heeft onder meer toepassingen bij data- en verkeersnetwerken, peer-to-peernetwerken en GSP-veilingen, die bijvoorbeeld in Google Adwords worden gebruikt. Bart de Keijzer van het Centrum Wiskunde & Informatica (CWI) in Amsterdam onderzocht voor zijn promotie algoritmes voor speltheorie, met een focus op coöperatieve aspecten. De CWI-wiskundige promoveerde op 16 juni aan de Vrije Universiteit op zijn proefschrift *Externalities and Cooperation in Algorithmic Game Theory*.

Speltheorie is een tak van de wiskunde die zich onder meer met economische processen bezighoudt. Bij het nieuwe onderzoek gaat het niet alleen meer om puur egoïstische spelers, maar ook om beïnvloeding door anderen, waarbij de ene speler de andere niet wil beschadigen met zijn beslissingen. Dit is soms realistischer dan de situatie waarin spelers alleen in zichzelf geïnteresseerd zijn, zoals in klassieke modellen gebruikelijk is.

De Keijzer bestudeerde tijdens zijn promotieonderzoek verschillende soorten veilingen. Hij analyseerde de invloed van samenwerking, vriendschappen en vijandigheid op verschillende spellen. Een van zijn conclusies is dat de doorstroming in een wegen- of datanetwerk slechter kan worden als spelers zich altruïstischer gedragen. “Als altruïsme wordt geïntroduceerd in de modellen, dan kan de uitkomst dus slechter worden. Maar dat wiskunde nu zou bewijzen dat je je eigen koers moet varen, wil ik niet zeggen”, lacht de promovendus. “Maar het is zeker een opvallende uitkomst dat je voor sociale welvaart — een wiskundig begrip — soms beter strategisch kunt kiezen ten koste van anderen, dan te wisselen van strategie om hen te plezieren.” Onderzoekers en beleidsmakers kunnen hun voordeel doen met de realistischer modellen en betere kwalitatieve voorspellingen doen. Andere onderzoeksresultaten van De Keijzer hebben mogelijk toepassingen in inkoopveilingen, treasury-veilingen, radiospectrumveilingen en het toewijzen van woningen.

Annette Kik

Hopkins-promovendus maakt 169-jaar oude methode nuttig

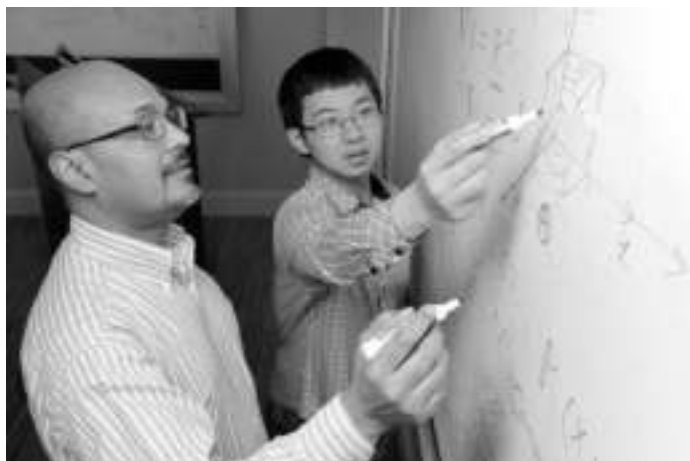
Xiang Yang, promovendus aan de John Hopkins Universiteit, heeft de Jacobi-methode substantieel verbeterd. De Jacobi-methode is een algoritme uit de numerieke wiskunde om een stelsel lineaire vergelijkingen op te lossen dat *diagonaal dominant* is, dit wil zeggen dat de absolute waarde van het diagonale element groter is dan de absolute som

van de andere elementen in de vergelijking. Het algoritme dat onder andere gebruik maakt van de oplossing van het systeem met alleen maar diagonale elementen is origineel bedacht door Carl Gustav Jacob Jacobi, die leefde van 1804–1851. Natuurlijk was de methode in de tijd van Jacobi niet gemaakt voor de supercomputers van tegenwoordig. Het bleek dan ook dat de methode te langzaam was in vergelijking met andere methoden. Hier heeft Yang, samen met professor Rajat Mittal een einde aan gemaakt door het algoritme dusdanig aan te passen dat het 200 keer sneller is.

Schokkend is dat de aanpassing van het algoritme niet meer vereist dan de aanpassing van 5–6 regels code. Yang en Mittal hadden elkaar ontmoet in het college Numerical Mathematics in 2012. Mittal doceerde over het wiskundig elegante maar desalniettemin nutteloze algoritme.

De nieuwe methode maakt het mogelijk om veel problemen numeriek makkelijker op te lossen. Een voorbeeld is vloeistofmechanica. Hierin komen veel elliptische vergelijkingen voor, die wanneer gediscretiseerd diagonaal dominante lineaire problemen kunnen oplossen.

jhu.edu



Will Kirk, homeworkphoto.jhu.edu

Gödel's stelling als muziekstuk

In voorbereiding op de jaarlijkse *Gödelprijs*, een prestigieuze prijs in de theoretische informatica, heeft de Deense componist Niels Marthinsen een muziekstuk geschreven waarin de logische axioma's die Gödel gebruikte gecodeerd zijn. Het stuk heet 'The Hilbert Heartbreak Hotel', naar het beroemde theoretische hotel met oneindig veel bezette kamers. Het idee voor het stuk kwam van Thore Husfeldt, een informaticus aan de Lund University in Zweden. Hij verklaart dat een van de redenen dat hij een informaticus is geworden het boek *Gödel, Escher, Bach* is.

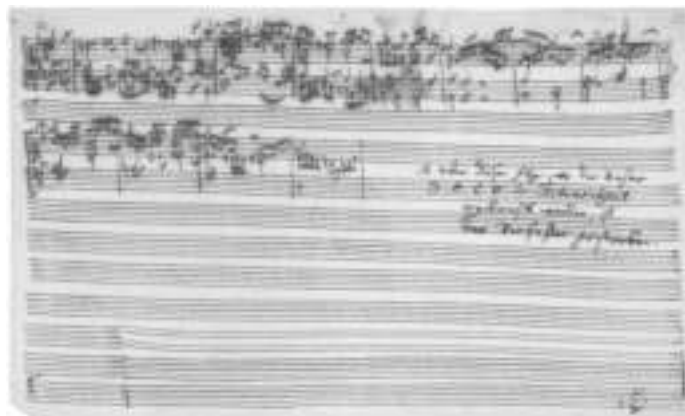
Marthinsen is niet geheel onbekend in het combineren van wiskunde en muziek. Zijn leermeester was Per Nørgård, die in de jaren zestig veel experimenteerde met het idee van fractals in muziek. Het principe van *oneindige reeksen* speelt hierin ook een rol.

De axioma's waar muziek van gemaakt is, zijn de axioma's van de rekenkunde, geformuleerd door Giuseppe Peano. Gödel heeft in 1931 bewezen dat de rekenkunde zichzelf niet kan bewijzen (de zogeheten *onvolledigheidsstelling*). Om de axioma's in muziek om te toveren heeft Marthinsen aan ieder logisch symbool een muzikale korte zin toegekend. Bovenop de muziek die gegenereerd wordt door deze codering heeft Marthinsen een liedtekst geschreven over Hilberts hotel, hoe een harteloze persoon het hotel binnenstapt en de gast in de eer-

ste kamer gevraagd wordt zijn hart te geven aan de nieuwe gast, en hoe vervolgens de harten worden doorgegeven van kamer naar kamer tot iedereen een hart heeft.

Er is nog geen opname van het nummer, deze zal voor het eerst bij de uitreiking van de Gödelprijs te horen zijn.

Nature



De onvolledige fuga van Bach

Opening van het KorolevLab

Op 12 juni is het KorolevLab voor de ruimtevaart geopend in de faculteit Elektrotechniek, Wiskunde en Informatica van de TU Delft. Het Lab, een samenwerking tussen TU Delft Robotics Institute en Delft Aerospace Rocket Engineering (DARE), is een plek waar studenten van de raketbouwvereniging en medewerkers van het Robotics Institute kunnen ontwerpen, simuleren en werken aan het uiteindelijke doel: de ruimte bereiken met een raket. De naam komt van de Russische raketpionier Sergei Korolev.

DARE is opgericht in 2001. Het is een vereniging voor raketbouw helemaal opgezet door studenten van de TU Delft. De leden leren zelf raketten bouwen, testen en lanceren. Sinds de oprichting zijn er al meer dan honderd lanceringen gedaan. Het record van de hoogte die de raketten hebben bereikt, staat op dit moment op 12,5 km. De raket, genaamd Stratos I, heeft hiermee een Europees hoogterecord voor amateur-raketbouw gevestigd.

Nu willen de studenten van DARE als eerste team de ruimte bereiken. Dit is nog een grote klus want de ruimte begint op ongeveer acht keer de hoogte van het record (100 km hoogte). De studenten zijn momenteel bezig met het klaarmaken voor de lancering van de Stratos II. Deze zal worden gelanceerd in september vanaf een lanceerterrein in Zuid-Spanje. Het doel voor de te behalen hoogte van de raket is 50 km, dus als het lukt zijn de studenten al op de helft.

tudelft.nl

Bewegende knopen in ons DNA

Natuurkundigen van de Johannes Gutenberg Universiteit Mainz (JGU) en de Graduate School of Excellence "Material Science in Mainz" hebben met behulp van computersimulaties een opmerkelijk mechanisme aangetoond.

Het mechanisme werkt op knopen in ons DNA, het was al eerder verondersteld dat twee knopen van plek konden verwisselen in een enkele streng DNA, tot dusver was niet zeker hoe dit gebeurde. Met behulp van de simulaties hebben de wetenschappers laten zien dat één van de knopen genoeg groeit zodat de andere knoop langs de contour naar de andere kant kan bewegen. De wetenschappers denken dat het

onderzoek uiteindelijk zou kunnen worden gebruikt in technologieën zoals die van de nanoporie-ketens waar lange ketens DNA door poriën worden getrokken.

uni-mainz.de

Sander Dekker: geen nieuwe verplichte rekentoetsen

Tijdens de vergadering van de Kamercommissie Onderwijs, Cultuur en Wetenschap op 18 juni 2014 heeft staatssecretaris Sander Dekker laten weten dat hij gehoor heeft gegeven aan de vele kritiek op de rekentoetsen. De twee hoofdrolspelers van het verhaal zijn de begintoetsen rekenen in groep 3 en de rekentoets op ongeveer de helft van de middelbare school. Sander Dekker heeft laten weten dat hij de verplichte begintoets niet zal invoeren, en dat hij ook de verplichte diagnostische tussentoets niet laat doorgaan.

Het commentaar op de toets kwam voornamelijk voort uit de kwaliteit van de toetsen, zo waren ze *moeilijk, te lang, te talig* en sommige vragen waren erg vaag. Iedereen was het er echter wel mee eens dat de leerlingen niet de dupe mogen worden. Instellingen kunnen nu officieel dus nog niet gebruik maken van de resultaten van de rekentoets om voorselecties te doen. Enkele mbo's hebben hier echter niet naar geluisterd en hebben desalniettemin hier op geselecteerd. Minister Bussemaker zegde toe hierover te praten met de mbo's.

Ongeduldige internetgebruikers

Ongeduldige internetgebruikers zijn een groot probleem voor de kwaliteit van het web. Er gaat veel data verloren omdat mensen voortijdig downloads stoppen. De meeste modellen voor internetgebruik houden met dit verlies van data geen rekening. Dit kan een probleem vormen als er een hoop mensen op hetzelfde netwerk zitten en de verbinding daardoor erg langzaam is, waardoor mensen voortijdig afhaken.

CWI-onderzoekers hebben dit fenomeen nu in model gebracht. Dankzij dit model kunnen internetproviders beter inspelen op voortijdig afbreken van transfers. Onderzoeker Maria Remerova heeft op 20 mei 2014 haar proefschrift verdedigd over dit onderwerp met de titel *Fluid Limit Approximations of Stochastic Networks*.

Het probleem is in sommige opzichten vergelijkbaar met callcenters waar bellers soms ook voortijdig afhaken. Het verschil zit hem erin dat er bij de ongeduldige internetgebruiker al data verspild is en bij het callcenter nog niets.

Remerova heeft nu methoden ontwikkeld die het mogelijk maken om de prestaties en problemen bloot te leggen in een systeem waarin ongeduldigheid van de gebruikers wordt meegenomen.

cwi.nl

Hoogleraarsbenoemingen Freudenthal Instituut

Bij het Freudenthal Instituut van de Universiteit Utrecht zijn drie nieuwe hoogleraren benoemd. Per 1 april 2014 is Toine Pieters hoogleraar en algemeen directeur van het instituut. Wouter van Joolingen is op 1 mei aangetreden als hoogleraar en wetenschappelijk directeur. Met ingang van 1 juni is Paul Drijvers in deeltijd benoemd tot hoogleraar in de didactiek van de wiskunde. Daarnaast blijft Drijvers werkzaam voor Cito.

fisme.uu.nl

Prehistorische wiskunde

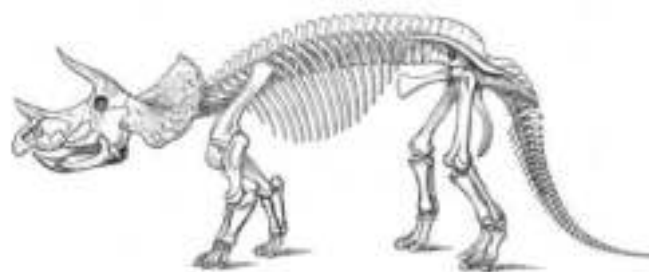
Hoewel op het eerste gezicht een rare combinatie, is wiskunde doorslaggevend geweest in het analyseren van de botten van een dinosau-

rus. De wiskundige biologie-groep van professor Robert Sinclair aan de Okinawa Institute of Science and Technology heeft dit in een artikel in *Alcheringa: An Australasian Journal of Palaeontology* gepubliceerd.

Het begon allemaal met een gevonden dinosaurusbot. Dit bot was een deel van een arm gevonden in Zuid-Australië. Het was oorspronkelijk geïdentificeerd als het bot van een dinosaurus die behoort tot de *Neoceratopsia*-familie (dit is dezelfde familie als de Triceratops). Kort nadat het artikel waarin dit wordt uiteengezet verscheen, kwam er een reactie van een andere onderzoeksgroep die de resultaten weerlegde, omdat tot dan toe werd aangenomen dat er nooit zulke dinosaurussen leefden op het zuidelijke halfrond.

De doorslag kwam uiteindelijk van Sinclair die met de wiskunde liet zien dat het bot inderdaad tot de *Ceratopsia* behoorde. Hij deed dit overtuigend genoeg om het bot tot de familie toe te laten kennen.

oist.jp



Een triceratops

Michelle Sweering beste wiskundemeisje van de wereld

De Nederlandse Michelle Sweering is op de Internationale Wiskunde Olympiade in Zuid-Afrika als beste meisje van de wereld geëindigd. Ze haalde als enige meisje een gouden medaille. Ook Jeroen Winkel (17) en Peter Gerlagh (18) legden beslag op een gouden medaille, iets wat tot nu toe voor slechts vier Nederlanders weggelegd was. De andere drie teamleden haalden zilver (2x) en brons. Hiermee werd Nederland dertiende in het landenklassement en versloeg het alle andere West-Europese landen. Nooit eerder haalde Nederland zo'n goed resultaat.

De Internationale Wiskunde Olympiade vond van 6 tot 13 juli plaats in Kaapstad, Zuid-Afrika. Op elk van de twee wedstrijddagen kregen de leerlingen drie opgaven van hoog wiskundig niveau voor hun kiezen, waar ze vier en een half uur aan konden werken. Voor elke opgave waren zeven punten te behalen. Michelle Sweering was één van de slechts vijftien deelnemers die de allermoeilijkste opgave wisten op te lossen.

Van de 560 deelnemers ontvingen er in totaal 133 deelnemers een bronzen medaille, 113 een zilveren medaille en 49 een gouden medaille. Het officiële landenklassement werd aangevoerd door China, de Verenigde Staten en Taiwan. Met Japan (vijfde) erbij zijn dit de enige landen die meer gouden medailles wisten te bemachtigen dan Nederland.

Merlijn Staps

Ruimteschoenen de ruimte in gestuurd

NASA heeft de ForceShoe de ruimte in gestuurd, de schoenen zijn momenteel op het International Space Station (ISS). De schoenen, ontworpen door Xsens en Universiteit Twente worden gebruikt om te helpen

bij de training van astronauten. Astronauten blijven vaak een langere tijd in de ruimte, het is dan belangrijk om de spieren te blijven trainen zodat er een gezonde spier- en botmassa behouden blijft. De schoen kan hier een grote rol in spelen door een-op-een hele accurate manier krachten te meten.

De NASA maakt al gebruik van veel andere Xsens-producten, veelal om het onderzoek in de ruimte makkelijker te maken. Voordat de schoenen de ruimte in werden gestuurd, moesten ze uitgebreid getest worden door de NASA. Toen dit achter de rug was konden de schoenen worden gelanceerd met de Russische Sojoez op 28 mei 2014.



Foto: NASA

Twee winnaars Stieltjesprijs voor beste proefschrift

Op voordracht van de selectiecommissie heeft WONDER besloten om bij hoge uitzondering, gezien de uitzonderlijke kwaliteit dit jaar, twee Stieltjesprijzen uit te reiken voor beste wiskundeproefschrift 2013.

Benjamin Sanderse van de TU Eindhoven won de prijs voor zijn proefschrift *Energy-conserving discretization methods for the incompressible Navier–Stokes equations*, waarop hij op 19 maart 2013 cum laude gepromoveerd is aan de TU/e bij prof.dr.ir. Barry Koren.

Pavel Zorin-Kranich won de prijs voor zijn proefschrift *Ergodic theorems for polynomials in nilpotent groups*, waarop hij op 12 september 2013 gepromoveerd is aan de UvA bij prof.dr. Ale Jan Homburg en copromotor dr. Tanja Eisner.

De Stieltjesprijs wordt sinds 1996 jaarlijks toegekend aan het beste proefschrift in de wiskunde. Voor 2013 werden 74 proefschriften ingestuurd. De prijs bedraagt 2500 euro, beschikbaar gesteld door Stichting Compositio Mathematica. De 2500 euro voor de extra prijs is beschikbaar gesteld door de Thomas Stieltjes Stichting.

WONDER

Wiskundig model voorspelt na-aapgedrag

Onderzoekers van Oxford, Harvard Institute for Public Health en de universiteit van Limerick hebben een wiskundig model geconstrueerd voor ons online-gedrag. Specifiek de samenhang tussen wat onze vrienden doen en wat iedereen buiten onze sociale kring doet.

De onderzoekers deden het onderzoek met behulp van Facebook-apps. Ze keken naar de data van Facebook over de apps die geïnstalleerd werden en vergeleken dit met de apps die vrienden installeerden en met de apps van de *bestsellerlijsten*.

Na simulaties van enorme proporties (met behulp van de supercomputers van het Irish Centre for High-End Computing), bleek dat tussen de twee factoren de recente activiteit van vrienden een veel

grotere invloed had op het gedrag dan de bestsellerlijst. Op de vraag of dit online-gedrag ook vertaald kan worden naar waarnemingen in de offline-wereld is nog geen antwoord. Wel is het waar dat het na-aapgedrag vaker voorkomt onder de mensen, zowel online als offline.

Oxford Universiteit



Foto: Fruggo

Eerste Breakthrough Prize in de wiskunde uitgereikt

Een nieuwe prijs in de wiskunde is dit jaar in het leven geroepen. De *Breakthrough Prize in Mathematics* is speciaal voor wiskundigen die een grote bijdrage leveren aan de fundamenteën van de wetenschap. De prijs bestaat uit drie miljoen dollar en wordt gefinancierd door onder anderen Mark Zuckerberg en Yuri Milner. De uitreikingen worden op televisie uitgezonden in de hoop jonge wetenschappers te inspireren.

Winnaars van de Breakthrough Prize van dit jaar zijn Simon Donaldson (algebraïsche meetkunde), Maxim Kontsevich (voor zijn betekenis in diverse gebieden), Jacob Lurie (categorie theorie en algebraïsche meetkunde), Terence Tao (vele doorbraken in onder andere harmonische analyse, combinatoriek en getaltheorie) en Richard Taylor (theorie van automorfe vormen en lineaire groepen).

De nominaties voor 2015 staan nu open en kunnen ingediend worden op www.breakthroughprize.org.

euro-math-soc.eu

Fieldsmedaille voor Maryam Mirzakhani

Op 13 augustus zijn tijdens het ICM 2014 in Seoul de Fieldsmedailles uitgereikt. De Fieldsmedailles worden eens in de vier jaar toegekend aan twee tot vier wiskundigen die jonger dan veertig jaar zijn. De Iraanse Maryam Mirzakhani (Stanford University) kreeg dit jaar als eerste vrouw ooit de prijs toebedeeld. Zij kreeg de prijs voor haar bijdragen in onder andere topologie, Riemann-oppervlakken en dynamica. Verder werd de prijs toegekend aan Artur Avila (CNRS, Parijs, en IMPA, Rio de Janeiro), Manjul Bhargava (Princeton University en Universiteit Leiden) en Martin Hairer (University of Warwick). Avila is de eerste Braziliaan die de Fieldsmedaille heeft mogen ontvangen. Hij doet onderzoek naar de relaties tussen dynamische systemen en spectraaltheorie. Bhargava onderzoekt de geometrie van getallen, die hij toepast om bijvoorbeeld ringstructuren van kleine rang te tellen. De Oostenrijker Hairer houdt zich bezig met diverse onderwerpen in de kansrekening.

mathunion.org/general/prizes/2014

Wim Caspers

Adelbert College, Wassenaar

Faculteit EWI en Lerarenopleiding, TU Delft

w.t.m.caspers@tudelft.nl

Onderwijs

Bespreking examen vwo wiskunde B 2014

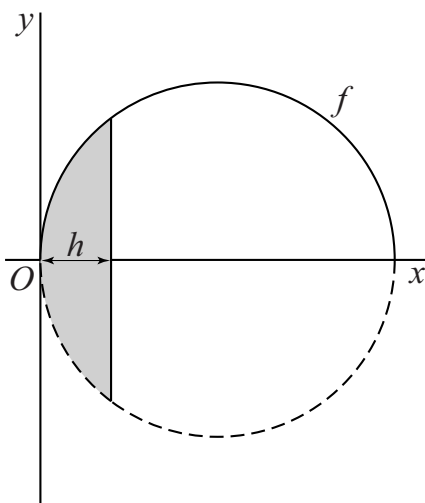
De eindexamens zijn weer achter de rug. Vele scholieren zijn inmiddels, met een diploma op zak, aan een vervolgopleiding begonnen. Daar zal men ervaren of hetgeen men geleerd heeft op de middelbare school goed aansluit bij de studie die men gekozen heeft. Met die vraag in gedachte bekijkt Wim Caspers, docent wiskunde aan het Adelbert College te Wassenaar, het examen vwo wiskunde B van 20 mei 2014. Caspers is tevens werkzaam aan de TU Delft bij de faculteit EWI en de lerarenopleiding. Daarnaast is hij lid van de onderwijscommissie van Platform Wiskunde Nederland.

In mei worden de scores die leerlingen behaald hebben voor het Centraal Examen door de examinatoren digitaal verstuurd naar bevoegde instanties. Bij dat versturen verschijnt bij wijze van enquête de vraag in beeld of het examen aansloot bij het gegeven onderwijs. Dat is een gewetensvraag, want wordt het antwoord gebruikt om het examen te kwalificeren of probeert men het gegeven onderwijs langs de meetlat te leggen? Met bevoegde instanties weet je het maar nooit. Gelukkig is er ook een knop waarmee je de enquête kunt overslaan.

Alsnog blijft de vraag: toetst het examen wat er in de wiskundeles zoal geleerd wordt op het vwo of niet? In het vervolgonderwijs bestaat al jaren het beeld dat het cijfer voor wiskunde B heel aardig het studiesucces in het eerste jaar voorspelt, maar is aan de examenopgaven af te lezen wat afnemende onderwijsinstellingen van hun eerstejaarsstudenten mogen verwachten op het gebied van de wiskunde? Met die vraag voor ogen bekijken we het examen vwo wiskunde B 2014.

Bal onder water

Het examen begint met een sympathieke opgave over een bal die zich h cm onder het wateroppervlak bevindt. Als service wordt de



Figuur 1

figuur met de doorsnede van de situatie een kwartslag gedraaid. Om het rekenwerk te vereenvoudigen, staat erbij. Eerlijk gezegd wordt het rekenwerk pas beperkt door het handig kiezen van een assenstelsel (zie Figuur 1). Draaien om de x -as is voor leerlingen iets makkelijker dan draaien om de y -as inderdaad. Het handig kiezen van een assenstelsel evenals het functievoorschrift dat de doorsnede beschrijft, is een stukje wiskunde dat wordt weggegeven, en dat is helemaal niet erg bij een openingsopgave. Waarschijnlijk zijn er wel leerlingen geweest die zich afvroegen of het werkelijk zo eenvoudig was.

Buigpunten

De tweede opgave gaat over grafieken met buigpunten (zie Figuur 2). Voor elke waarde van p met $p \neq 0$ is een functie f_p gegeven waarbij voor de tweede afgeleide geldt:

$$f_p''(x) = 12(x - p)(x + p).$$

Met primitiveren moet worden aangetoond dat er geldt:

$$f_p(x) = x^4 - 6p^2x^2 + ax + b,$$

met a en b constanten. Dat verklaart de 12 in die dubbele afgeleide waar de opstellers van het examen voor gekozen hebben. Voor de rest van de opgave wordt ervoor gekozen

Boven en onder de lijn door de buigpunten

Voor elke waarde van p met $p \neq 0$ is een functie f_p gegeven waarbij voor de tweede afgeleide geldt: $f_p''(x) = 12(x-p)(x+p)$

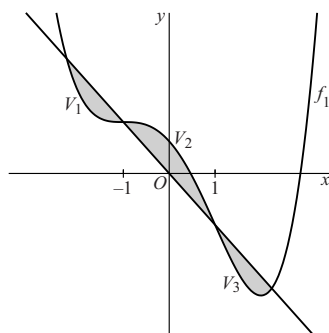
Er geldt: $f_p(x) = x^4 - 6p^2x^2 + ax + b$ met a en b constanten.

4p 3 Toon dit aan met primitiveren.

Voor $a = -8$ en $b = 5$ wordt f_1 gegeven door $f_1(x) = x^4 - 6x^2 - 8x + 5$.

In de figuur zie je de grafiek van f_1 . Deze grafiek heeft buigpunten voor $x = -1$ en $x = 1$. De lijn door deze buigpunten heeft vergelijking $y = -8x$. Deze lijn en de grafiek van f_1 begrenzen drie vlakdelen V_1 , V_2 en V_3 die om en om onder en boven de lijn liggen.

figuur



De lijn met vergelijking $y = -8x$ snijdt de grafiek van f_1 niet alleen in de twee buigpunten, maar ook in twee andere punten.

4p 4 Bereken exact de x -coördinaten van de twee andere snijpunten.

De vlakdelen V_1 en V_3 hebben gelijke oppervlakte, namelijk $3\frac{1}{5}$.

4p 5 Bewijs dat de gezamenlijke oppervlakte van V_1 en V_3 gelijk is aan de oppervlakte van V_2 .

Figuur 2

om alleen nog maar de functie f_1 te bekijken en dan ook nog met $a = -8$ en $b = 5$. Bovendien wordt er verkapt dat de grafiek buigpunten heeft voor $x = 1$ en $x = -1$ en dat de lijn door die buigpunten vergelijking $y = -8x$ heeft, en wordt de grafiek gegeven. De vragen die gesteld worden gaan over andere snijpunten van de lijn en de grafiek en over oppervlakten die worden ingesloten door lijn en grafiek. Doorsnee rekenwerk voor veel leerlingen. In een alledaagse wiskundeles mag je verwachten dat er meer van de leerlingen gevraagd wordt, bijvoorbeeld om te onderzoeken waarom alleen dat speciale geval gekozen is. Is hier sprake van een algemenere opgave op de achtergrond, vereenvoudigd om in het examen op te durven nemen? Het zou zomaar kunnen. In de les zouden de leerlingen aan de algemenere versie worden blootgesteld. Er zou dan uitgezocht worden

dat de grafiek van f_p buigpunten heeft voor $x = p$ en $x = -p$, dat de lijn door de buigpunten richtingscoëfficiënt a heeft en dat als $b = 5p^4$ gekozen wordt, dat dan die lijn vergelijking $y = ax$ heeft. De vragen die gesteld werden over andere snijpunten en oppervlakten kunnen ook in het algemene geval beantwoord worden. Op die manier wordt er meer wiskunde gedaan in de les dan op het examen gevraagd is.

Kogelstoter

Iets dergelijks geldt voor de opgave over de ideale stoothoek α van een kogelstoter (zie Figuur 3). Er wordt een keurige context geschetst van een kogelstoter die een kogel altijd met dezelfde snelheid wegstoot. Wat die snelheid is, dat blijft geheim. De afmetingen van de kogel worden verwaarloosd (over die van de kogelstoter wordt niet gerept) en voor

het geval $\cos(\alpha) = 0,6$ wordt een parametervoorstelling van de vlucht gegeven. Het blijkt een parabool te zijn:

$$\begin{cases} x(t) = 8,4t, \\ y(t) = h + 11,2t - 4,9t^2, \end{cases}$$

met afstanden in meters en tijd in seconden. Dat zelf bedenken, wordt niet van de leerling gevraagd, waarschijnlijk om leerlingen zonder natuurkunde in hun pakket niet te benadelen. Ze hoeven aanvankelijk alleen de overbrugde afstand uit te rekenen voor het geval dat $h = 1,96$. Daardoor blijft de mededeling $\cos(\alpha) = 0,6$ geheimzinnig als nutteloos gegeven in de opgave zweven. In de wiskundeles zou wel aan de orde komen dat die 0,6 uit een 3-4-5-driehoek afkomstig is, als u begrijpt wat ik bedoel, en dat de snelheid blijkbaar 14 m/s is geweest. De parametervoorstelling is dan afhankelijk van hoek α :

$$\begin{cases} x(t) = 14 \cos(\alpha)t, \\ y(t) = h + 14 \sin(\alpha)t - 4,9t^2, \end{cases}$$

met $0 \leq \alpha \leq \frac{1}{2}\pi$. De examenopgave vervolgt dan met te melden hoe de horizontale afstand r die de kogel overbrugt, afhangt van α . Voor een examen voert het te ver, dat valt te begrijpen, maar in een les kan leerlingen prima gevraagd worden de formule af te leiden. Immers, in geval van ontsporing kunnen ze met een klein beetje hulp weer op weg geholpen worden. Er zou dan blijken dat het getal 14 zo handig gekozen is, omdat 14 in het kwadraat gelijk is aan 20 keer de valversnelling (afgerond op 9,8).

In de les zou het in zijn volle omvang een goede opgave zijn, maar in het examen is hij behoorlijk beperkt tot redelijk standaard rekenwerk, af en toe met rekenmachine. (De opgave kan nog algemener bekeken worden door op de plaats van 14 telkens v te schrijven, maar met 14 is het wel zo duidelijk welke rol de snelheid speelt.)

Even lang

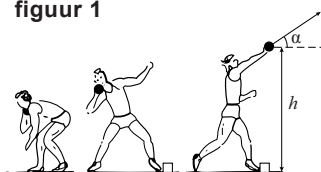
Een opgave die een stuk lastiger voor leerlingen bleek, is de opgave 'Even lang', waarbij uitgaande van gelijkzijdige driehoeken in stappen wordt toegewerkt naar de lengte van lijnstuk EH (zie Figuur 4). Bij deze opgave werd niet de service verleend om de figuur bijvoorbeeld 120 graden of 30 graden te draaien en een handig assenstelsel aan te brengen met A of D als oorsprong. Pas in 2018 doet de

De ideale stoothoek

Een kogelstoter stoot een kogel weg onder een hoek α (in radialen, $0 < \alpha < \frac{1}{2}\pi$).

De hoogte in meters waarop de kogelstoter de kogel loslaat is h . Zie figuur 1.

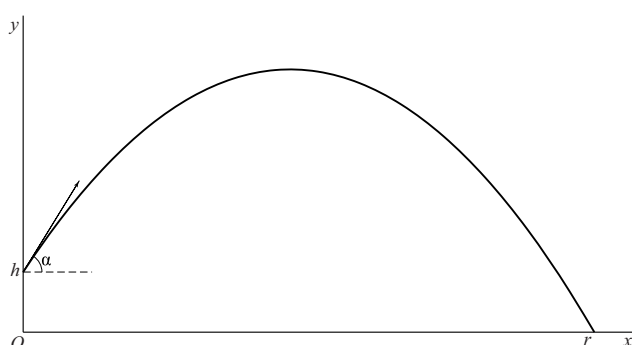
figuur 1



Bij deze situatie kiezen we een assenstelsel waarbij de plaats waar de kogel wordt losgelaten zich op hoogte h op de verticale as bevindt. De kogel komt op afstand r in meters van de oorsprong op de grond. Zie figuur 2.

In deze opgave gaan we ervan uit dat de kogelstoter de kogel altijd met dezelfde snelheid wegstoot.

figuur 2



Als α zo is dat $\cos \alpha = 0,6$ en we de afmetingen van de kogel en de wrijving met de lucht verwaarlozen, dan gelden (bij benadering) de volgende formules voor de coördinaten van de kogel tijdens de vlucht:

$$\begin{cases} x(t) = 8,4t \\ y(t) = h + 11,2t - 4,9t^2 \end{cases}$$

Hierin is t de tijd in seconden met $t = 0$ op het moment van loslaten, x de horizontale afstand in meters en y de hoogte in meters.

De kogelstoter laat de kogel los op een hoogte van 1,96 m.

- 4p 7 Bereken op hoeveel meter afstand van de kogelstoter de kogel op de grond komt. Rond je antwoord af op een geheel aantal decimeters.

De horizontale afstand r die de kogel overbrugt, hangt af van de hoek α waaronder deze wordt weggestoten.

In het algemeen geldt voor elke waarde van α de volgende formule voor r :

$$r = 20 \cos \alpha \left(\sin \alpha + \sqrt{\sin^2 \alpha + 0,1h} \right)$$

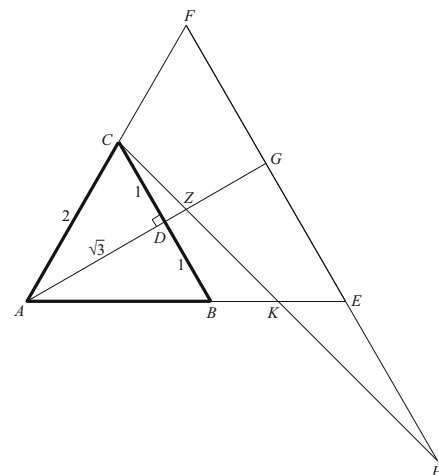
De ideale stoothoek is de hoek α waarbij r zo groot mogelijk is.

We bekijken nu de situatie waarbij de kogelstoter de kogel loslaat op een hoogte van 1,85 m.

- 3p 8 Bereken voor deze situatie de ideale stoothoek.

Tot slot bekijken we de denkbeeldige situatie waarin $h = 0$.

- 6p 9 Bereken exact de ideale stoothoek voor deze denkbeeldige situatie.



Figuur 4

eerste lichting examen met analytische meetkunde in het programma wiskunde B en zal het rekenen in een assenstelsel bij deze opgave voor de hand liggen. Nu wordt er gewerkt met een hoop gelijkvormigheid, waarbij de plek van Z op twee derde van AG een belangrijke rol speelt.

Goniometrie was al aan de orde gekomen bij het bepalen van de ideale stoothoek. In een volgende opgave wordt voor $a \neq 0$ de functie f_a opgevoerd met

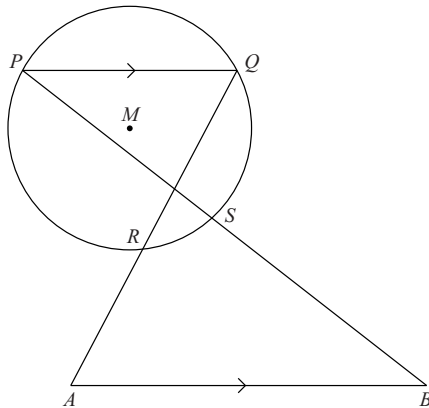
$$f_a = 2 \sin(ax) + \sin(2ax).$$

Er volgt een vraag over de x -as als raaklijn en een vraag over puntsymmetrie van de grafiek van f_2 in het punt $(\frac{1}{2}\pi, 0)$. Nu wordt een beroep gedaan op kennis van de afgeleide van sinus en cosinus en allerlei goniometrische gelijkheden. Een aantal van die gelijkheden worden bij het examen gegeven (formules voor $\sin(t+u)$ en $\sin(t)-\sin(u)$ en hun varianten met plus en min en de cosinus). Andere formules over bijvoorbeeld het verband tussen cosinus en sinus kan een leerling opgeslagen hebben in de grafische rekenmachine. Een aantal leerlingen zal gebruikmaken van de regeltjes als ware het toverspreuken, maar vaak zie je toch ook grafiekjes of eenheidscirkeltjes getekend in de kantlijn die op iets meer begrip van de materie lijken te wijzen. De opgave kan dus met meer of minder inzicht gemaakt worden.

Koordenvierhoek

De laatste opgave, 'Koordenvierhoek', is er eentje in de traditie van de vlakke examenmeetkunde (zie Figuur 5). We zien parallelle lijnstukken (een ervaren leerling denkt onmiddellijk aan Z -hoeken), een cirkel (diezelfde ervaren leerling denkt aan de stelling van

Figuur 3



Figuur 5

de constante hoek) en gevraagd wordt te bewijzen dat een vierhoek een koordenvierhoek is (wat volgens de leerling neerkomt op het bewijzen dat de overstaande hoeken opgeteld 180 graden opleveren). En inderdaad levert die wijsheid, gecombineerd met een buitenhoek van een driehoek of een gestrekte hoek, onvermijdelijk het gevraagde bewijs. De examenmeetkunde is op deze manier een flauw spelletje geworden. Zoek relevante stellingen bij elkaar — een lijst waaruit gekozen kan worden, wordt bij het examen gegeven — en zet ze in een volgorde die een bewijs ople-

vert. In het nieuwe examenprogramma zit zoals gezegd veel meer analytische meetkunde, ten koste van deze vlakke meetkunde. Goed idee wat mij betreft. De vlakke examenmeetkunde dreigt inmiddels in het onderwijs (en het bijlesonderwijs) tot een te trainen bezigheid te verworden.

Conclusie

Niet alle opgaven uit het examen zijn hierboven aan de orde gekomen, maar het examen overziend zou je het vermoeden kunnen krijgen dat voor veel onderwerpen geldt: de wiskunde teruggebracht tot stappenplannen. Als er 'dit' staat moet je 'dat' doen en 'zus' moet je 'zo' aanpakken. Ik ben ervan overtuigd dat er in de aanloop naar het examen veel op die manier onderwezen wordt. Dat wordt ook niet ontmoedigd door het correctievoorschrift, waarin de te doorlopen stappen nauwkeurig beschreven zijn en dat in toenemende mate van detail besproken en geïnterpreteerd wordt, bijvoorbeeld op de website van de NVvW. Het doet geen recht aan verschillen tussen docenten, maar ook niet aan verschillen tussen leerlingen. De een volgt in zijn uitwerking keurig de aangeleerde stapjes, de ander zet wat grotere stappen in

zijn denken en weer een ander bedenkt ter plekke een eigen, soms wat onbeholpen opgeschreven methode. Allemaal doen ze wiskunde, maar het examen en (het gebruik van) het correctievoorschrift zijn vooral gericht op de keurig aangeleerde stapjes.

Ik ben er ook van overtuigd dat er in de jaren voor de laatste sprint naar het examen, veel meer recht gedaan wordt aan de andere aspecten van de wiskunde: onderzoeken, ontdekken, modelleren, vastlopen, opnieuw beginnen, probleemoplossen. De opgaven uit het examen over buigpunten en kogelstoter lenen zich daarvoor als ze niet zo teruggebracht waren tot rekenwerk. Nu is aan de opgaven niet direct af te lezen wat leerlingen allemaal nog meer kunnen. De beste manier om werkelijk op de hoogte te raken van wat er verwacht mag worden van eerstejaarsstudenten blijft toch om het ze gewoon eens zelf te vragen. En voor zo'n gesprek is het examen, dat ze immers allemaal gemaakt hebben, een mooi uitgangspunt. Dat dan weer wel. ←

De afgedrukte opgaven en losse figuren zijn afkomstig uit het eindexamen vwo wiskunde B, eerste tijdvak, 20 mei 2014, en zijn gebruikt met toestemming van het College voor Examens.

“Bewijs” versus “Toon aan”

Er is verschil tussen de opdracht “Bewijs” en “Toon aan”. Dat zit zo. (Voor alle regelgeving, examenprogramma's, examenopgaven, correctievoorschriften enzovoorts, zie www.examenblad.nl.) Tijdens het examen mag de kandidaat gebruikmaken van een grafische rekenmachine; een aantal types is toegestaan. In het geheugen van die machine mag de kandidaat van alles zetten, behalve dan de app ZoomMath. Daarmee kan de rekenmachine opeens allerlei computeralgebra-achtige dingen uitvoeren en dat is niet de bedoeling. Controle tijdens het examen van alle rekenmachines is nogal een gedoe, vooral ook omdat de app gecamoufleerd kan worden.

Wordt er in de opgave om een exacte of algebraïsche uitwerking gevraagd, dan wordt er een uitwerking verwacht waarin de grafische rekenmachine geen rol speelt. (De rekenmachine kan je natuurlijk nog steeds wel op weg helpen om zo'n exacte uitwerking te vinden.) Nieuw dit jaar is het onderscheid tussen de opdrachten “Bewijs” en “Toon aan”. Als er gevraagd wordt om iets te bewijzen, dan mag de grafische rekenmachine geen rol spelen in de uitwerking. Wordt er gevraagd om iets aan te tonen, dan mag dat wel. Zo wordt

er gevraagd in opdracht 5 om iets te bewijzen over de oppervlakte van vlakdelen begrensd door een lijn en de grafiek van een functie. Het gebruik van integralen ligt voor de hand, en de berekening ervan dient zonder sporen van de grafische rekenmachine opgeschreven te worden. Anders was er wel gevraagd om het aan te tonen.

Zelfs nu dit ragfijne onderscheid is gemaakt, geeft het examen niet een volledig beeld van het gebruik van de grafische rekenmachine door aankomende studenten. Sommige opgaven waarbij toepassing van de rekenmachine is toegestaan worden door een groot deel van de leerlingen exact opgelost. Dat het niet hoeft, wil dus niet zeggen dat ze het ook niet kunnen. Ontegengesteld zijn ze wel gewend om de rekenmachine altijd ter beschikking te hebben. Ze zijn er ook erg handig mee. Daar hebben ze helaas weinig aan wanneer ze tijdens hun studie te maken krijgen met Maple of Mathematica of iets dergelijks.

Dat de grafische rekenmachine zijn langste tijd heeft gehad is een veilige voorspelling. Of en waardoor de rol wordt overgenomen is lastiger te voorspellen.

Ross Kang

IMAPP

Radboud Universiteit Nijmegen

ross.kang@gmail.com

The Solution

The latest designs

One of the oldest problems in combinatorics — dating back to mid-nineteenth century work of, independently, Plücker, Kirkman and Steiner — asserts the existence of what are referred to as ‘Steiner systems’ (subject essentially to only some simple divisibility conditions). These highly symmetric structures are foundational to the field of combinatorial design theory. Until this year, this existence conjecture has remained largely open. In January 2014, Peter Keevash announced a proof of the conjecture, which also confirms a more general conjecture for designs. In this article Ross Kang describes the conjecture and the solution of Keevash.

The Reverend Thomas P. Kirkman, a Church of England clergyman, in 1850 posed the following innocent puzzle in *The Lady’s and Gentleman’s Diary*, a recreational mathematics magazine of the time:

“Fifteen young ladies in a school walk out three abreast for seven days in succession: it is required to arrange them daily so that no two shall walk twice abreast.”

This became known as *Kirkman’s schoolgirl problem*. Its popularity partly led to the systematic study of discrete structures called Steiner systems.

These structures and their relatives (defined precisely below) are foundational to the field of combinatorial design theory. They are collections of finite sets that have specified regularity and incidence properties. Although their properties can be quite useful, they impose particular algebraic, arithmetic or geometric restrictions. Indeed, a very difficult challenge is to prove the existence of such systems, let alone construct, count or classify them. Questions of this nature can be traced as far back as 1835, with a brief remark implicitly about the existence of Steiner triple systems made in a book of J. Plücker.

A design $B(n, q, r, \lambda)$ with parameters (n, q, r, λ) is a collection B of q -element subsets of an n -element set X with the property that every r -element subset of X belongs to exactly λ members of B . These are so named for their relevance to experimental design in statistics, especially when $r = 2$, but they also have other applications in several areas of mathematics and computer science. A Steiner system $S(n, q, r)$ with parameters (n, q, r) is just a design with parameters $(n, q, r, 1)$. The schoolgirl problem asked for a particularly nice type of $S(15, 3, 2)$. The well-known Fano plane in Figure 1 is an $S(7, 3, 2)$ and the finite projective planes form an important class of Steiner systems.

Observe that some simple divisibility conditions among the parameters must hold in order for $B(n, q, r, \lambda)$ to exist. In particular, $\binom{q-i}{r-i}$ must divide $\lambda \binom{n-i}{r-i}$ for each $i \in \{0, 1, \dots, r-1\}$, as seen by considering the members of B that contain any fixed i -element subset of X . A natural and long-standing conjecture, referred to in literature as the ‘Existence Conjecture’, is that for fixed q, r, λ these divisibility conditions are not only necessary but also sufficient for the existence of designs, apart from a finite number of exceptional n .

Until this year, only the cases of the Existence Conjecture with $r = 2$ had been settled, by a constructive proof due to Richard M. Wilson (Caltech), a seminal work carried out in the seventies during Wilson’s doctorate at Ohio State. Another breakthrough was by Luc Teirlinck (Auburn) in 1987: for each r , he constructed infinitely many ‘non-trivial’ designs, that is, $B(n, q, r, \lambda)$ with λ independent of n . No Steiner system with $r \geq 6$ was known to exist.

In January at Oberwolfach, Peter Keevash announced the proof of the Existence Conjecture in its entirety, and he posted a manuscript online soon after (‘The existence of designs’, arxiv:1401.3665, 56 pp.). In March, Dutch mathematicians had the opportunity to hear him discuss this remarkable result at a discrete mathematics seminar in Eindhoven. Keevash is a 35-year-old British mathematician who works mainly in probabilistic and extremal combinatorics. He

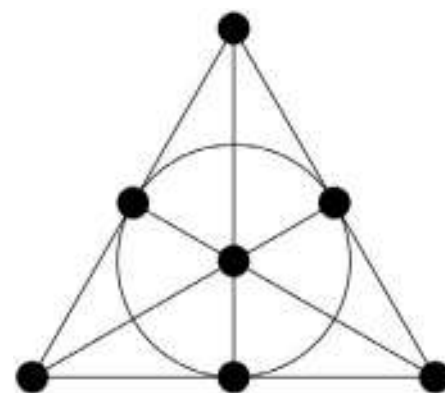


Figure 1 Fano plane.



Photo: Luc Devroey

Peter Keevash during a hiking break from a workshop in Barbados

obtained his bachelor's in Cambridge and his doctorate in Princeton, and was afterwards at Caltech (where he began this work), Birmingham and Queen Mary University of London, before taking up a professorship in Oxford last autumn.

The proof is probabilistic in nature, repeatedly using the following basic principle: having set up a probability space over a set of combinatorial objects, to find *just one* with some desired property it suffices to prove that the probability of a random object having that property is *positive*. Called the *probabilistic method*, this principle appears tautological, but has proven powerful and versatile. It was pioneered by the prolific, collaborative, itinerant Hungarian mathematician Paul Erdős (1913–1996). For interest, the probabilistic method is central to new national master's courses (Mastermath

'Advanced Combinatorics' and 'Probabilistic and Extremal Combinatorics') taught by Tobias Müller (Utrecht) and the author.

An early hint that the probabilistic method could be helpful in the hunt for designs was when Vojtěch Rödl (Emory) in 1985 established an approximate form of the Existence Conjecture for Steiner systems. In doing so, he confirmed a two-decade-old conjecture of Erdős and H. Hanani, and at the same time introduced a technique which has since had wide use in discrete mathematics. (In August Rödl was a main plenary speaker at the ICM in Seoul.) This technique, evocatively named the *Rödl nibble*, is an iterated form of the probabilistic method. It builds up an object gradually over a sequence of steps, each of which is a single application of the 'ordinary' probabilistic method, so that at each step the partial object so far built retains some structural properties that allow the sequence to continue (at least for a time).

In fact, the nibble is integral to Keevash's proof of the Existence Conjecture. Rödl's original approach was to repeatedly, randomly select a set of disjoint q -element subsets to add to the system and then forbid any of the intersected q -element subsets from being selected later. When done skillfully, this procedure can be run until nearly all the elements of X have been covered, yielding an asymptotically optimal Steiner system; however, this approach eventually breaks down as the structure of the remaining eligible q -element subsets deteriorates. The ingenuity of Keevash's approach, which circumvents this difficulty, is that he first constructs (partly by probabilistic means) a special algebraically-defined template — this template induces a partial Steiner system and also admits a flexible set of possible local modifications. The utility of the template is that, after a careful nibble procedure is run to produce another par-

tial Steiner system that is almost complementary, it is possible to use some admissible local modifications of the template to reconcile the difference, so the two partial Steiner systems can be merged into one full one. This is a grossly simplified sketch, and, besides the fact that we discussed only Steiner systems, there are for instance inherent difficulties of handling sparse combinatorial structures, and moreover the proof relies on establishing a stronger result for quasirandom simplicial complexes by a top-level induction on r . The full proof is extremely delicate and it is a phenomenal achievement.

Although the guarantees on n have not yet been carefully optimised, they are not of tower type, as seen say in applications of Szemerédi's regularity lemma. The proof thus constitutes a randomised algorithm that could conceivably be implemented to produce concrete examples, say, for $r = 6$, but this has yet to be carried out.

Keevash's work is a cadence to a fundamental open problem, but certainly there are many further questions to pursue. Just one first step might be to consider if related existence questions for other symmetric rigid combinatorial structures could be resolved with similar techniques. It is well worth mentioning recent work of Kuperberg, Lovett and Peled (2012), in which a different probabilistic approach, a special local central limit theorem for certain lattice random walks, was used to attack several similar questions, where for example they had significantly improved upon Teirlinck's result.

Chatting at drinks following the talk in Eindhoven, Aart Blokhuis (Eindhoven) reminded us of another long-standing and major conjecture in the area, one that is very unlikely to be confirmed with probabilistic methods: projective planes only exist for prime power orders. 

Lex ZandeeNWO, Den Haag
l.zandee@nwo.nl**Petra de Bont**NWO, Den Haag
p.debont@nwo.nl**Onderzoek**

Vernieuwingsimpuls en wiskunde: 14 jaar ervaring

In de artikelen die volgen, worden diverse wiskundeprojecten beschreven die gehonoreerd zijn in de Vernieuwingsimpuls van NWO. In dit inleidende artikel geven Lex Zandee en Petra de Bont van NWO achtergrondinformatie over dit subsidiesysteem, waarbij zij in het bijzonder ingaan op de discipline wiskunde. Zandee is in mei 2014 met pensioen gegaan als disciplinehoofd wiskunde, De Bont is programmamanager voor de discipline wiskunde.

Op 15 februari 2000 reikte minister Hermans van OCW de Spinozapremie voor dat jaar uit aan professor Ronald Plasterk. Het juryrapport vermeldde dat: “de combinatie van zijn jonge leeftijd, speelse geest en fundamentele belangstelling voor biologische fenomenen maakt dat van Plasterk zeker verwacht kan worden dat hij nog jaren ten minste op zijn huidige niveau van creativiteit verder zal gaan”. Bij die gelegenheid ontvouwde minister Hermans ook zijn plannen voor een nieuw financieringsinstrument, de Vernieuwingsimpuls (VI) met een eerste ronde al in 2000. De minister wilde met het geld hiervoor veelbelovende wetenschappers die nog zonder vaste baan zijn de mogelijkheid bieden hun onderzoek een nieuwe impuls te geven en daarmee voor de wetenschap te behouden. In de woorden van Hermans moest het programma zich richten op jonge, dwarse, onorthodoxe onderzoekers. De kandidaten wordt gevraagd hun ideeën kort op papier te zetten ten behoeve van een gesprek met een selectiecommissie waarin het vooral gaat om de creativiteit en gedrevenheid van de kandidaat. De selectieprocedure zou niet-bureaucratisch en snel moeten zijn.

Of het Spinoza-juryrapport voor Ronald Plasterk wat betreft die creativiteit het bij het rechte eind had, laten we aan u ter beoordeling over. Ongetwijfeld werd er in 2007 toen hij aantrad als de nieuwe minister van OCW een geheel andere vorm van creativiteit van hem gevraagd.

De betekenis voor wiskundigen

Die eerste ronde van de Vernieuwingsimpuls in 2000 was een kleine pilot waarin slechts twintig beurzen aan bèta-wetenschappers uitgereikt konden worden. Ze leidde in 2001 tot de eerste toekenning voor een wiskundig voorstel aan Rob Stevenson voor het onderzoek ‘Wavelets for solving operator equations’. De pilot werd als succesvol beschouwd. Als gevolg daarvan kwam er meer geld beschikbaar en werd het programma in 2002 opgesplitst in drie fasen die we nog steeds kennen: Veni, Vidi en Vici. Het jaarlijks budget was 75 miljoen euro, waarvan het NWO-gebied Exacte Wetenschappen (EW: wiskunde, astronomie en informatica) voor de drie disciplines gezamenlijk rond 5 miljoen euro te verdelen kreeg. De universiteiten waren verplicht eveneens hun bijdragen te leveren via

een matching van 32,4 procent aan ieder project.

Toen Ronald Plasterk eenmaal zelf minister van OCW was geworden was net het evaluatierapport over de eerste jaren Vernieuwingsimpuls beschikbaar. Het eindoordeel was positief: de beoordelaars stelden vast dat de Vernieuwingsimpuls “een impuls geeft aan de wetenschappelijke loopbaan van kwalitatief goede onderzoekers”. Op grond van deze positieve evaluatie kondigde de minister een Vernieuwingsimpuls nieuwe stijl aan met een verdubbeld budget en zonder de verplichte matching vanuit de universiteiten. Het klonk mooi maar er ontstond een boel wrevel in het land over de combinatie met de overheveling van 100 miljoen euro die hiermee gepaard ging van de universiteiten naar NWO. Deze overheveling hield voor het gebied EW wel in dat het jaarlijks VI-budget omhoog ging naar een kleine 8 miljoen euro. En dat exclusief de fondsen voor de VI-beurzen die de eerste jaren na 2008 vanuit de disciplines nog in de domeinbeoordeling in de wacht gesleept konden worden. Overigens is deze stap in de procedure alweer afgeschaft.

Financiën VI en VI-EW

Ondertussen zijn we weer vijf jaar verder. Hoe staat het nu met het VI-budget? In 2013 was binnen geheel NWO een VI-budget voorhanden van 150 miljoen euro. Daarvan was voor Vici 46,5 miljoen euro beschikbaar. Omgere-

kend komt dit neer op 31 Vici-posities voor alle wetenschappelijke disciplines bij elkaar.

Dit jaar, 2014, heeft EW ongeveer 7,7 procent van het totale budget van NWO ter beschikking voor de Veni- en de Vidi-ronde, een kleine 8 miljoen euro. Hiermee zijn acht Veni- en zeven Vidi-posities gemoeid. Het Gebiedsbestuur EW stelt ieder jaar vast wat de verdeling van de financiën is over de Veni- en de Vidi-ronde. Vrijkomende middelen, door vertrekkende laureaten, zorgen ervoor dat er eventueel meer posities kunnen worden uitgedeeld. Het gevolg voor dit jaar was dat er uiteindelijk elf Veni-posities beschikbaar waren.

Naast de EW-pot kunnen aanvragen voor Veni's en Vidi's ook bij het gebiedsoverstijgende compartiment ingediend worden. Het ingediende voorstel dient dan een multidisciplinair karakter te hebben en betrekking te hebben op meerdere NWO-gebieden. Kandidaten moeten tegenwoordig wel duidelijk aangeven wat de toegevoegde waarde voor de aangegeven disciplines is. Deze motivatie wordt dan ook meegenomen tijdens het beoordelingsproces.

Naast deze basisposities voor EW is er voor vrouwelijke wiskundigen nog een andere mogelijkheid om financiering binnen te halen binnen de VI.

Aspasia

Het programma Aspasia stimuleert de doorstroom van vrouwelijke wetenschappers naar hogere universitaire functies. Tot nu toe zijn vrouwen in die functies sterk ondervertegenwoordigd. Hoe hoger op de carrièreladder, des te minder vrouwen. Dat geldt zeker voor het wetenschappelijke onderwijs en onderzoek in Nederland. Het programma Aspasia is bedoeld om dat te veranderen.

Aspasia is gekoppeld aan de Vidi- en Vici-competitie. Het programma voorziet in een premie voor universiteiten, bestemd voor de benoeming van vrouwelijke Vidi-kandidaten tot UHD en vrouwelijke Vici-kandidaten tot hoogleraar. Ook voor vrouwelijke onderzoekers die na de interviewselectie voor Vidi of Vici als zeer goed of excellent zijn beoordeeld maar die geen beurs hebben gekregen, kunnen universiteiten onder voorwaarden een premie krijgen als ze deze kandidaten bevorderen tot respectievelijk UHD of hoogleraar. In 2014 bedroeg het budget 3 miljoen euro voor 15–30 premies.

Procedure en commissies wiskunde

Bij de 'officiële' start van de volledige Vernieuwingsimpuls in 2002 maakte de discipli-

ne natuurkunde nog deel uit van het gebied Exacte Wetenschappen. Hierdoor was er ook een groter aantal posities beschikbaar. Er waren in die tijd nog geen strikte voorwaarden verbonden aan de kandidaten die mochten indienen. Het gevolg was dat we overstelpt werden met voorstellen. De interviews werden om die reden uitgevoerd met drie parallelle gebiedsbrede commissies. Aan het eind van de interviewdag kwamen alle commissieleden tezamen om de drie prioriteringslijstjes in elkaar te schuiven. Dat was een interessante exercitie, maar na het opstellen van striktere voorwaarden en het vertrek van de natuurkunde in 2003 uit het gebied EW kon dit gelukkig bijgesteld worden.

Binnen Veni en Vidi bepalen nu discipline (wiskunde, astronomie of informatica) commissies op basis van de voorstellen, referentenoordelen en de weerwoorden welke kandidaten voor een interview worden uitgenodigd. Bij de samenstelling van de discipline wiskundecommissie wordt geprobeerd zoveel mogelijk spreiding te krijgen van expertise, de wiskundecusters en de universiteiten. Daarnaast wordt getracht minstens één vrouwelijk commissielid in de commissie te hebben. Commissieleden hebben maximaal drie keer zitting in een betreffende commissie. Het gebiedsbestuur van Exacte Wetenschappen keurt de samenstelling van deze commissie goed. Parallelle interviewsessies worden nu niet meer gehouden. Een gebiedsbrede commissie neemt de interviews af. Op basis van de te interviewen wiskundigen bepaalt de disciplinaire wiskundecommissie zelf welke commissieleden worden afgevaardigd naar de interviewsessies.

Af en toe worden nog veranderingen in de beoordelingsprocedure doorgevoerd. De laatste grote veranderingen waren in 2012, te weten de wetenschapsbrede Vici-beoordeling en de invoering van het beoordelingscriterium kennisbenutting. Dergelijke veranderingen kunnen vanuit OCW, het Algemeen Bestuur van NWO, maar ook vanuit de gebieden en de onderzoekers worden geïnitieerd via VI-evaluaties. Voor eventuele ontwikkelingen binnen de Vernieuwingsimpuls dient men de nieuw te verschijnen NWO-strategienota in de gaten te houden. Deze verschijnt in het najaar van 2014.

Vici-procedure nu

De Vici-procedure anno 2014 komt voor de wiskundigen er op neer dat hun vooraanmelding eerst binnen het bèta-domein (N, CW, STW, ALW en EW) wordt beoordeeld en het advies wel of niet uitwerken meekrijgt. Na in-

diening van het uitgewerkte voorstel volgt de interviewselectie. Deze selectie vindt plaats op basis van het volledige voorstel, referentenoordelen en het weerwoord en vindt ook binnen het bèta-domein plaats. De commissie die het uiteindelijke interview afneemt, is samengesteld uit alle wetenschappelijke disciplines. In totaal worden ongeveer zestig interviews gehouden in drie dagen, waarvan uiteindelijk ongeveer dertig kandidaten worden gehonoreerd. Suggesties voor wiskundige commissieleden komen vanuit het EW-bureau. Referenten worden nog wel steeds door het bureau van het gebied gezocht op de manier zoals hier verderop wordt beschreven. Hieruit volgt gelijk de spagaat waarin de aanvrager zich bevindt. Het voorstel moet leesbaar zijn voor niet-experts, maar ook uitdagingen bevatten voor de experts vanuit de wiskunde.

Referenten

Binnen Exacte Wetenschappen is het gebruikelijk deze experts in het buitenland te zoeken. Ze worden gezocht op basis van de informatie in het ingediende voorstel. Denk daarbij bijvoorbeeld aan de aangeleverde keywords, de referenties in het voorstel, de belangrijkste publicaties van de kandidaat met relevantie voor het ingediende voorstel, deelname aan workshops, et cetera. Mogelijke referenten worden daarna zorgvuldig gecontroleerd op een eventuele belangenverstrengeling. In het verleden werden ook de commissieleden verzocht om mogelijke suggesties aan te dragen voor referenten. Krapte in het tijdsplan zorgt er tegenwoordig voor dat deze weg nog nauwelijks bewandeld wordt.

De algemene tendens is dat onderzoekers het steeds drukker krijgen, waardoor een positieve respons op het verzoek voor het referentenrapport afneemt. In sommige extreme gevallen moeten er zelfs vijf keer zoveel referenten benaderd worden dan er nodig zijn om tot het gewenste referentenaantal te komen.

Kennisbenutting

Sinds 2012 is aan de subsidieaanvraag ook een paragraaf toegevoegd waarin de benutting van de uit het onderzoek voortvloeiende kennis dient te worden beschreven. Veel wiskundigen hebben hier hun bedenkingen over geuit omdat ze hun onderzoek niet willen opzetten met het oog op toepassingen op korte termijn. In sommige aanvragen is zelfs geschreven dat de kennis uit het voorgestelde onderzoek niet benut kan worden. In praktijk weet een beoordelingscommissie een dergelijk statement niet te waarderen omdat er

ook een gebrek aan bereidheid uit naar voren komt om zelfs over het aspect van een eventuele toepassing na te denken. Nog erger is het als de selectiecommissie overduidelijke toepassingen herkent terwijl de indiener die zelf niet aangeeft. En dat is jammer want het criterium kennisbenutting weegt wel voor 20 procent mee in het eindoordeel over het voorstel. Gelukkig is de uitleg bij de desbetreffende paragraaf in de loop der jaren wel verbeterd. Op de NWO-website is nu ook een document beschikbaar waarin voor de indieners verdere handreikingen en suggesties staan om de kennisparagraaf op de juiste manier in te vullen. Hierbij wordt ook als mogelijkheid aangegeven om het aspect van kennisdisseminatie uit te werken, bijvoorbeeld via lezingen en interviews met studenten, en zo het onderzoek en de resultaten laagdrempelig te presenteren. Deze *outreach*-activiteiten dragen immers bij aan de bewustwording bij jongeren voor het belang van wiskunde als wetenschap, nodig voor een economisch en sociaal welvarend land.

Vereniging voor VI-onderzoekers

Mocht men uiteindelijk bij de gelukkigen binnen de Vernieuwingsimpuls horen dan kan men gratis lid worden van de Vereniging Voor Vernieuwingsimpuls Onderzoekers (VVViO). De VVViO behartigt sinds 2004 de belangen van alle VI-laureaten. VVViO vertegenwoordigt hiermee de nieuwe generatie van Nederlandse toponderzoekers uit alle gebieden van de wetenschap. De activiteiten van VVViO zijn onder andere: een jaarlijks symposium met thema's rond wetenschapsbeleid en prominente gastsprekers, netwerkborrels, gesprekken met beleidsmakers bij NWO en met Tweede Kamerwoordvoerders wetenschapsbeleid.

In de afgelopen jaren heeft VVViO zich onder meer sterk gemaakt voor de invoering van het *Principal Investigator* en *Tenure Track*-systeem, de afschaffing van de matchingsverplichting en veranderingen in het wetenschapsbeleid (zoals verschuivingen in eerste en derde geldstromen). Actuele thema's van dit moment zijn de keerzijden van 'focus en massa' en 'valorisatie' voor innovatie en excellent onderzoek.

VI-resultaten voor de wiskunde

Dan nu mogelijk de belangrijkste paragraaf voor de wiskundigen in dit artikel. Wat waren de prestaties van Exacte Wetenschappen en de wiskunde in het bijzonder binnen de Vernieuwingsimpuls? In Tabel 1 tot en met 4 vindt men de honoreringspercentages binnen

de Veni, Vidi en de Vici van Exacte Wetenschappen over de afgelopen jaren.

Kijkend naar de cijfertjes valt het volgende op (zie Tabel 1–3): 36 procent van de totaal ingediende VI-voorstellen binnen EW hebben een wiskundige achtergrond. Het gemiddelde honoreringspercentage van de wiskunde ligt een klein beetje hoger dan het gemiddelde honoreringspercentage voor geheel EW. Wiskundigen zijn net zo succesvol en vaak succesvoller dan een van de andere disciplines binnen Exacte Wetenschappen geweest.

Opvallend is dat de wiskundige vrouwen het binnen het Veni-compartiment beduidend slechter doen dan de vrouwen binnen de andere disciplines van EW. Wat we al jaren weten ten aanzien van de vrouwen in de bètawetenschappen komt ook hier duidelijk uit de getallen naar voren. Van de in totaal 421 ingediende wiskundige VI-voorstellen zijn er slechts 52 ingediend door een vrouwelijke wiskundige. Dit komt neer op een percentage van 12 procent. De twee andere disciplines

binnen EW komen tot een gemiddeld percentage van 18 procent. Hoe verder men komt in de VI-carrièrelijn, hoe lager het percentage vrouwelijke kandidaten dat indient (bij Vici slechts 8 procent). Dit blijft natuurlijk een punt van zorg voor zowel beleidsmakers als universiteiten en wordt al jaren aangekaart in de verschillende strategie/masterplannen van de wiskunde.

In Tabel 4 is getracht enige indicatie voor het carrièrepad van wiskundigen binnen de Vernieuwingsimpuls weer te geven. Combineren van deze tabel met gegevens in Tabel 2 en 3 leert ons het volgende: acht van de 29 tot nu toe gehonoreerde Vidi's hadden eerst een Veni-beurs binnengehaald. Van de Vici-gehonoreerden hebben zelfs acht van de vijftien al eerder een VI-beurs gekregen. Tot nu toe zijn er twee Veni's die het uiteindelijk tot een Vici geschopt hebben. Één heeft het gehele traject van Veni–Vidi–Vici doorlopen, de andere heeft de Vidi-stap overgeslagen. De laatste vijf Vici's (2010–2013) die geho-

	Veni 2002 t/m 2013			Veni 2002 t/m 2013		
	EW ingediend	EW gehonoreerd	%	Wiskunde ingediend	Wiskunde gehonoreerd	%
Totaal	607	119,5	19,7	206	48	23,4
Vrouw	114	25	21,9	31	3	9,8
Man	493	94,5	19,2	175	45	25,7

Tabel 1 Honoreringspercentage Veni voor de periode 2002 t/m 2013 voor Exacte Wetenschappen (alle drie de disciplines) en wiskunde.

	Vidi 2002 t/m 2013			Vidi 2002 t/m 2013		
	EW ingediend	EW gehonoreerd	%	Wiskunde ingediend	Wiskunde gehonoreerd	%
Totaal	417	72	17,3	154	29	18,8
Vrouw	61	15	24,6	16	4	25,0
Man	356	57	16,0	138	25	18,1

Tabel 2 Honoreringspercentage Vidi voor de periode 2002 t/m 2013 voor Exacte Wetenschappen (alle drie de disciplines) en wiskunde.

	Vici 2002 t/m 2013			Vici 2002 t/m 2013		
	EW ingediend	EW gehonoreerd	%	Wiskunde ingediend	Wiskunde gehonoreerd	%
Totaal	151	35	22,8	61	15	24,6
Vrouw	15	4	26,7	5	1	20,0
Man	136	31	22,5	56	14	25,0

Tabel 3 Honoreringspercentage Vici voor de periode 2002 t/m 2013 voor Exacte Wetenschappen (alle drie de disciplines) en wiskunde.

	Veni	Vidi	Veni en Vidi	Totaal
Veni	-	-	-	-
Vidi	7	-	-	7
Vici	1	6	1	8
Totaal	8	6	1	15

Tabel 4 Stapeling gehonoreerde wiskundige Veni's, Vidi's en Vici's. Kolomsgewijs: zeven Vidi's hadden eerst een Veni-beurs ontvangen.

noreerd zijn waren allen al eerder succesvol binnen de Vernieuwingsimpuls. Dit geeft een mooie illustratie van het geconstateerde feit uit de evaluatie van 2006 dat de Vernieuwingsimpuls “een impuls geeft aan de wetenschappelijke loopbaan van kwalitatief goede onderzoekers”.

Ondertussen hopen we erop dat de Vernieuwingsimpuls als instrument gebruikt wordt om talentvolle onderzoekers klaar te stomen voor de volgende stap in hun carrière, het binnenhalen van een *ERC grant*. Met dit Europese instrument van de European Research Council (ERC) is veel meer geld gemoeid dan met de Vernieuwingsimpuls. De honoreringspercentages voor de wiskunde liggen binnen de ERC tegenwoordig om en nabij de 14 procent. Hier liggen duidelijk kansen voor de Nederlandse wiskundigen. Het

blijkt dat acht van de elf *ERC starting grant*-laureaten uit de totale EW-achterban eerder een Veni- of Vidi-beurs hebben ontvangen.

Helaas worden we de laatste tijd ook steeds vaker met het feit geconfronteerd dat gehonoreerde Vidi's en Vici's naar het buitenland vertrekken, de welbekende *braindrain*. Sommige gehonoreerden vertrekken zelfs al voordat ze begonnen zijn met hun VI-project. Voor de onderzoekers in kwestie zeer begrijpelijk, zij kunnen een nog betere positie in het buitenland krijgen. De aldus vrijgekomen middelen worden wederom in de VI van Exacte Wetenschappen gestopt, echter is dit bedrag pas beschikbaar in de volgende honoringsronde.

Tot slot

Met een gemiddelde duur van een VI-project

van vijf tot zeven jaar zijn er binnen de wiskunde al aardig wat projecten afgerond sinds de introductie van de VI in 2000. Veel gehonoreerden komen we bij Exacte Wetenschappen regelmatig tegen in beoordelingscommissies, programmacommissies en andere gerelateerde gremia. Al deze (toen nog) jonge, dwarse en onorthodoxe onderzoekers hebben we nodig om in Nederland het wiskundig onderzoek op peil te houden. Deze onderzoekers dragen ondertussen ook bij aan de strategiebepaling van wiskunde in de vorm van masterplannen en visiedocumenten. Laten we hopen dat de Vernieuwingsimpuls in de komende jaren steeds nieuwe talentvolle wiskundigen op weg helpt in hun wetenschappelijke carrière. Via hun talent blijft de wiskunde in Nederland op hoog niveau floreren. 

Ronald de Wolf

CWI, Amsterdam

en ILLC, Universiteit van Amsterdam

rdewolf@cwi.nl

Onderzoek Vidi-project

Kwantumcomputers

Van december 2008 tot februari 2014 werkt Ronald de Wolf aan het Vidi-project 'Quantum computing: fault-tolerance, communication, and classical spin-offs'. Dit project gaat over het gebruik van kwantummechanische technieken in de informatica. Sinds het eerste kwart van de twintigste eeuw domineert de kwantummechanica de natuurkunde van het 'kleine': het gedrag van deeltjes als fotonen, elektronen, atomen, enzovoort. Hoewel de combinatie van de kwantummechanica met de relativiteitstheorie (die de zwaartekracht beschrijft) problematisch is, zijn tot nu toe al haar experimentele voorspellingen uitgekomen. Kwantummechanica is veel meer dan alleen esoterische theorie: volgens sommige berekeningen is een derde van ons Bruto Nationaal Product afhankelijk van onze kennis van de kwantummechanica, denk bijvoorbeeld aan elektronische apparatuur.

Kwantummechanica heeft allerlei tegen-intuïtieve effecten, zoals *superpositie* van verschillende toestanden, constructieve en destructieve *interferentie*, en *verstrengeling* tussen verschillende kwantumsystemen. Sinds het werk van Feynman [12] en Deutsch [9] in de jaren tachtig wordt er geprobeerd om dit soort vreemde effecten te gebruiken om computers te verbeteren: te versnellen, veiliger te maken, enzovoort.

Er zijn grofweg twee soorten vragen die onderzoekers zich hierover stellen: (1) kun je een grote kwantumcomputer bouwen? en (2) wat zou zo'n computer kunnen doen? De eerste vraag is voer voor experimenteel natuurkundigen. Er is gestage vooruitgang op dit gebied, hoewel de grootste kwantumcomputers die tot nu toe gerealiseerd zijn maar op een handvol kwantumbits werken. Informatici richten zich op de tweede vraag: wat zijn de potentiële toepassingen van een kwantumcomputer? Een aantal belangrijke voorbeelden zijn het algoritme van Shor [21] voor het efficiënt vinden van de priemfactoren van grote getallen (dit breekt allerlei veelgebruikte cryptografie, zoals RSA), het algoritme van

Grover [15] voor het doorzoeken van grote databases, en het protocol van Bennett en Brassard [4] voor het veilig uitwisselen van geheime sleutels over een publiek kwantumcommunicatiekanaal.

In dit Vidi-project heb ik, samen met promovendus Giannicola Scarpa en postdocs Fernando de Melo en Niel de Beaudrap, geprobeerd de theorie van kwantumcomputers verder te ontwikkelen en meer toepassingen te vinden.

Het project en de resultaten

Aangezien dit project fundamenteel onderzoek is, zijn de voornaamste resultaten publicaties: dertien artikelen in tijdschriften, dertien artikelen in proceedings van conferenties, en zes preprints die naar verwachting de komende tijd ook in tijdschriften of proceedings zullen verschijnen. Daarnaast was er één proefschrift, van Giannicola Scarpa.

Hieronder zal ik de drie onderdelen van het project bespreken met een paar van de interessantste uitkomsten. Het eerste onderdeel viel een beetje tegen, de andere twee waren behoorlijk succesvol.

Fout-tolerante kwantum computers

Het eerste onderdeel van het project was gericht op technieken om kwantumcomputers te beschermen tegen ruis en kleine foutjes in de implementatie van de operaties. Zulke foutjes zijn vrijwel onvermijdelijk wanneer je een echte kwantumcomputer wilt bouwen, dus het is essentieel dat we daarvoor kunnen corrigeren. Een van de belangrijkste theoretische resultaten is de 'fault-tolerant threshold theorem' [1]. Dit zegt dat als je de fout per operatie kleiner kunt maken dan een bepaalde constante waarde p (de 'threshold'), en als de fouten op de verschillende operaties niet al te sterk gecorreleerd zijn, dan kun je je kwantumcomputer 'fault-tolerant' maken, dat wil zeggen je kunt de kans dat het eind-antwoord fout is zo klein maken als je wilt. De precieze waarde van deze p is natuurlijk erg belangrijk — het vertelt experimentalisten hoe precies ze hun operaties moeten implementeren om een werkende kwantumcomputer mogelijk te maken. Er is nog veel onzekerheid over deze waarde: p is minstens 0,1 procent [2] en hoogstens ongeveer 36 procent [17]. Numerieke experimenten suggereren dat de correcte waarde boven 1 procent ligt [16].

Het voornaamste doel van dit deel van het project was om de waarde van de threshold veel preciezer te bepalen. Dit is helaas niet gelukt, we zijn er niet in geslaagd om de ondergrenzen en/of de bovengrenzen op p te verbeteren (overigens is er ook in de rest van de wereld de afgelopen vijf jaar geen vooruitgang geboekt op dit punt). Het interessantste wat wel uit dit project is gekomen is een artikel van de Melo et al. [19] dat nieuwe (maar

nog steeds niet erg precieze) boven- en ondergrenzen geeft op de waarde van de threshold wanneer zogenaamde ‘Majorana Fermionen’ gebruikt worden voor de kwantum-bits.

Kwantumcommunicatie

Sommige van de interessantste kwantummechanische toepassingen betreffen netwerken van verschillende computers. Soms gaat het hierbij om het *beveiligen* van gegevens en communicatie (kwantumcryptografie) en soms om het *minimaliseren* van de benodigde hoeveelheid communicatie tussen de verschillende computers (kwantumcommunicatie-complexiteit). Het project leverde een aantal publicaties op over kwantumcommunicatie-complexiteit, maar het interessantste resultaat hier is waarschijnlijk een toepassing op zogenaamde *kwantum-non-lokaliteit*, die we hieronder zullen bespreken.

Stel je een spel voor met twee spelers, die we Alice en Bob zullen noemen, en die onderling niet mogen communiceren. Beide spelers krijgen een invoer, respectievelijk x en y , volgens een bepaalde waarschijnlijkheidsverdeling. Beide spelers geven daarop een uitvoer, respectievelijk a en b . De regels van het spel stipuleren dat (gegeven het invoerpaar x, y) sommige uitvoerparen het spel ‘winnen’ en andere uitvoerparen het spel ‘verliezen.’ Het doel van de spelers is om de kans om het spel te winnen te maximaliseren. Laten we de maximale winkans van spelers die de klassieke natuurkunde volgen ω noemen. Bovengrenzen op deze waarde ω staan bekend als Bell-ongelijkheden, genoemd naar Jon Bell [6]. Het blijkt nu dat als de spelers *kwantumverstrengeling* delen, dat ze hun gedrag beter kunnen coördineren en dat de winkans soms hoger wordt. Laten we de maximale winkans die mogelijk is met behulp van verstrengeling ω^* noemen. Elk spel waarbij $\omega^* > \omega$ wordt een ‘schending van de Bell-ongelijkheid’ genoemd. In simpele gevallen kunnen dit soort verstrengelingstrategieën in het laboratorium worden uitgevoerd, en dan blijkt de kwantumwinkans inderdaad hoger te zijn dan het maximale wat klassieke spelers kunnen bereiken. Dit soort experimenten heeft een diepere betekenis: ze laten zien dat onze wereld zich niet gedraagt volgens wat voor ‘klassieke’ natuurkunde dan ook. Het is interessant om spellen te ontwerpen die het verschil tussen de kwantum- en de klassieke winkans (gemeten als de ratio ω^*/ω) zo groot mogelijk maken. In [7] hebben we spellen beschreven waarbij de-

ze ratio vrijwel maximaal is (als functie van de ‘hoeveelheid’ verstrengeling waarmee de spelers beginnen), gebaseerd op eerdere resultaten uit de kwantumcommunicatie-complexiteit.

Een tweede hoogtepunt is het proefschrift van Giannicola Scarpa [20], wat ook over non-lokaliteit gaat. Neem als voorbeeld het volgende spel. Er is een bepaalde graaf G die bekend is gemaakt aan Alice en Bob. Alice en Bob krijgen elk een knoop van G als invoer en moeten (zonder te communiceren) een kleur als uitvoer geven met de volgende eigenschappen: als Alice en Bob dezelfde knoop als invoer krijgen dan moeten ze *dezelfde* kleur als uitvoer geven, en als hun twee invoerknoppen een kant in G vormen dan moeten ze *verschillende* kleuren als uitvoer geven. Wat is het minimale aantal verschillende kleuren dat Alice en Bob moeten gebruiken om dit spel met zekerheid te kunnen winnen? Dat blijkt het chromatisch getal $\chi(G)$ van de graaf G te zijn: het minimale aantal kleuren dat je nodig hebt om de knopen van G te kleuren zodanig dat buurknopen een verschillende kleur hebben. Het blijkt dat er (voor sommige grafen) strategieën zijn die door gebruik van kwantumverstrengeling minder kleuren nodig hebben om het spel met zekerheid te kunnen winnen. Dit leidt tot een definitie van het *kwantumchromatisch getal* van de graaf G [8]. Scarpa et al. bewijzen allerlei eigenschappen van dit soort kwantumgraafparameters, en laten in het bijzonder zien dat voor sommige grafen het kwantumchromatisch getal exponentieel kleiner kan zijn dan het chromatisch getal. Scarpa et al. hebben ook voorbeelden gegeven waarbij kwantumverstrengeling de capaciteit van een klassiek communicatiekanaal flink kan verhogen.

Toepassingen op klassieke problemen

De laatste tien jaar zijn er een aantal verrassende toepassingen gevonden van *quantum computing* (beter gezegd: van de wiskundige technieken die ontwikkeld zijn in dit vakgebied) op problemen in de klassieke informatica en de wiskunde. Een van de eerste voorbeelden hiervan was een ondergrens voor bepaalde fout-corrigerende codes [18]. Dit loste een open vraag op over klassieke codes, maar het bewijs maakte essentieel gebruik van technieken uit de kwantuminformatietheorie. Dit kun je vergelijken met het bewijzen van eigenschappen van reële getallen door gebruik te maken van de complexe getallen, of met Paul Erdős’ ‘probabilistic method’ waarin existentie-bewijzen gegeven worden

met behulp van gereedschap uit de waarschijnlijkheidsrekening. Sindsdien zijn er nog een aantal andere voorbeelden van dit fenomeen gevonden, en het doel van dit deel van het project was om meer van zulke onverwachte toepassingen van het ‘kwantumgereedschap’ te vinden. Ik zal er hieronder twee noemen. Voor meer voorbeelden, zie het overzicht van Drucker en mijzelf [10]. Merk op dat voor dit soort toepassingen geen grote kwantumcomputer nodig is. We gebruiken hier alleen het wiskundig gereedschap dat voor de analyse van kwantumcomputers ontwikkeld is.

Polynomen

Ten eerste kunnen we gebruikmaken van een al bekende connectie tussen kwantumalgoritmes en polynomen [5]: grof gezegd kan de output van een kwantumalgoritme geschreven worden als een polynoom over de inputvariabelen. Hoe efficiënter het algoritme, hoe lager de graad van het polynoom. Dit betekent dat je soms het bestaan van laaggraadspolynomen met bepaalde gewenste eigenschappen kunt bewijzen door middel van het construeren van efficiënte kwantumalgoritmes.

Samen met Drucker heb ik dit gebruikt om een nieuw bewijs te geven van de stelling van Jackson uit de analyse [11]. Deze stelling is een kwantitatieve versterking van de beroemde stelling van Weierstrass, die zegt dat elke continue functie op een gesloten interval willekeurig goed kan worden benaderd door een polynoom. Jacksons versterking geeft aan hoe klein we de benaderingsfout kunnen maken, in termen van de ‘gladheid’ van de te approximeren functie, en de maximale graad die het approximerende polynoom mag hebben. Door gebruik te maken van efficiënte kwantumalgoritmes voor het tellen van het aantal enen in een gegeven binaire string, konden we een nieuw bewijs geven van deze klassieke stelling.

Een andere toepassing van deze connectie komt van Ambainis en mijzelf [3]. Met Fourier-analytische technieken konden we laten zien wat de minimale graad is van polynomen die een n -bits functie approximeren; en met behulp van efficiënte kwantumalgoritmes konden we laten zien dat er functies bestaan waarvoor onze ondergrens op de graad optimaal is.

Het handelsreizigersprobleem

Ten tweede hebben we een resultaat over kwantumcommunicatie kunnen gebruiken om te laten zien dat lineaire programma’s voor

het bekende *handelsreizigersprobleem* ("traveling salesman problem") exponentieel groot moeten zijn [13–14]. Deze onverwachte connectie loste een oud open probleem op, en kreeg de 'Best Paper Award' op de STOC'12-conferentie. Dit resultaat is waarschijnlijk het interessantste dat uit dit Vidi-project is gekomen.

In het handelsreizigersprobleem moeten we, op een gegeven graaf met n knopen en gewichten op de kanten, een kortste tour vinden die precies één keer langs elke knoop gaat en die terugkeert op zijn beginpunt. Dit is een van de bekendste 'NP-harde' problemen. Waarschijnlijk (als $P \neq NP$) is er geen efficiënt algoritme voor — maar niemand weet hoe we dit kunnen bewijzen. Het handelsreizigersprobleem correspondeert met het optimaliseren van een lineaire functie (de lengte van de route) over de *polytoop* die opgespannen wordt door alle tours door de graaf. Als je deze polytoop met een klein aantal lineaire ongelijkheden zou kunnen karakteriseren, dan heb je een lineair programma waarmee je efficiënt

het handelsreizigersprobleem kunt oplossen. In de jaren tachtig waren er mensen die claimden dit te kunnen [22]. Yannakakis [24] bewees al in 1987 dat de 'symmetrische' manier waarop dit gebeurde niet kon werken. Wij hebben nu laten zien dat *elke* set van ongelijkheden voor deze polytoop exponentieel groot moet zijn, zelfs wanneer je allerlei hulpvariabelen en niet-symmetrische stelsels ongelijkheden mag gebruiken. Dit bewijst dat een grote klasse van programma's niet in staat is efficiënt het handelsreizigersprobleem op te lossen.

Waar zit nu de connectie met kwantumcommunicatie? Yannakakis liet al zien dat het aantal benodigde ongelijkheden precies gelijk is aan de 'positieve rank' van de zogenaamde '*slack matrix*' die bij de polytoop hoort. Voor een ondergrens op het aantal ongelijkheden is het dus voldoende om een submatrix van de bijbehorende *slack matrix* te vinden die aantoonbaar een hoge positieve rank heeft. Nu bleek een matrix die ik tien jaar eerder gebruikt en geanalyseerd had om

iets te bewijzen over kwantumcommunicatiecomplexiteit [23], hiervoor precies te passen.

Conclusie

Kwantumcomputers zijn veelbelovend, maar er moet nog veel gebeuren om die belofte uit te laten komen. Het zou mooi zijn als iemand kan aantonen dat de 'fault-tolerance threshold' redelijk hoog is. Dat zou het makkelijker maken om een grote kwantumcomputer in het lab te maken. En hopelijk worden er in de toekomst nog meer toepassingen gevonden zoals kwantumalgoritmes, communicatie-protocollen, enzovoort. Dit project heeft een aantal bijdrages geleverd aan dit laatste. Sommige van deze bijdrages zijn afhankelijk van de bouw van een grote kwantumcomputer, andere bijdrages zijn toepassingen van kwantumwiskundig gereedschap op de klassieke informatica en wiskunde, en zijn daarom vandaag al relevant. Inmiddels heeft de EU mij een ERC Consolidator Grant toegekend, waarmee ik dit onderzoek voort kan zetten.

Referenties

- 1 D. Aharonov en M. Ben-Or, Fault tolerant quantum computation with constant error, in *Proceedings of 29th ACM STOC*, 1997, pp. 176–188.
- 2 P. Aliferis, D. Gottesman en J. Preskill, Accuracy threshold for postselected quantum computation, *Quantum Information and Computation* 8 (2008), 181–244.
- 3 A. Ambainis en R. de Wolf, How low can approximate degree and quantum query complexity be for total boolean functions?, in *Proceedings of 28th IEEE Annual Conference on Computational Complexity (CCC'13)*, 2013, pp. 179–184.
- 4 C. H. Bennett en G. Brassard, Quantum cryptography: Public key distribution and coin tossing, in *Proceedings of the IEEE International Conference on Computers, Systems and Signal Processing*, 1984, pp. 175–179.
- 5 R. Beals, H. Buhrman, R. Cleve, M. Mosca en R. de Wolf, Quantum lower bounds by polynomials, *Journal of the ACM* 48 (2001), 778–797.
- 6 J. S. Bell, On the Einstein-Podolsky-Rosen paradox, *Physics* 1 (1964), 195–200.
- 7 H. Buhrman, O. Regev, G. Scarpa en R. de Wolf, Near-optimal and explicit Bell inequality violations, *Theory of Computing* 8 (2012), 623–645.
- 8 P. J. Cameron, A. Montanaro, M. W. Newman, S. Severini en A. Winter, On the quantum chromatic number of a graph, *Electronical Journal of Combinatorics* 14 (2007).
- 9 D. Deutsch, Quantum theory, the Church–Turing principle, and the universal quantum Turing machine, in *Proceedings of the Royal Society of London*, Vol. A400, 1985, pp. 97–117.
- 10 A. Drucker en R. de Wolf, Quantum proofs for classical theorems, *Theory of Computing*, 2011, ToC Library, Graduate Surveys 2.
- 11 A. Drucker en R. de Wolf, Uniform approximation by (quantum) polynomials, *Quantum Information and Computation* 11 (2011), 215–225.
- 12 R. Feynman, Simulating physics with computers, *International Journal of Theoretical Physics* 21 (1982), 467–488.
- 13 S. Fiorini, S. Massar, S. Pokutta, H. R. Tiwary en R. de Wolf, Linear vs. semidefinite extended formulations: exponential separation and strong lower bounds, in *Proceedings of 44th ACM STOC*, 2012, pp. 95–106.
- 14 S. Fiorini, S. Massar, S. Pokutta, H. R. Tiwary en R. de Wolf, Exponential lower bounds for polytopes in combinatorial optimization, te verschijnen in *Journal of the ACM*, 2014.
- 15 L. K. Grover, A fast quantum mechanical algorithm for database search, in *Proceedings of 28th ACM STOC*, 1996, pp. 212–219.
- 16 M. Knill, Quantum computing with realistically noisy devices, *Nature* 434 (2005), 39–44.
- 17 J. Kempe, O. Regev, F. Unger en R. de Wolf, Upper bounds on the noise threshold for fault-tolerant quantum computing, *Quantum Information and Computation* 10 (2010), 361–376.
- 18 I. Kerenidis en R. de Wolf, Exponential lower bound for 2-query locally decodable codes via a quantum argument, in *Proceedings of 35th ACM STOC*, 2003, pp. 106–115.
- 19 F. de Melo, P. Cwiklinski en B. M. Terhal, The power of noisy fermionic quantum computation, *New Journal of Physics* 15 (2013), 013015.
- 20 G. Scarpa, *Quantum entanglement in non-local games, graph parameters and zero-error information theory*, PhD thesis, University of Amsterdam, 2013.
- 21 P. W. Shor, Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer, *SIAM Journal on Computing* 26 (1997), 1484–1509 (eerdere versie in FOCS'94).
- 22 T. Swart, $P = NP$, Technical report, University of Guelph, 1986. Revision 1987.
- 23 R. de Wolf, Characterization of non-deterministic quantum query and quantum communication complexity, in *Proceedings of 15th IEEE Conference on Computational Complexity*, 2000, pp. 271–278.
- 24 M. Yannakakis, Expressing combinatorial optimization problems by linear programs (extended abstract), in *Proceedings of 20th ACM STOC*, 1988, pp. 223–228.

Bert Zwart

Research Group Stochastics
CWI, Amsterdam
bert.zwart@cwi.nl

Onderzoek Vidi-project

De macroscop

In 2008 ontvangt Bert Zwart een Vidi-subsidie voor het project 'High dimensional service systems'. Dit fundamentele onderzoek richt zich op analyse van complexe systemen en procedures waarin zoveel factoren een rol spelen dat traditionele analysemethoden onbruikbaar zijn. Daarbij kan bijvoorbeeld gedacht worden aan de bezetting in een callcenter met honderden telefonisten. Dat soort systemen valt niet door te rekenen. Als je meer ongeduldige klanten hebt, dan verandert ook het aantal benodigde medewerkers.

Onlangs liep mijn periode als Vidi-laureaat af, een mooie periode waarin ik dankzij NWO in staat werd gesteld me te richten op enkele fundamentele vragen in mijn onderzoeksrichting. Hoewel mijn Vidi-beurs werd toegekend in augustus 2008, begonnen de voorbereidingen achteraf gezien al in 2005. Toen liep mijn Veni-beurs af, en besloot ik om geen Vidi-voorstel in te dienen. In plaats daarvan koos ik voor een verblijf in het buitenland.

Ik kwam als associate professor terecht bij het Georgia Institute of Technology in Atlanta. Daar had ik het naar mijn zin en kreeg ik in februari 2008 ook een vaste aanstelling (tenure). Toch besloot ik terug te keren naar Nederland. Ik had, om alle opties open te houden, al een Vidi-voorstel ingediend. Dit voorstel was geïnspireerd door diverse ontwikkelingen in mijn vakgebied die zich in die tijd grotendeels in de Verenigde Staten afspeelden, en waar ik in Atlanta ook aan werkte. Op 1 augustus 2008, mijn eerste werkdag op het CWI, ontving ik het heuglijke nieuws dat mijn Vidi-voorstel was toegekend.

Waar ging het voorstel over? Op de NWO-website staat nog steeds de volgende accurate informatie bij de Vidi-toekenningen in 2008:

Grootschalige bedieningssystemen onder de macroscop

Dr. A.P. (Bert) Zwart (m) 16-04-1974, CWI - Wiskunde

Wiskundige modellen voor computer- en communicatienetwerken, callcenters en productieprocessen zijn vaak hoogdimensionaal en daarom moeilijk analyseerbaar. Dit onderzoeksproject beoogt de complexiteit van dergelijke modellen te reduceren door zich te richten op het macroscopische gedrag.

Belangrijke standaardwerken binnen mijn vakgebied zijn [2] en [8], maar de technieken beschreven in die standaardwerken zijn vaak alleen geschikt voor modellen op een eindig-dimensionale toestandsruimte. Een belangrijke categorie van modellen welke modernere technieken vereisen zijn wachtrijen waarbij het aantal bediendes zeer groot is, hetgeen relevant is voor bijvoorbeeld callcenters en cloud computing. Hoewel ik hier binnen mijn Vidi-project ook aan gewerkt heb, zal ik me in dit artikel verder richten op een ander model. Dit model beschrijft congestie in communicatienetwerken, en vereist ook een oneindig-dimensionale toestandsruimte. De resultaten

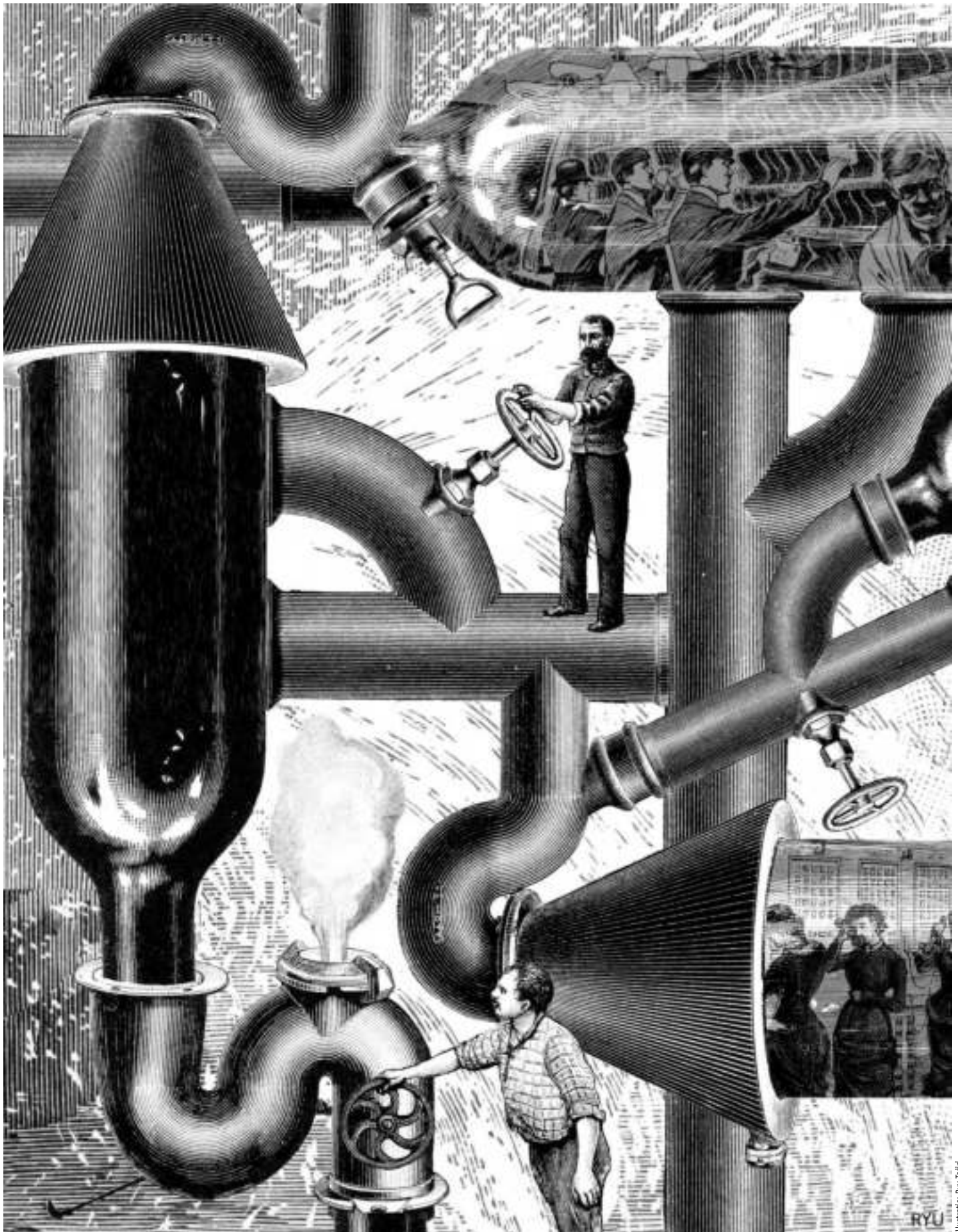
zijn beschreven in [6], alsmede in Hoofdstuk 3 van het proefschrift van Maria Remerova [5].

Wanneer je het internet gebruikt voor het bekijken van een video, het versturen van een file, of het voeren van een telefoongesprek, dan maak je doorgaans gebruik van meerdere knooppunten, ook wel links genoemd. Deze links kunnen bottlenecks vormen, waardoor vertraging op kan treden. Dit kan leiden tot ongewenst gedrag, zoals het afbreken van een sessie door ongeduldige gebruikers. Om deze reden is het belangrijk om inzichten te verwerven in het gedrag van communicatienetwerken. Dit soort inzichten kunnen worden ontwikkeld met behulp van wiskundige modellen, hetgeen de motivatie is voor het gedane onderzoek.

Modelbeschrijving

In Figuur 1 is elke link in een netwerk, die je in traditionele wachtrij-terminologie bedienen zou kunnen noemen, weergegeven door een cirkel. Een communicatiesessie (denk bijvoorbeeld aan een datatransmissie of telefoongesprek) in het netwerk volgt een bepaalde route die uit meerdere links bestaat. Zo'n sessie zou je in traditionele wachtrij-terminologie klant kunnen noemen. Er zijn I routes en J links. A is een $0-1$ matrix waarbij $A_{ji} = 1$ als route i gebruik maakt van link j . De totale hoeveelheid data die link j per tijdseenheid kan verwerken is C_j .

Het aantal klanten dat gebruikmaakt van route i geven we weer met z_i , en we noemen $z = (z_1, \dots, z_I)$ de populatievector. Ge-





Figuur 1 Een netwerk met drie links en vier routes.

geven een populatie z definiëren we $\Lambda(z)$ als de vector met bedieningssnelheden per route, deze worden ook wel bandbreedtes genoemd. Elke klant op route i wordt bediend met snelheid $\Lambda_i(z)/z_i$ — klanten op dezelfde route worden bediend met dezelfde snelheid. Daarnaast hebben klanten op route i ook een bovengrens m_i op de individuele bandbreedte.

Verder nemen we aan dat een klant op route i een nut $U_i(x)$ toekent aan een bedieningssnelheid x , en dat de allocatie van toegewezen bandbreedtes $\Lambda(z)$ in elke toestand z wordt bepaald door het totale, gezamenlijk nut te maximaliseren. De functie U_i voldoet aan enkele regulariteitseigenschappen (stijgend, tweemaal differentieerbaar, strikt concaaf). De vector $\Lambda(z)$ wordt nu gedefinieerd als de oplossing van het probleem

$$\max \sum_i z_i U_i(\Lambda_i/z_i)$$

onder de condities $\Lambda \leq C$ en $\Lambda_i/z_i \leq m_i$, $i = 1, \dots, I$.

Een belangrijke eigenschap van de functie $\Lambda(\cdot)$ is dat deze differentieerbaar is in elke richting. Dit kan worden aangetoond met behulp van algemene theorie voor continue optimaliseringsproblemen zoals is beschreven in [1], en uitgewerkt in [4].

Dit allocatiemechanisme lijkt op het eerste gezicht ver te staan van de werkelijkheid maar, indien U_i goed wordt gekozen, blijkt het toch diverse eigenschappen te hebben die de werkelijkheid goed beschrijven. Voor meer informatie en referenties verwijs ik naar [9].

We beschouwen dit model in stochastische dynamische context:

- Het aantal aankomsten van gebruikers/klanten bij route i tot en met tijdstip t is $E_i(t)$.
- De hoeveelheid werk per klant op route i is verdeeld als de stochast B_i .
- Elke klant heeft daarnaast een deadline D_i , die kan afhangen van B_i . Een klant vertrekt als zijn hoeveelheid werk is afgehandeld, of als zijn deadline is verstreken.
- We nemen aan dat klanten die continu op hun maximale snelheid bediend worden, niet ongeduldig zijn: $D_i \geq B_i/m_i$.

Om de dynamiek van dit systeem te kunnen analyseren moeten we voor elk tijdstip en elke

klant zowel de resterende hoeveelheid werk, alsmede de resterende tijd tot het verstrijken van de deadline bijhouden. Dit resulteert in een toestandsbeschrijving welke grafisch is weergegeven in Figuur 2.

Schaling en resultaten

Omdat er geen bovengrens op het aantal gebruikers in het netwerk is, is de toestand oneindig-dimensionaal, en is het soms nodig om een maatwaardig proces te analyseren. Het lijkt onmogelijk om prestatie-maten voor dit soort processen, zoals de fractie klanten die vertrekt wegens het aflopen van hun deadline, te berekenen. Om de complexiteit te reduceren kijken we daarom naar het realistische geval waarbij de C_j 's veel groter zijn dan de m_i 's, en waarbij het aantal aankomsten per route ook hoog is. Formeel vervangen we C door Cr en $E_i(t)$ door $E_i(rt)$ en laten we r willekeurig groot worden. We nemen aan dat $E_i(rt)/r \rightarrow v_i t$ en bekijken het stochastische proces $Z^{(r)}(t)$ dat voor elk tijdstip t het totale aantal klanten per route weergeeft. Het blijkt nu dat, als $r \rightarrow \infty$,

$$\frac{1}{r} Z^{(r)}(t), \quad t \geq 0 \rightarrow z(t), t \geq 0,$$

voor een proces $z(\cdot)$ welke voldoet aan de vergelijking

$$z_i(t) = v_i \int_0^t P(D_i > t - u, B_i > S_i(u, t)) du, \quad i = 1, \dots, I,$$

waarbij $S_i(u, t) = \int_u^t \Lambda_i(z(v))/z_i(v) dv$. We

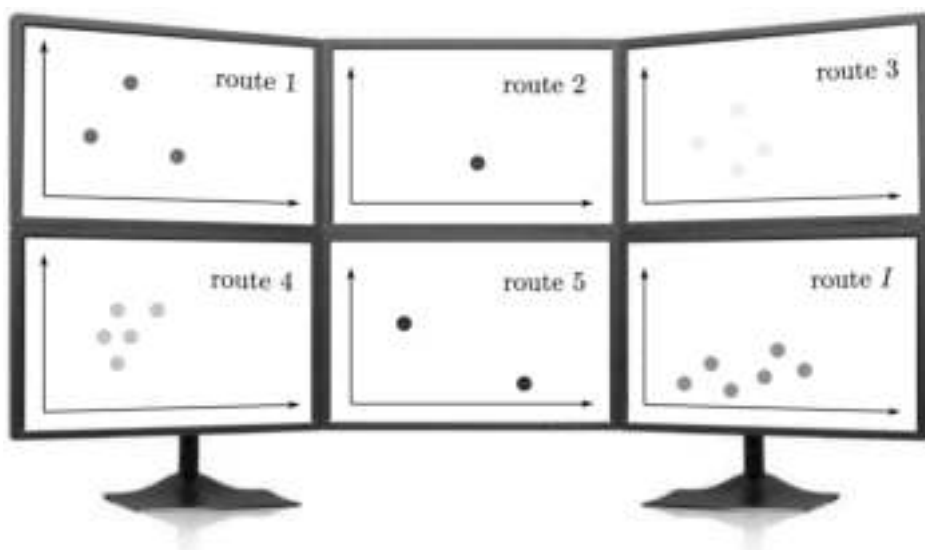
zien dat het limietproces $z(t), t \geq 0$, deterministisch is, maar volledig afhangt van de gezamenlijke verdeling van B_i en D_i . Het type vergelijking dat $z(t), t \geq 0$, karakteriseert is equivalent aan een functionaaldifferentiaal-vergelijking. De vergelijking voor $z(t)$ is intuïtief als volgt te verklaren: vloeistof van type i komt op tijdstip u het systeem binnen met intensiteit v_i . De fractie van die vloeistof die nog steeds aanwezig is op tijdstip t is $P(D_i > t - u; B_i > S_i(u, t))$, waarbij $S_i(u, t)$ de totale hoeveelheid bediening is per klant van type i in het interval $[u, t]$.

Ten slotte convergeert $z(t)$ naar een vector z^* als $t \rightarrow \infty$. Deze vector voldoet aan de vergelijking

$$z_i^* = v_i E[\min\{D_i, B_i z_i^*/\Lambda_i(z^*)\}], \quad i = 1, \dots, I.$$

Ook deze vergelijking heeft een fysische interpretatie. Volgens de wet van Little is het gemiddeld aantal klanten in een wachtrij-systeem (z_i) in evenwicht gelijk aan het gemiddeld aantal aankomsten per tijdseenheid (v_i), vermenigvuldigd met de gemiddelde verblijftijd van een klant. In ons geval is de verblijftijd het minimum van de deadline D_i en de potentiële verblijftijd. In evenwicht zal de gemiddelde bedieningssnelheid gelijk blijven; deze is gelijk aan $\Lambda_i(z)/z_i$, waarmee de potentiële verblijftijd gelijk is aan $B_i/(\Lambda_i(z)/z_i)$.

De vraag is of de vergelijking waaraan z^* voldoet een unieke oplossing heeft. Dit blijkt het geval te zijn, al duurde het even voor het bewijs gevonden was. Het is bijvoorbeeld niet eenvoudig om een argument gebaseerd op contracties te construeren. Het door ons ge-



Figuur 2 Snapshot van de gedetailleerde toestandsbeschrijving. Elk punt geeft de resterende hoeveelheid werk en de resterende tijd tot de deadline weer voor een klant, en verschuift richting het zuidwesten met snelheid $(z_i/\Lambda_i(z), 1)$.

vonden bewijs is algoritmisch en geeft ook een procedure om de vector z^* uit te rekenen. Het idee is om eerst $\Lambda^* = \Lambda(z^*)$ te karakteriseren, waarmee z^* kan worden gevonden door I eendimensionale bisecties. Definieer $g_i(x) = v_i E[\min\{xD_i, B_i\}]$ en laat G_i een functie zijn zodanig dat $G'_i(x) = U'_i(g_i^{-1}(x))$. Dan is Λ^* de unieke oplossing van het concave optimaliseringsprobleem

$$\min_{\Lambda} \sum_i G_i(\Lambda_i)$$

onder de voorwaarden $\Lambda \leq \rho$ en $A\Lambda \leq C$, met $\rho_i = v_i E[B_i]$. Dankzij de structuur van dit optimaliseringsprobleem (de functie G_i is strikt concaaf) volgt niet alleen uniciteit van z^* , maar is het ook mogelijk om Λ^* te vinden in polynomiale tijd (als functie van I en J).

Samenvattend zien we dat het macroscopisch gedrag van dit oneindig-dimensionale stochastische systeem te beschrijven valt door een functionaaldifferentiaalvergelijking, die een uniek invariant punt heeft. Dit invariante punt kan gekarakteriseerd worden door middel van de oplossing van een concaaf optimaliseringsprobleem. Cruciaal is dat de functie $\Lambda(\cdot)$ voldoet aan de nodige regulariteitseigenschappen. Deze kunnen worden

afgeleid met technieken uit de continue optimalisering.

De convergentie van $Z^{(r)}(t)/r, t \geq 0$, naar $z(t), t \geq 0$, volgt uit de meer gedetailleerde maatwaardige beschrijving van het systeem, gebaseerd op Figuur 2. Om relatieve compactheid van het rijtje processen $Z^{(r)}(\cdot)/r$ vast te stellen is het belangrijk aan te tonen dat het aantal punten in L-vormige verzamelingen in Figuur 2 afgeschat kan worden in termen van de dikte van L . Hierdoor is het dan niet mogelijk dat veel klanten vertrekken in een kort tijdsbestek, waarmee het systeem ook geen oscillaties kan vertonen. Dit impliceert dan uiteindelijk de gewenste compactheidseigenschap. De benodigde afschattingen volgen onder meer uit de theorie van empirische processen, welke terug te vinden is in [7].

Excursies

Bovengenoemde studie is illustratief voor mijn Vidi-onderzoeksproject. Een ander resultaat waar ik trots op ben is verkregen in samenwerking met Amaury Lambert en mijn voormalige postdoc Florian Simatos. We hebben een nieuwe methode ontwikkeld voor het afleiden van convergentie van stochastische processen, gebruikmakend van excursietheorie. Het idee is dat wachtrijen vaak relatief eenvoudig te beschrij-

ven zijn zolang het systeem niet leeg raakt. De zogenaamde bezige perioden zijn voorbeelden van wat in de kansrekening excursies worden genoemd. Om nu aan te tonen dat een rijtje stochastische processen $Z^{(r)}$ convergeert naar een stochastisch proces Z blijkt het voldoende te zijn dat (i) het rijtje $(Z^{(r)})$ relatief compact is; (ii) de excursies van $Z^{(r)}$ zwak convergeren naar de excursies van Z , en (iii) Z gekarakteriseerd wordt door zijn excursies. Voor meer details verwijs ik naar [3]. Dit resultaat is krachtig genoeg om één van de moeilijkste problemen in mijn Vidi-voorstel op te lossen, een probleem dat ik tijdens het schrijven van het voorstel nogal speculatief vond en ik ergens helemaal op het eind noemde. Ik prijs me gelukkig met het gegeven dat Simatos een uitstekende postdoc was die bereid was om het risico te nemen aan dit probleem te werken.

Tot slot

Terugziend heeft de Vidi-beurs me in staat gesteld enkele talentvolle jonge onderzoekers aan te stellen, en me te richten op uitdagende open problemen in mijn vakgebied. Hierbij kon ik ook de tijd nemen om me te verdiepen in onderwerpen uit aangrenzende vakgebieden. Ik ben NWO daar zeer dankbaar voor. 

Referenties

- 1 J. Bonnans en A. Shapiro, *Perturbation Analysis of Optimization Problems*, Springer, 2001.
- 2 H. Chen en D. Yao, *Stochastic Networks: Performance, Asymptotics & Optimization*, Springer, 2003.
- 3 A. Lambert, F. Simatos en B. Zwart, Scaling limits via excursion theory: Interplay between Crump–Mode–Jagers branching processes and Processor-Sharing queues, *Annals of Applied Probability* 23 (2013), 2357–2381.
- 4 J. Reed en B. Zwart, Fluid and diffusion approximations for Markovian bandwidth sharing networks with rate constraints, te verschijnen in *Operations Research* (2014).
- 5 M. Remerova, *Fluid Limit Approximations of Stochastic Networks*, proefschrift, VU, Amsterdam, 2014.
- 6 M. Remerova, J. Reed en B. Zwart, Fluid limits for bandwidth-sharing networks with impatience, te verschijnen in *Mathematics of Operations Research* (2014).
- 7 A. van der Vaart en J. Wellner, *Weak Convergence and Empirical Processes*, Springer, 1996.
- 8 W. Whitt, *Stochastic Process Limits*, Springer, 2002.
- 9 Y. Yi en M. Chiang, Stochastic network utility maximization – A tribute to Kelly’s paper published in this journal a decade ago, *European Transactions on Telecommunications* 19 (2008), 421–442.

Jan van Neerven

Faculteit EWI/DIAM

TU Delft

j.m.a.m.vanneerven@tudelft.nl

Onderzoek Vidi- en Vici-project

Stochastische integratie in Banachruimten

Jan van Neerven ontving in 2002 een Vidi-subsidie voor het project 'Stochastic Integration in Banach Spaces and Applications to Stochastic Evolutions' en in 2007 een Vici-subsidie voor het project 'Infinite-Dimensional Stochastic Analysis and Harmonic Analysis'. In dit artikel blikt hij terug op twaalf jaar Vernieuwingsimpuls.

Al weer een jaar of twaalf geleden zat ik eens te puzzelen aan een probleem toen er aan mijn deur werd geklopt: een onverwacht bezoekje van de toenmalige decaan. Ik was net UHD geworden en de decaan zag daar in een goede aanleiding om een aanvraag in te dienen voor een Vidi-subsidie. Onderzoeksgeld aanvragen was iets dat ik nog associeerde met het postdoc-bestaan dat ik juist achter mij had gelaten, en ik had mij nog niet georiënteerd op de Vernieuwingsimpuls die toen net van start was gegaan. Nu was ik net samenwerking met Lutz Weis uit Karlsruhe aangegaan om een theorie van stochastische integratie in Banachruimten te ontwikkelen. Zoiets heb je nodig om stochastische partiële differentiaalvergelijkingen op functionaalanalytische wijze te behandelen, met name als je daarvoor L^p -theorie wilt ontwikkelen (daarover zo dadelijk meer). Zo'n theorie was er nog niet, en sterker nog, veel collega's in het vakgebied dachten dat zoiets helemaal niet kon. Een uitdagend en risicodragend project dus, dat goed leek te passen in de strategie van de Vernieuwingsimpuls.

De referentenrapporten waren prima en ik werd uitgenodigd voor een interview. De begeleiding van projectaanvragen indienen was in die tijd nog niet zo geprofessionaliseerd, dus oefende ik mijn presentatie nogal informeel in het bijzijn van de decaan en een hoogleraar. Wat ik mij vooral herinner is de tip om een overheadsheet (het presenteren met beamers was nog niet de standaard) toe te voe-

gen over 'positionering', iets waar ik nog nooit over had nagedacht.

Als wiskundige verwacht je in een interview met een panel dat deels bestaat uit niet-wiskundigen veel vragen over mogelijke toepassingen van het voorgestelde onderzoek. Maar dit onderwerp kwam nauwelijks ter sprake. De meest onverwachte vraag kwam van een van de niet-wiskundige panelleden die met een brede grijns te kennen gaf het voorstel weliswaar 'erg geleerd' te vinden, maar of ik hem ook kon uitleggen wat een stochastische integraal nou eigenlijk is? Ik kan mij niet meer precies herinneren wat ik toen gezegd heb, maar kennelijk was de commissie tevreden want niet lang daarna ontving ik het heugelijke nieuws dat de aanvraag was goedgekeurd.

Stochastische integratie: het discrete geval

Nu zou ik de bovengenoemde vraag beantwoorden met de socratische constatering dat iedereen, misschien zonder het te weten, weet wat stochastische integratie is. Stel we zetten 10 euro in op de uitkomst $r_1 = \pm 1$ van een worp met een eerlijke munt (de 'r' staat voor 'Rademacher variabele'). De winst is de inzet $\times$ de uitkomst van de worp en bedraagt $10r_1$; in geval $r_1 = -1$ is de 'winst' negatief. Voorafgaand aan de volgende worp, die het toevalsgetal $r_2 = \pm 1$ oplevert, zetten we opnieuw een bedrag in, zeg 20 euro, en de winst bedraagt dit keer $20r_2$. Zo gaan we verder.

We kunnen dit als volgt formaliseren. Na de worpen $r_1, \dots, r_{n-1}$ bepalen we de inzet

f_{n-1} voor de n de worp. Na N worpen bedraagt de cumulatieve winst

$$\sum_{n=1}^N f_{n-1} r_n.$$

Belangrijk is dat de worpen onafhankelijk zijn en dat we niet in de toekomst kunnen kijken, wat er wiskundig op neerkomt dat de inzet f_{n-1} alleen mag afhangen van de uitkomsten $r_1, \dots, r_{n-1}$, maar niet van $r_n, \dots, r_N$ (we kunnen bijvoorbeeld de inzet verdubbelen na ieder verliespotje en stoppen na de eerste keer winst).

Het herhaald werpen van een eerlijke munt kunnen we beschrijven als een random walk. Zetten we

$$w_n := \sum_{j=1}^n r_j,$$

dan is het increment $w_n - w_{n-1} = r_n$ precies de uitkomst van de n de worp en kunnen we de cumulatieve winst $\sum_{n=1}^N f_{n-1} r_n$ schrijven als een 'random Stieltjes-integraal' over de indexverzameling $I = \{1, \dots, N\}$:

$$\int_I f dw = \sum_{n \in I} f_{n-1} (w_n - w_{n-1}).$$

Ziehier de eerste stochastische integraal!

Stochastische integratie: het continue geval

Vervangen we de (discrete) random walk w door een (continue) Brownse beweging W , dan kunnen we voor een interval I de stochastische integraal

$$\int_I f dW$$

interpreteren als de cumulatieve winst bij het

in real-time gokken op het verloop van de Brownse beweging. De functie f beschrijft de inzet als functie van de tijd; we maken winst als de Brownse beweging “dezelfde kant op gaat” als het voorteken van de inzet. Kansrenkeners zullen hier protesteren, want Brownse bewegingen zijn zo grillig dat ze met kans 1 nooit even één kant opgaan; maar dat terzijde.

Het voorgaande kan als volgt worden geformaliseerd. We beschouwen een Brownse beweging, die we beschrijven als een meetbare functie $W : \mathbb{R}_+ \times \Omega \rightarrow \mathbb{R}$; hierbij is Ω de onderliggende kansruimte, voorzien van een kansmaat die we met $\mathbb{P}$ zullen aanduiden. Onder een *random stapfunctie* verstaan we een functie f op $\mathbb{R}_+ \times \Omega$ van de vorm

$$f(t, \omega) = \sum_{n=1}^N 1_{(t_{n-1}, t_n]}(t) g_{n-1}(\omega),$$

waarbij alle g_{n-1} simpele functies zijn op Ω . Voor zulke f definiëren we

$$\int_0^\infty f \, dW := \sum_{n=1}^N g_{n-1}(W(t_{n-1}) - W(t_n)).$$

Beide zijden geven een reëelwaardige toevalsvariable gedefinieerd op Ω ; aan de rechterzijde gebruiken we de notatie $W(t) : \omega \mapsto W(t, \omega)$. We hebben nog niet uitgesloten dat we op geen enkel moment informatie uit de toekomst tot onze beschikking krijgen; deze impliciete veronderstelling omzetten, kunnen we vertalen naar de wiskundige aanname dat voor iedere $r \in \mathbb{R}_+$ de toevalsvariable $f(t) : \omega \mapsto f(t, \omega)$ meetbaar is in de σ -algebra $\mathcal{F}_t$ gegenereerd door een Brownse beweging tot aan tijdstip t . We noemen het inzetproces f dan *aangepast* aan de Brownse beweging W .

Nu geldt de volgende fundamentele stelling van Itô uit de jaren veertig van de vorige eeuw, die het startpunt vormde van de theorie van stochastische differentiaalvergelijkingen:

Stelling 1 (Itô's isometrie). *Zij $f : \mathbb{R}_+ \times \Omega \rightarrow \mathbb{R}$ een aangepaste random stapfunctie. Dan geldt*

$$\int_\Omega \left| \int_0^\infty f \, dW \right|^2 d\mathbb{P} = \int_\Omega \int_0^\infty |f(t)|^2 dt d\mathbb{P}.$$

Dankzij deze isometrie kunnen we de stochastische integraal uitbreiden naar willekeurige aangepaste kwadratisch integreerbare processen $f : \mathbb{R}_+ \times \Omega \rightarrow \mathbb{R}$ middels approxi-

matie (dat de hierboven beschouwde klasse van random stapfuncties dicht ligt in de L^2 -norm moet natuurlijk netjes bewezen worden, maar dat is niet zo moeilijk) en de Itô-isometrie geldt ook voor deze grotere klasse van processen. Voorts kunnen we, voor een deelinterval I van $\mathbb{R}_+$, definiëren

$$\int_I f \, dW := \int_0^\infty 1_I f \, dW.$$

De bovenstaande procedure is analoog aan de constructie van de Fourier–Plancherel-transformatie in $L^2(\mathbb{R})$: daar bewijst men de Plancherel-isometrie

$$\begin{aligned} \int_{-\infty}^\infty \left| \int_{-\infty}^\infty e^{-2\pi i x y} f(y) dy \right|^2 dx \\ = \int_{-\infty}^\infty |f(x)|^2 dx \end{aligned} \quad (1)$$

eerst voor de Fourier-transformatie van functies in $f \in L^1(\mathbb{R}) \cap L^2(\mathbb{R})$ en gebruikt deze isometrie vervolgens om de Fourier-transformatie uit te breiden naar een isometrie voor willekeurige $f \in L^2(\mathbb{R})$.

Stochastische integratie in Banachruimten I

Vanaf nu zullen we integralen $\int_\Omega \xi \, d\mathbb{P}$ afkorten tot $\mathbb{E} \xi$ en interpreteren als de verwachtingswaarde (‘expectatie’) van ξ . Met deze notatie neemt Itô's isometrie de vorm

$$\mathbb{E} \left| \int_0^\infty f \, dW \right|^2 = \mathbb{E} \int_0^\infty |f(t)|^2 dt$$

aan. De vraag die we willen beschouwen is of (een versie van) de Itô-isometrie geldig is voor aangepaste processen $f : \mathbb{R}_+ \times \Omega \rightarrow X$, waarbij X een Banachruimte is. Voordat we ons hierop werpen, laten we ons eerst inspireren door de Fourier–Plancherel-isometrie. Geldt die ook voor functies $f \in L^2(\mathbb{R}; X)$, dat wil zeggen functies $f : \mathbb{R} \rightarrow X$ waarvoor $\int_{-\infty}^\infty \|f(t)\|_X^2 dt < \infty$?

Voor Hilbertruimten X is het antwoord bevestigend; de enige verandering is dat het product $x y$ in (1) nu geïnterpreteerd dient te worden als het inwendig product $\langle x, y \rangle$ in X en absolute waarden vervangen dienen te worden door normen in X . Met deze aanpassingen werkt het bewijs *mutatis mutandis*.

Veel dieper ligt de volgende stelling van Kwapien, die zegt dat als de Fourier–Plancherel-transformatie uitbreidt naar een begrensde lineaire transformatie op $L^2(\mathbb{R}; X)$, dan is X isomorf met een Hilbertruimte. Met andere woorden: zelfs als we ‘isometrisch’ af-

zwakken tot ‘begrensd’ is er alleen een vectorwaardige uitbreiding naar Hilbertruimten X !

Met deze waarschuwing in gedachten kijken we nu naar vectorwaardige uitbreidingen van de Itô-isometrie. Ook deze breidt *mutatis mutandis* uit naar Hilbert-waardige processen. Karakteriseert dit feit wederom Hilbertruimten te midden van alle Banachruimten? Het antwoord is ‘ja’ en ‘nee’. Als we alleen een begrensde uitbreiding wensen, dan is het antwoord ‘nee’; als we een isometrische uitbreiding wensen is het antwoord ‘ja’. Dit is interessant genoeg om even langer bij stil te staan.

Als we het bewijs van de Itô-isometrie analyseren (wat we hier niet zullen doen), blijkt dat het met enige handigheid (zie [9]) herleid kan worden op de ‘isometrie’

$$\mathbb{E} \left\| \sum_{n=1}^N d_n \right\|^2 = \mathbb{E} \sum_{n=1}^N |d_n|^2 \quad (2)$$

voor zekere reëelwaardige toevalsvariabelen d_n die een zogenaamde martingaaldifferentierij blijken te vormen. Voor het opzetten van een stochastische integraal via approximatie met random stapfuncties volstaat een ongelijkheid in (2) in plaats van gelijkheid. Dit motiveert de volgende definitie. Een Banachruimte X heeft *martingaal-type 2* als er een constante C bestaat zodanig dat

$$\mathbb{E} \left\| \sum_{n=1}^N d_n \right\|_X^2 \leq C^2 \mathbb{E} \sum_{n=1}^N \|d_n\|_X^2$$

voor iedere eindige martingaaldifferentierij $(d_n)_{n=1}^N$ met waarden in X .



Kiyoshi Itô

We kunnen het bewijs van Stelling 1 nu overdoen voor aangepaste random stapfuncties f met waarden in X . Het resultaat is de volgende Itô-ongelijkheid voor Banachruimten X met martingaal-type 2:

$$\mathbb{E} \left\| \int_0^\infty f \, dW \right\|_X^2 \leq C^2 \mathbb{E} \int_0^\infty \|f(t)\|_X^2 \, dt. \quad (3)$$

Het is een ‘back of the envelope’-oefening om na te gaan dat Hilbertruimten martingaal-type 2 hebben (met constante $C = 1$). Maar Hilbertruimten zijn geenszins het enige voorbeeld: de Lebesgue-ruimten $L^p(M, \mu)$, met (M, μ) een willekeurige maatruimte, hebben martingaal-type 2 voor iedere $p \in [2, \infty)$. In het bijzonder geldt de Itô-ongelijkheid (3) in $L^p(M, \mu)$ en kunnen we stochastische analyse bedrijven in deze ruimten. Deze observatie gaat terug op het werk van Hoffmann-Jørgensen en Pisier, Dettweiler en Neidhardt uit de jaren tachtig en is voor het eerst toegepast op stochastische PDV's door Belop'skaya, Daletskiï en Brzeźniak.

Goldt ook een omgekeerde ongelijkheid in (3), dat wil zeggen is de Itô-ongelijkheid in feite een Itô-isomorfisme? Het blijkt dat de omgekeerde ongelijkheid

$$\mathbb{E} \int_0^\infty \|f(t)\|_X^2 \, dt \leq C^2 \mathbb{E} \left\| \int_0^\infty f \, dW \right\|_X^2 \quad (4)$$

geldt onder de ‘duale’ eigenschap *martingaal-cotype 2*. Voorbeelden van zulke ruimten zijn Hilbertruimten en de Lebesgue-ruimten $L^p(M, \mu)$ met $p \in [1, 2]$.

Met behulp van een diepe stelling uit de Banachruimtetheorie, wederom van Kwapien, kan men nu bewijzen dat een Banachruimte X waarvoor (3) en (4) gelden isomorf is met een Hilbertruimte. Met andere woorden, de geldigheid van een Itô-isomorfisme

$$\mathbb{E} \left\| \int_0^\infty f \, dW \right\|_X^2 \approx \mathbb{E} \int_0^\infty \|f(t)\|_X^2 \, dt$$

karacteriseert Hilbertruimten (met $\approx$ bedoelen we dat ongelijkheid in beide richtingen geldt met constanten onafhankelijk van f).

Slecht nieuws

Laten we even samenvatten wat we tot dusverre hebben gevonden. In Banachruimten X met martingaal-type 2 kunnen we ieder aangepast stochastisch proces $f \in L^2(\mathbb{R}_+ \times \Omega; X)$ stochastisch integreren tegen een Brownse beweging en de ongelijkheid (3) geldt. Anders gezegd, de stochastische integraal $f \mapsto \int_0^\infty f \, dW$ is begrensd van $L^2_a(\mathbb{R}_+ \times \Omega; X)$ naar

$L^2(\Omega; X)$ (de ‘a’ staat voor de gesloten deelruimte van alle aangepaste processen). Via restrictie zien we dat, meer algemeen, voor ieder deelinterval I van $\mathbb{R}_+$ de afbeelding $f \mapsto \int_I f \, dW$ begrensd is van $L^2_a(I \times \Omega; X)$ naar $L^2(\Omega; X)$. We hebben eveneens gezien dat de ruimten $X = L^p(M, \mu)$ met $p \in [2, \infty)$ martingaal-type 2 hebben.

Hoe zit het met exponenten $p \in [1, 2)$? Het blijkt dat voor $X = \ell^p$ ($= L^p(\mathbb{N}, \tau)$ met τ de telmaat op $\mathbb{N}$) met $p \in [1, 2)$ de afbeelding $f \mapsto \int_0^1 f \, dW$, die dankzij de Itô-isometrie goed gedefinieerd is als lineaire afbeelding van $C[0, 1] \otimes \ell^p$ naar $L^2(\Omega; \ell^p)$, geen uitbreiding heeft tot een begrensde lineaire afbeelding van $C([0, 1]; \ell^p)$ naar $L^2(\Omega; \ell^p)$. Hier is $C[0, 1] \otimes \ell^p$ het algebraïsch tensorproduct van $C[0, 1]$ en ℓ^p , dat willen zeggen de vectorruimte opgespannen door alle functies van de vorm $t \mapsto g(t)x$ met $g \in C[0, 1]$ en $x \in \ell^p$. Met andere woorden:

Yors observatie. Voor $p \in [1, 2)$ bestaan er continue functies $f : [0, 1] \rightarrow \ell^p$ die niet stochastisch integreerbaar zijn tegen een Brownse beweging.

Deze observatie van Yor [15] lijkt de doodsteek voor iedere poging tot stochastische integratie in algemene Banachruimten.

Laten we Yors observatie eens nader bekijken. We beschouwen in ℓ^p de standaardbasis $(e_n)_{n=1}^\infty$:

$$e_n = (0, 0, \dots, 0, \underbrace{1}_{\text{(plaats } n)}, 0, 0, \dots).$$

We equipartitioneren $[0, 1]$ in N deeltintervallen $I_n = (t_{n-1}, t_n]$ van lengte $1/N$ en merken op dat de geschaalde incrementen

$$y_n := \sqrt{N}(W(t_n) - W(t_{n-1}))$$

standaard normaal verdeeld en onafhankelijk zijn; dit volgt uit de definiërende eigenschappen van een Brownse beweging. We zetten nu

$$f_N := \sum_{n=1}^N 1_{(t_{n-1}, t_n]} \otimes e_n$$

en vinden

$$\begin{aligned} \mathbb{E} \left\| \int_0^1 f_N \, dW \right\|_{\ell^p}^p &= \mathbb{E} \left\| \frac{1}{\sqrt{N}} \sum_{n=1}^N y_n e_n \right\|_{\ell^p}^p \\ &= \frac{1}{N^{p/2}} \sum_{n=1}^N \mathbb{E} |y_n|^p \\ &= m_p N^{1-p/2} \end{aligned}$$



Marc Yor

met

$$\begin{aligned} m_p &:= \mathbb{E} |y_n|^p = \frac{1}{\sqrt{2\pi}} \int_{-\infty}^{\infty} |x|^p e^{-x^2/2} \, dx \\ &= \frac{2^{p/2}}{\sqrt{\pi}} \Gamma((p+1)/2). \end{aligned}$$

Hier is $\Gamma(x) = \int_0^\infty t^{x-1} e^{-t} \, dt$ de Euler-gammafunctie. Wegens $p \in [1, 2)$ geldt $\lim_{N \rightarrow \infty} N^{1-p/2} = \infty$, terwijl de integranden evident voldoen aan

$$\sup_{N \geq 1} \left(\sup_{t \in \mathbb{R}_+} \|f_N(t)\|_{\ell^p} \right) = 1.$$

We zijn er bijna, ware het niet dat we de L^p -norm van de stochastische integralen hebben berekend in plaats van hun L^2 -norm en dat we stapfuncties gebruikt hebben in plaats van continue functies.

Om het eerste defect weg te werken, gebruiken we een belangrijke stelling van Kahane, die een Banach-waardige uitbreiding is van een klassiek resultaat van Khintchine. Deze stelling zegt dat voor iedere $p \in [1, \infty)$ een constante $1 \leq K_p < \infty$ bestaat met de volgende eigenschap: voor iedere Banachruimte X en iedere Gaussische toevalsvariabele $\xi : \Omega \rightarrow X$ (dat wil zeggen $x^* \circ \xi : \Omega \rightarrow \mathbb{R}$ is Gaussisch verdeeld voor iedere begrensde lineaire functionaal x^* in X^* , de duale ruimte van X), geldt

$$\begin{aligned} \frac{1}{K_p} (\mathbb{E} \|\xi\|_X^2)^{1/2} &\leq (\mathbb{E} \|\xi\|_X^p)^{1/p} \\ &\leq K_p (\mathbb{E} \|\xi\|_X^2)^{1/2}. \end{aligned}$$

Merk op dat één van beide ongelijkheden volgt uit Hölders ongelijkheid (met constante 1); wat Kahanes stelling zegt is dat we de omgekeerde ongelijkheid er gratis bij krijgen voor Gaussisch verdeelde ξ , met een universele constante die enkel van p afhangt.

Combineren we Kahanes stelling met het eerder bewezen, dan zien we dat ook de L^2 -normen van de stochastische integralen van

de functies f_N divergeren voor $N \rightarrow \infty$. Tot slot kunnen we de indicatorfuncties in de definitie van f_N vervangen door continue benaderingen zonder de normen van de stochastische integralen noemenswaardig te veranderen. Daarmee is Yors resultaat bewezen.

PDV's en SPDV's

We hebben nog niets gezegd over de beweegredenen om stochastisch te willen integreren in Banachruimten. Die komen uit de hoek van de stochastische partiële differentiaalvergelijkingen. Om dit uit te leggen bekijken we eerst een klasse van deterministische partiële differentiaalvergelijkingen van de vorm

$$\frac{\partial u}{\partial t}(t, \xi) = \Delta u(t, \xi) + f(t, u(t, \xi)) \quad (5)$$

op een open deelverzameling D van $\mathbb{R}^d$, voorzien van beginvoorwaarden en randvoorwaarden. Functionaalanalytisch kan men deze vergelijking in de abstracte vorm

$$u'(t) = Au(t) + f(t, u(t)) \quad (6)$$

brengen. Deze vergelijking beschouwt men in een Banachruimte X van functies op D , bijvoorbeeld $X = L^p(D)$. De operator A is dan de Laplace-operator Δ ; de randvoorwaarden op D zijn verwerkt in de keuze van het domein van definitie van A . Verder schrijven we, voor $x \in L^p(D)$ en $\xi \in D$, $(f(t, x))(\xi) := f(t, x(\xi))$. Een *milde oplossing* wordt gedefinieerd als een functie $u : \mathbb{R}_+ \rightarrow L^p(D)$ die voldoet aan de vergelijking

$$u(t) = e^{tA}u(0) + \int_0^t e^{(t-s)A}f(s, u(s))ds. \quad (7)$$

Hier is $(e^{tA})_{t \geq 0}$ de warmtehalfgroep voortgebracht door A . De idee achter deze definitie is dat formele differentiatie van (6) (onder gebruikmaking van $(e^{tA})' = Ae^{tA}$) de oorspronkelijke vergelijking (6) teruggeeft, maar in tegenstelling tot (6) wordt in (6) geen *a priori* differentieerbaarheid van u verlangd. Het mag duidelijk zijn dat we hier nogal wat details onder het tapijt schuiven, maar alles kan helemaal precies worden gemaakt.

Laten we nu eens het volgende stochastische analogon van (5) beschouwen:

$$\frac{\partial u}{\partial t}(t, \xi) = \Delta u(t, \xi) + g(t, u(t, \xi))W'(t), \quad (8)$$

met W een Brownse beweging. Deze vergelij-

king kunnen we abstract schrijven als

$$du(t) = Au(t)dt + g(t, u(t))dW(t). \quad (9)$$

De heuristiek is dat op het interval $[t, t + \Delta t]$ het $(L^p(D)$ -waardige) increment van u bij benadering gegeven wordt door

$$\Delta u(t) \approx Au(t)\Delta t + g(t, u(t))\Delta W(t).$$

Met andere woorden, bovenop het lineaire deel van de vergelijking wordt op infinitesimale tijdschaal met een 'Gaussische dobbelsteen' geworpen die de oplossing op toevallige wijze beïnvloedt. Deze interpretatie verklaart waarom we in (8) de 'ruis' met de tijdsafgeleide van een Brownse beweging modelleren. Er is echter een klein probleem: met kans 1 zijn de paden van een Brownse beweging nergens differentieerbaar.

Naar analogie van (7) zou men een *milde oplossing* nu willen definiëren als een $L^p(D)$ -waardig proces u dat voldoet aan

$$u(t) = e^{tA}u(0) + \int_0^t e^{(t-s)A}f(s, u(s))dW(s). \quad (10)$$

Om een en ander precies te maken zijn we genooddzaak de integraal aan de rechterzijde te interpreteren als een stochastische integraal in de Banachruimte $X = L^p(D)$. Niet alleen hebben we in deze milde formulering geen *a priori* differentieerbaarheid van u nodig, we omzeilen tegelijkertijd het probleem van de nergens-differentieerbaarheid van W .

De reden dat we niet tevreden zijn met stochastische integratie in de Hilbertruimte $L^2(D)$ is tweeledig:

- (a) voor veel (S)PDV's is $L^2(D)$ niet de 'natuurlijke' toestandsruimte;
- (b) door te werken in $L^p(D)$ verkrijgt men betere regulariteitseigenschappen voor de oplossing.

Wat betreft punt (a) kunnen we bijvoorbeeld opmerken dat de warmtevergelijking in $L^1(D)$ een natuurlijke interpretatie heeft: de L^1 -norm geeft de totale warmte-inhoud. Wat betreft punt (b) is het in de meeste gevallen zo dat betere regulariteit wordt verkregen naar mate p groter gekozen wordt (de achterliggende reden is dat Sobolev-inbeddingen een betere Hölder-exponent opleveren voor grote p).

Stochastische integratie in Banachruimten II

Wat betreft punt (b) hebben we goed nieuws, want de ruimten $L^p(D)$ hebben martingaal-

type 2 voor grote waarden van p . Dit betekent dat we de vergelijking (9) kunnen bestuderen met de hierboven beschreven theorie van stochastische integratie in martingaal-type 2 ruimten. Maar we hebben ook gezien dat die theorie ruimten zoals $L^1(D)$ uitsluit, en dit is onbevredigend wat betreft punt (a): 'in het echt' evolueren warmteprofielen immers ook in de aanwezigheid van ruis, daarbij niet gehinderd door enige mathematische tegenwerkingen vanuit de universiteiten.

Een tweede tegenwerping tegen de martingaal-type 2-theorie is subtieler. We hebben gezien dat in de aanwezigheid van martingaal-type 2 de Itô-isometrie een Itô-ongelijkheid wordt. Is deze scherp, of verliezen we belangrijke informatie?

Om hier antwoord op te krijgen kunnen we kijken naar de kritieke Sobolev-exponent van de regulariteit van de oplossingen. Hieraan is in de afgelopen een à twee decennia intensief onderzoek verricht. Daar is uitgekomen dat een ruime klasse van vergelijkingen van het type (6) oplossingen in $L^p(D)$ hebben met Sobolev-regulariteit bij de kritieke exponent (we spreken dan van *maximale regulariteit*). Pogingen om eenzelfde resultaat te bewijzen voor de stochastische vergelijkingen (9) in ruimten met martingaal-type 2 hebben daarentegen nooit iets opgeleverd: met behulp van deze theorie krijgt men alleen Sobolev-regulariteit voor exponenten strikt kleiner dan de kritieke exponent.

Dit was ongeveer de situatie toen ik het Vidi-project indiende. Belangrijke vragen die open lagen waren:

- (i) Is het mogelijk een bevredigende theorie van stochastische integratie op te zetten voor een grotere klasse van Banachruimten dan alleen de martingaal-type 2-ruimten?
- (ii) Is het mogelijk een Itô-isomorfisme voor de stochastische integraal te bewijzen?
- en zo ja, in het verlengde daarvan:
- (iii) Is het mogelijk stochastische maximale regulariteit te bewijzen voor een interessante klasse stochastische vergelijkingen?

Uit Yors resultaat valt af te leiden dat we op (i) en (ii) alleen een positief antwoord kunnen hebben als we bereid zijn $L^2_{\mathbb{A}}(\mathbb{R}_+ \times \Omega; X)$ op te offeren als de 'correcte' ruimte waarop stochastische integratie gedefinieerd kan worden.

Om een idee te krijgen wat dan wel de correcte ruimte is, gaan we terug naar het begin en beschouwen de allereenvoudigste situatie van een deterministische X -waardige stapfunctie als integrand. Zo'n functie kunnen we

schrijven als

$$f = \sum_{n=1}^N \frac{1(t_{n-1}, t_n]}{\sqrt{t_n - t_{n-1}}} \otimes x_n \quad (11)$$

met $x_n \in X$ voor $n = 1, \dots, N$. De normalisering is zo gekozen dat de toevalsvariabelen

$$y_n := \frac{W(t_{n-1}) - W(t_n)}{\sqrt{t_n - t_{n-1}}}$$

standaard normaal verdeeld zijn. Ze zijn tevens onafhankelijk, en met bovenstaande notatie krijgen we

$$\int_0^\infty f \, dW = \sum_{n=1}^N y_n x_n. \quad (12)$$

Nu kunnen we f algebraïsch opvatten als een element in $L^2(\mathbb{R}_+) \otimes X$, en de vraag hoe we de L^2 -norm van de stochastische integraal kunnen afschatten kunnen we herformuleren als een vraag over het afschatten van Banachwaardige Gaussische sommen. Nu komt de cruciale observatie: als H een Hilbertruimte is, dan definieert op $H \otimes X$,

$$\left\| \sum_{n=1}^N h_n \otimes x_n \right\|_{H \otimes X}^2 := \mathbb{E} \left\| \sum_{n=1}^N y_n x_n \right\|_X^2 \quad (13)$$

een norm mits we $h_1, \dots, h_N$ orthonormaal in H kiezen. Dit laatste kan altijd via een Gram-Schmidt-argument worden bereikt. Merk ook op dat de functies $h_n := 1(t_{n-1}, t_n]/\sqrt{t_n - t_{n-1}}$ in (11) inderdaad orthonormaal zijn in de Hilbertruimte $H = L^2(\mathbb{R}_+)$.

Het bewijs dat de norm (13) welgedefinieerd is, berust op het feit dat het beeld van een standaard normaal verdeelde toevalsvariabele met waarden in $\mathbb{R}^N$ (hier nemen we $(y_n)_{n=1}^N$) onder een orthogonale transformatie op $\mathbb{R}^N$ wederom standaard normaal verdeeld is. Onder de norm (13) is de afbeelding $f \mapsto \int_0^\infty f \, dW$ isometrisch:

$$\begin{aligned} \mathbb{E} \left\| \int_0^\infty f \, dW \right\|^2 &= \mathbb{E} \left\| \sum_{n=1}^N y_n x_n \right\|_X^2 \\ &= \left\| \sum_{n=1}^N h_n \otimes x_n \right\|_{L^2(\mathbb{R}_+) \otimes X}^2 \\ &= \|f\|_{L^2(\mathbb{R}_+) \otimes X}^2. \end{aligned}$$

De completering van $H \otimes X$ met betrekking tot de norm in (13) noteren we als $\gamma(H, X)$. Voor $H = L^2(\mathbb{R}_+)$ kunnen we de elementen

van deze ruimte opvatten als ‘gegeneraliseerde’ X -waardige functies in een Gaussische zin van het woord. Maar er is een alternatieve manier om de elementen van $\gamma(H, X)$ te beschrijven die werkt voor algemene Hilbertruimten H . Hiertoe merken we op dat het algebraïsch tensorproduct $H \otimes X$ op natuurlijke wijze geïdentificeerd kan worden met de vectorruimte van alle eindigerangoperatoren van H naar X : de tensor $h \otimes x$ identificeren we daartoe met de rang 1-operator

$$h' \mapsto \langle h, h' \rangle x.$$

Nu is het niet lastig om in te zien dat de identiteitsafbeelding op $H \otimes X$ een continue voortzetting heeft tot een begrensde injectieve afbeelding

$$\gamma(H, X) \subseteq \mathcal{L}(H, X),$$

waarbij $\mathcal{L}(H, X)$ de ruimte van alle begrensde lineaire operatoren van H naar X voorstelt. De elementen in $\gamma(H, X)$ kunnen dus ‘een-op-een’ worden geïdentificeerd met zekere begrensde operatoren van H naar X . In het speciale geval $H = L^2(\mathbb{R}_+)$ neemt deze identificatie de volgende vorm aan: een functie $f \in L^2(\mathbb{R}_+) \otimes X$ correspondeert met de integraaloperator van $L^2(\mathbb{R}_+)$ naar X gegeven door

$$g \mapsto \int_0^\infty f(t)g(t) \, dt.$$

Terugkerend naar de stochastische integraal hebben we bewezen:

Stelling 2 (Itô-isometrie voor deterministische integranden in X). *Voor alle stapfuncties $f : \mathbb{R}_+ \rightarrow X$ geldt*

$$\mathbb{E} \left\| \int_0^\infty f \, dW \right\|_X^2 = \|f\|_{\gamma(L^2(\mathbb{R}_+), X)}^2.$$

Eigenlijk hebben we helemaal niets bewezen, want de isometrie geldt per definitie van de $\gamma(L^2(\mathbb{R}_+), X)$ -norm. Toch is er meer aan de hand. Ten eerste kunnen we de $\gamma(H, X)$ -norm voor een aantal belangrijke ruimten expliciet uitrekenen.

Voorbeeld 1. Zij X een Hilbertruimte. Dan geldt

$$\gamma(H, X) = \mathcal{C}^2(H, X)$$

met gelijke normen. Hier is $\mathcal{C}^2(H, X)$ de ruimte van alle Hilbert-Schmidt-operatoren van H

naar X . Dit volgt vrijwel direct uit de definitie van een Hilbert-Schmidt-operator.

Voorbeeld 2. Zij $X = L^p(M, \mu)$ met $1 \leq p < \infty$. Dan geldt

$$\gamma(H, L^p(M, \mu)) = L^p(M, \mu; H)$$

met equivalente normen. De identificatie geschiedt door tensor $h \otimes f$ enerzijds op te vatten als functies $\xi \mapsto f(\xi)h$ en anderzijds als operatoren $h' \mapsto \langle h, h' \rangle f$. Het bewijs is een eenvoudig gevolg van de eerder genoemde Khintchine-ongelijkheid.

Ten tweede heeft de ruimte $\gamma(H, X)$ allerlei bijzondere eigenschappen. De belangrijkste is dat het een tweezijdig ‘ideaal’ is, in de volgende zin: Als $S : \tilde{H} \rightarrow H$ een begrensde operator is tussen de Hilbertruimten $\tilde{H}$ en H en $U : X \rightarrow \tilde{X}$ een begrensde operator tussen de Banachruimten X en $\tilde{X}$, dan geldt voor iedere $T \in \gamma(H, X)$ dat $U \circ T \circ S \in \gamma(\tilde{H}, \tilde{X})$ en

$$\begin{aligned} \|U \circ T \circ S\|_{\gamma(\tilde{H}, \tilde{X})} &\leq \|U\|_{\mathcal{L}(X, \tilde{X})} \|T\|_{\gamma(H, X)} \|S\|_{\mathcal{L}(\tilde{H}, H)}. \end{aligned}$$

Ten derde geldt een dominiestelling: als $T : H \rightarrow X$ en $\tilde{T} : \tilde{H} \rightarrow X$ begrensde operatoren zijn waarvan de geadjungeerden voldoen aan $\|\tilde{T}^* x^*\|_{\tilde{H}} \leq \|T^* x^*\|_H$ voor alle begrensde lineaire functionalen $x^* \in X^*$, dan impliceert $T \in \gamma(H, X)$ dat $\tilde{T} \in \gamma(\tilde{H}, X)$ en

$$\|\tilde{T}\|_{\gamma(\tilde{H}, X)} \leq \|T\|_{\gamma(H, X)}.$$

Deze resultaten kan men vervolgens gebruiken om allerlei krachtige approximatiestellingen te bewijzen voor de $\gamma(H, X)$ -norm. Al met al blijkt dus dat we prima met de $\gamma(H, X)$ -norm kunnen omgaan.

De opmerkelijke lezer heeft inmiddels echter gezien dat we nog niet veel hebben bereikt. We kunnen weliswaar omgaan met deterministische integranden in willekeurige Banachruimten, maar voor toepassingen op realistische stochastische PDV's moeten we random integranden kunnen integreren. En als we proberen het bovenstaande te generaliseren naar zulke integranden lopen we onmiddellijk vast: de stochastische integraal van een *random* stapfunctie is geen Gaussische som. Het gaat meteen al mis bij de identiteit (12)!

Op momenten dat alles hopeloos lijkt, gebeurt er soms een klein wonder. Dat wonder

overkwam de wiskundige Garling, die in een geheel andere context, namelijk de geometrie van Banachruimten, keek naar Banachwaardige stochastische integralen en zich het volgende realiseerde. Als men een Brownse beweging W 'randomiseert' door op gezette tijden t_n een muntje te gooien en bij '+1' niets doen, maar bij '-1' de bewegingsrichting van de Brownse beweging vanaf t_n 'om te klappen', dan krijgt men wederom een Brownse beweging. Als men nu de partitiepunten t_n steeds fijner kiest, krijgt men in de verdelingslimiet een Brownse beweging $\tilde{W}$ die onafhankelijk is van de oorspronkelijke Brownse beweging W (we veronderstellen uiteraard dat het werpen van de munt onafhankelijk is van W). Deze procedure van randomiseren suggereert een link met een Banachruimte-eigenschap, de zogenaamde UMD-eigenschap (de afkorting staat voor 'unconditional martingale differences'), die eveneens gedefinieerd is in termen van omklappen van incrementen.

Een Banachruimte heeft de *UMD-eigenschap* als er een exponent $1 < p < \infty$ bestaat, alsmede een constante B , zodanig dat voor iedere X -waardige martingaal-differentierij $(d_n)_{n=1}^N$ en voor iedere rij $(\varepsilon_n)_{n=1}^N \in \{-1, +1\}^N$ de volgende afchatting geldt:

$$\mathbb{E} \left\| \sum_{n=1}^N \varepsilon_n d_n \right\|_X^p \leq B^p \mathbb{E} \left\| \sum_{n=1}^N d_n \right\|_X^p.$$

Deze eigenschap is komen bovendrijven in het grensverleggende werk van Burkholder in de jaren tachtig en negentig op het gebied van Banachwaardige martingaaltheorie en blijkt onafhankelijk te zijn van de exponent $1 < p < \infty$. Hilbertruimten zijn UMD (neem $p = 2$) en L^p -ruimten zijn UMD voor $1 < p < \infty$ (neem exponent p en pas Fubini toe).

Garling bewees nu het volgende [4]. Als X een UMD-Banachruimte is, dan geldt voor alle aangepaste random stapfuncties $f: \mathbb{R}_+ \times \Omega \rightarrow X$ de tweezijdige ongelijkheid

$$\mathbb{E} \left\| \int_0^\infty f dW \right\|_X^p \approx \mathbb{E} \left\| \int_0^\infty f d\tilde{W} \right\|_X^p. \quad (14)$$

Met andere woorden, als we de L^p -norm van de stochastische integraal $\int_0^\infty f dW$ willen afschatten mogen we W door de onafhankelijke kopie $\tilde{W}$ vervangen! Dankzij een standaardargument in de kansrekening mogen we vervolgens ook veronderstellen dat W en $\tilde{W}$ op verschillende kansruimten $(\Omega, \mathbb{P})$ en $(\tilde{\Omega}, \tilde{\mathbb{P}})$ leven; de integraal $\int_0^\infty f d\tilde{W}$ is dan een toevalsvari-

abele op het product $(\Omega \times \tilde{\Omega}, \mathbb{P} \times \tilde{\mathbb{P}})$. Maar dat betekent dat we die integraal padsgewijs (dat willen zeggen per $\omega \in \Omega$) kunnen afschatten met behulp van de theorie voor deterministische integranden. Door Stelling 2 toe te passen op de functie $t \mapsto f(t, \omega)$ en Kahanes versie van de Khintchine-ongelijkheid te gebruiken om de L^2 -norm te vervangen door de L^p -norm vinden we

$$\mathbb{E} \left\| \int_0^\infty f(\cdot, \omega) d\tilde{W} \right\|_X^p \approx \|f(\cdot, \omega)\|_{\mathcal{Y}(L^2(\mathbb{R}_+), X)}^p. \quad (15)$$

In combinatie met Garlings equivalentie (14) hebben we dan het volgende gevonden:

Stelling 3 (Itô-isomorfisme voor random integranden in UMD-ruimten X). *Zij X een UMD-Banachruimte en zij $1 < p < \infty$. Er bestaat een constante B zodanig dat voor alle aangepaste random stapfuncties $f: \mathbb{R}_+ \times \Omega \rightarrow X$ de volgende tweezijdige afchatting geldt:*

$$\mathbb{E} \left\| \int_0^\infty f dW \right\|_X^p \approx \mathbb{E} \|f\|_{\mathcal{Y}(L^2(\mathbb{R}_+), X)}^p.$$

Deze stelling, die bewezen wordt in een gezamenlijk artikel met promovendus Mark Veraar en Lutz Weis [10], is een van de hoofdresultaten van het Vidi-project en bouwt voort op een eerder resultaat van McConnell [7], die echter geen L^p -afschattingen gaf en veel indirectere argumenten gebruikte. De stelling zegt dat, constanten in beide richtingen daargelaten, de L^p -norm van stochastische integralen in UMD-ruimten X precies gegeven wordt door de norm van de integrand als element in $L^p(\Omega; \mathcal{Y}(L^2(\mathbb{R}_+), X))$. Daarmee voorziet Stelling 3 in een volledig antwoord op de vragen (i) en (ii) die eerder zijn opgeworpen.

Het is interessant het resultaat van Stelling 3 te vergelijken met het eerdere resultaat voor martingaal-type 2-ruimten X . Voor zulke ruimten konden we de L^2 -norm van de integraal afschatten door de $L^2(\mathbb{R}_+ \times \Omega; X)$ -norm van de integrand. Met behulp van een slim stoptijdargument kan deze afchatting worden 'opgewerkt' tot een afchatting voor de L^p -norm van de stochastische integraal door de $L^p(\Omega; L^2(\mathbb{R}_+; X))$ -norm van de integrand. In deze vorm, om precies te zijn

$$\begin{aligned} \mathbb{E} \left\| \int_0^\infty f dW \right\|_X^p &\leq C^p \mathbb{E} \left(\int_0^\infty \|f(t)\|_X^2 dt \right)^{p/2}, \end{aligned} \quad (16)$$

staat de afchatting bekend als (de martingaal-type 2-versie van) *Burkholders ongelijkheid*.

Deze terminologie, alhoewel ingeburgerd, is eigenlijk niet correct, omdat de scalaire Burkholder-ongelijkheid een tweezijdige afchatting voor de L^p -norm van de stochastische integraal geeft. Dit is precies wat Stelling 3 doet voor UMD-ruimten X , en inderdaad reduceert deze stelling in het scalaire geval precies tot de tweezijdige Burkholder-ongelijkheid.

De bovenstaande theorie hebben we in het vervolgartikel [11] toegepast op een klasse van semilineaire beginwaardeproblemen die vergelijkingen van het type (9) als speciaal geval bevat. Voor zulke vergelijkingen kan men Stelling 3 gebruiken om een dekpuntargument toe te passen op (de corresponderende generalisatie van) de identiteit (10) en zo existentie, uniciteit en Hölder-regulariteit te bewijzen. De numerieke analyse van semilineaire stochastische PDV's is in vervolgwerk met Sonja Cox uitgewerkt [1].

Voordat we onze aandacht richten op maximale regulariteit wil ik één resultaat niet onvermeld laten: promovendus Sjoerd Dirksen heeft Stelling 3 uitgebreid, voor ruimten $X = L^q(M, \mu)$ met $1 < q < \infty$, naar Poisson-stochastische integralen [3]. Het verrassende resultaat is dat de L^p -norm van de integraal dan gekarakteriseerd wordt door zes verschillende normen, afhankelijk van de onderlinge positie van de exponenten 2 , p , en q . Het is vooralsnog een open probleem om dit resultaat uit te breiden naar willekeurige UMD-Banachruimten X .

Stochastische maximale regulariteit

Het einde van het Vidi-project begon intussen in zicht te komen en daarmee kom je, zeker bij het management, in de kijker als kandidaat voor het indienen van een Vici-aanvraag. Zelf had ik om eerlijk te zijn nogal het gevoel weinig kans te maken: NWO zou toch niet twee beurzen achtereen aan dezelfde persoon toekennen? Hoe dan ook, vraag (iii) stond nog wijd open en de oplossing ervan leek inmiddels binnen bereik te komen, dus dat leverde een goed onderwerp op.

Inmiddels schrijven we 2006, en er was veel veranderd. Iedere universiteit had inmiddels een hele infrastructuur rondom het binnenhalen van subsidies in de lucht. Communicatiedeskundigen, voorlichtingsmiddagen, schrijfcursussen en panels, allemaal om het beste uit een aanvraag te halen. Zo ook de TU Delft. Dit keer ging mijn aanvraag niet meteen naar NWO, maar eerst naar een universiteitsbreed panel van (niet-wiskundige) experts die er gehakt van maakten en een panel van communicatiedeskundigen dat verzuchtte dat het

voorstel “wellicht zelfs voor een doorgewinterde redacteur niet of nauwelijks te redigeren” was. Daar schrok ik nogal van, want ik dacht dat je een onderzoeksvoorstel zelf moest schrijven. Niet goed wetend wat ik met dit ‘advies’ moest aanvangen, heb ik het voorstel maar gewoon ingediend zonder er inhoudelijk nog iets aan te veranderen. Gelukkig bleken de referenten bij NWO zeer wel met mijn hiërogliefen uit de voeten te kunnen. Het daaropvolgende interview was, net als bij Vidi, vooral inhoudelijk (de meest onverwachte vraag was deze keer of ik wel eens iets aan het populariseren van mijn vak deed?) en uiteindelijk werd de aanvraag gehonoreerd.

U begrijpt, een leuke anekdote voor mijn afscheidsrede heb ik al. Anno nu is de begeleiding overigens veel beter geworden en ook PWN organiseert sinds kort succesvolle presentatietrainingen.

We pakken de draad van het verhaal weer op. Een van de belangrijkste stellingen aangaande de UMD-eigenschap is de stelling van Burkholder en Bourgain, volgens welke een Banachruimte X de UMD-eigenschap heeft dan en slechts dan als de Hilbert-transformatie

$$Hf(x) := \frac{1}{\pi} \int_{-\infty}^{\infty} \frac{f(y)}{x-y} dy,$$

die begrensd is op $L^p(\mathbb{R})$ voor $1 < p < \infty$ (dit is een klassieke stelling van Riesz), een voortzetting heeft tot een begrensde operator op $L^p(\mathbb{R}; X)$. Deze stelling legt een diep verband met Harmonische Analyse, waar de Hilbert-transformatie het prototype van een singuliere integraaloperator is en de aanzet vormt tot de Calderón–Zygmund-theorie van singuliere integraaloperatoren.

Nu wil het geval dat het probleem van stochastische maximale regulariteit voor deterministische vergelijkingen gereduceerd kan worden tot een probleem over X -waardige singuliere integralen. Om stochastische maximale regulariteit te bewijzen voor vergelijkingen van het type (9) blijkt dat we X -waardige singuliere stochastische integralen moeten bestuderen. Om precies te zijn dient men te bewijzen dat voor aangepaste $f \in L^p(\mathbb{R}_+ \times \Omega; X)$ het stochastische convolutieproces

$$t \mapsto \int_0^t (-A)^{1/2} e^{(t-s)A} f(s) dW(s) \quad (17)$$

welgedefinieerd is en wederom in $L^p(\mathbb{R}_+ \times \Omega; X)$ ligt. Deze stochastische integraal is ‘singulier’ vanwege het feit dat de norm van $(-A)^{1/2} e^{tA}$ in het algemeen schaal als $1/\sqrt{t}$,

hetgeen zich via Itô vertaalt in een $1/t$ singulariteit ten opzichte van de Lebesgue-maat dt .

Waarom is stochastische maximale regulariteit zo belangrijk? De convergentie van de stochastische integraal in (17) is equivalent met de uitspraak dat de milde oplossing van de vergelijking

$$du(t) = Au(t)dt + f(t)dw(t)$$

waarden aanneemt in het fractionele domein $\mathcal{D}((-A)^{1/2})$. Voor typische operatoren zoals $A = \Delta$ in $L^p(D)$ is dat fractionele domein gelijk aan een Sobolevruimte $H^{1,p}(D)$. Dit betekent dat de gradiënt van de oplossing, $\nabla u(t)$, goed gedefinieerd is. Als we alleen regulariteit tot (en niet tot en met) de kritieke exponent $1/2$ hadden, dan zou dit niet het geval zijn.

Met de genoemde L^p -afschatting voor (17) in de hand gaat de deur open naar een reeks belangrijke toepassingen: niet alleen kan men de niet-lineariteiten in de vergelijking ook van ∇u laten afhangen (een voorbeeld bespreken we hierbeneden), men kan de afschatting ook gebruiken om tijdsafhankelijke problemen te reduceren tot tijdsafhankelijke problemen.

Het bewijzen van de convergentie van singuliere integralen is meestal in hoge mate niet-triviaal en vereist delicate technieken uit de harmonische analyse. Het was dan ook verre van duidelijk hoe je de convergentie van (en L^p -afschattingen voor) de stochastische convoluties van het type (17) zou moeten bewijzen.

Voor $p = 2$ en Hilbertruimten X was stochastische maximale regulariteit al in de jaren negentig bewezen door Da Prato en Zabczyk [2] onder een aanname op A die equivalent is aan het hebben van een zogenaamde begrensde H^∞ -calculus. Dit is een spectrale calculus, die in Banachruimten een goed substituuut geeft voor de Borel-calculus voor zelfgeadjungeerde operatoren. Deze calculus is in de jaren tachtig en negentig ontwikkeld door Alan McIntosh, die er een aantal bekende open problemen in de spectrale theorie mee heeft opgelost. Voorbeelden van operatoren met een H^∞ -calculus zijn de Laplace-operator, elliptische operatoren, en de Stokes-operator.

Vervolgens bewees Krylov dat voor $2 < p < \infty$ de Laplace-operator, en algemener veel tweede-orde-elliptische operatoren, stochastische maximale regulariteit hebben op $L^q(\mathbb{R}^d)$ met $q \in [2, \infty)$ [5].

Het al dan niet begrensd zijn van de H^∞ -calculus van een gegeven operator is equi-

valent met het al dan niet convergeren van een zekere singuliere integraal geassocieerd met de operator. Dat bracht ons op het idee om H^∞ -calculus in te zetten bij de behandeling van stochastische maximale regulariteit via (17). Dat klinkt makkelijker gezegd dan gedaan, maar uiteindelijk bleek het idee te werken. In het artikel [13] konden Mark Veraar, Lutz Weis en ik stochastische maximale regulariteit voor $2 < p < \infty$ bewijzen voor willekeurige operatoren A met een H^∞ -calculus op $L^q(\mathbb{R}^d)$ met $2 \leq q < \infty$ (en voor $2 \leq p < \infty$ als $q = 2$). Het bewijs maakt op essentiële wijze gebruik van de precieze tweezijdige afschatting van Stelling 3 alsmede de Fefferman–Stein-stelling uit de harmonische analyse. Het is interessant om op te merken dat ons bewijs met de zwakkere martingaal-type 2-afschatting (16) niet zou werken.

In het vervolgartikel [12] hebben we het resultaat toegepast op een aantal stochastische PDV's, waaronder de incompressibele stochastische Navier–Stokes-vergelijking

$$\frac{\partial u}{\partial t} = \Delta u - (u \cdot \nabla)u - \nabla p + g(u, \nabla u)\dot{W}$$

met Dirichlet-randvoorwaarden op een begrensd gebied D in $\mathbb{R}^d$. We laten zien dat deze vergelijking een oplossing heeft in de Sobolevruimte $(H^{1,q}(D))^d$ voor alle $q \in [2, \infty)$. Voor $D = \mathbb{R}^d$ was dit al eerder bewezen door Mikulevicius en Rozovskii, die gebruik maakten van geheel andere technieken. Het feit dat de niet-lineaire term g ook van ∇u mag afhangen (we spreken dan ook wel van ‘gradient type noise’) wordt door fysici gebruikt om turbulentie te modelleren. Het is precies de stochastische maximale regulariteit die ons toestaat om de gradiënt ∇u mee te nemen in de ruisterm.

In het onlangs afgesloten Veni-project van Mark Veraar is het thema stochastische maximale regulariteit verder uitgediept en toegepast.

Malliavin-calculus

Een tweede hoofdresultaat van het Vici-project is eveneens een soort maximale regulariteitsstelling. Deze stelling, die promovendus Jan Maas en ik bewezen hebben in [6], geeft een nodige en voldoende voorwaarde, in termen van het bestaan van een H^∞ -calculus, voor de geldigheid van een oneindig-dimensionale generalisatie van Meyers ongelijkheid.

Meyers ongelijkheid is de centrale L^p -ongelijkheid in de Malliavin-calculus, een differentiaalcalculus waarbij de rol van de



Lebesgue-maat vervangen wordt door een Gauss-maat γ ; dit heeft als voordeel dat ook in oneindig veel dimensies gewerkt kan worden. Om te begrijpen wat Meyers ongelijkheid zegt, kijken we naar een van de eenvoudigste stochastische differentiaalvergelijkingen, de zogenaamde *Langevin-vergelijking*

$$du(t) = -u(t) dt + dW(t).$$

De oplossing van deze vergelijking heet het *Ornstein–Uhlenbeck-proces*. Dit is een Markov-proces; de generator van de bijbehorende Markov-halfgroep noemen we L . Een interessant terzijde is dat deze operator in de kwantumoptica bekend staat als de ‘number operator’ die het aantal fotonen telt. Meyers ongelijkheid zegt nu dat voor alle $1 < p < \infty$,

$$\|(-L)^{1/2} f\|_p \approx \|Df\|_p \quad (18)$$

met constanten die alleen van p afhangen. Hier is D de Malliavin-afgeleide, het Gaussische substitueert voor de gradiënt.

De stelling van Jan Maas en mijzelf geeft een analogon van (18) voor een algemene klasse van lineaire stochastische *partiële* differentiaalvergelijkingen. In zijn proefschrift

heeft Jan bovendien een begin gemaakt met een systematische UMD-waardige Malliavin-calculus, een waar mijnenveld waar al meerdere bekende wiskundigen onjuiste resultaten bleken te hebben gepubliceerd. Promovendus Matthijs Pronk heeft deze theorie verder uitgewerkt [14].

Internet seminar

Qua onderwijs was een van de hoogtepunten het Internet Seminar ‘Stochastic Evolution Equations’ dat ik in het academisch jaar 2007/08 heb aangeboden. Het Internet Seminar (ISem) [16] is een jaarlijks online college voor promovendi dat bestaat sinds de jaren negentig (een ‘OOC’ *avant la lettre*, met gemiddeld een honderdtal deelnemers nog net geen MOOC) en rouleert tussen Europese universiteiten.

Een ISem bestaat uit een aantal wekelijkse lezingen die via Internet verspreid worden, gevolgd door een projectfase waarin deelnemende studenten in kleine internationale groepjes aan projecten werken en een afsluitende workshop.

Dit was een goede gelegenheid de belangrijkste resultaten uit het Vidi-project te ordenen en toegankelijk te maken op graduate niveau. De ISem Lecture Notes [8] waren het begin van een omvangrijk boekproject met Tuomas Hytönen, Mark Veraar en Lutz Weis over analyse in Banachruimten, dat momenteel in volle gang is. Nu dat de drukke VI-jaren achter de rug zijn hoop ik daar weer meer tijd voor te kunnen vrijmaken.

Tot slot

Er is tegenwoordig veel te doen over de financiering van het vrije onderzoek. Door de topsectoren is er steeds minder budget voor vrij onderzoek, waardoor slaagkansen laag

zijn en veel onderzoekstijd in rook opgaat bij het schrijven van voorstellen die niet gehonoreerd worden.

In dit alles is de Vernieuwingsimpuls een redelijk constante succesfactor. Zeker voor wiskundigen die geen lab hoeven te runnen, zijn de subsidies in de VI enorm hoog. Velen, waaronder ikzelf, zijn van mening dat die best iets kleiner zouden kunnen, om zo meer voorstellen te kunnen honoreren (zie in dat verband mijn column in het maartnummer van dit blad en de bijdrage van Klaas Landsman in het afgelopen juninummer). Veel excellente voorstellen halen het nu niet en de scheidslijn tussen wel en geen succes is dun: doordat de aanvragen door een gemengd panel van wiskundigen, informatici en astronomen worden beoordeeld, bevat de uitslag onvermijdelijke ruis.

Dat gezegd hebbende blik ik terug op een intensieve en zeer productieve periode. In het begin moest ik erg wennen aan de vele ogen die ik opeens op me gericht voelde: persberichten, nieuwsitems en een interview in het universiteitsblad scheppen immers hoge verwachtingen en een navenante (zelfopgelegde) prestatiedruk. Maar al snel komen de positieve aspecten bovendrijven: met zoveel middelen krijg je de kans om echt iets op te bouwen. Omringd door de vele promovendi en postdocs (aan het werk van de laatstgenoemden heb ik in dit bestek helaas geen recht kunnen doen) waren er wel eens momenten dat ik mij een wetenschapsmanager voelde, maar het was altijd geweldig om met deze jonge mensen samen te werken en wetenschappelijk is er veel bereikt. En tot slot: met de onlangs toegekende Vidi van Mark Veraar krijgt het onderzoek aan stochastische PDV's in Nederland een uitstekend vervolg. 

Referenties

- 1 S.G. Cox en J.M.A.M. van Neerven, Pathwise Hölder convergence of the implicit Euler scheme for semi-linear SPDEs with multiplicative noise, *Numerische Mathematik* 125 (2013), 259–345.
- 2 G. Da Prato en J. Zabczyk, Stochastic Equations in Infinite Dimensions, *Encyclopedia of Mathematics and its Applications* 44, 2e editie, Cambridge University Press, 2014.
- 3 S. Dirksen, Itô isomorphisms for L^p -valued Poisson stochastic integrals, te verschijnen in *Ann. Probab.*, arXiv:1208.3885.
- 4 D.J.H. Garling, Brownian motion and UMD-spaces, in *Probability and Banach spaces (Zaragoza, 1985)*, Springer Lecture Notes in Math. 1221, 1986, pp. 36–49.
- 5 N.V. Krylov, On the foundation of the L_p -theory of stochastic partial differential equations, in *Stochastic partial differential equations and applications-VII*, Lect. Notes Pure Appl. Math. 245, Chapman & Hall/CRC, 2006, pp. 179–191.
- 6 J. Maas en J.M.A.M. van Neerven, Boundedness of Riesz transforms for elliptic operators on abstract Wiener spaces, *J. Funct. Anal.* 257 (2009), 2410–2475.
- 7 T.R. McConnell, Decoupling and stochastic integration in UMD Banach spaces, *Probab. Math. Statist.* 10 (1989), 283–295.
- 8 J.M.A.M. van Neerven, Stochastic Evolution Equations, Lecture Notes van het 2007/08 Internet Seminar, repository.tudelft.nl.
- 9 J.M.A.M. van Neerven, M.C. Veraar en L.W. Weis, Stochastic integration in Banach spaces – a survey, te verschijnen in *Proceedings of the 2012 EPFL Semester on Stochastic Analysis and Applications*, arXiv:1304.7575.
- 10 J.M.A.M. van Neerven, M.C. Veraar en L.W. Weis, Stochastic integration in UMD Banach spaces, *Ann. Probab.* 35 (2007), 1438–1478.
- 11 J.M.A.M. van Neerven, M.C. Veraar en L.W. Weis, Stochastic evolution equations in UMD Banach spaces, *J. Funct. Anal.* 255 (2008), 940–993.
- 12 J.M.A.M. van Neerven, M.C. Veraar en L.W. Weis, Maximal L^p -regularity for stochastic evolution equations, *SIAM J. Math. Anal.* 44 (2012), 1372–1414.
- 13 J.M.A.M. van Neerven, M.C. Veraar en L.W. Weis, Stochastic maximal L^p -regularity, *Ann. Probab.* 40 (2012), 788–812.
- 14 M. Pronk en M.C. Veraar, Tools for Malliavin calculus in UMD Banach spaces, *Potent. Anal.* 40(2014), 307–344.
- 15 M. Yor, Sur les intégrales stochastiques à valeurs dans un espace de Banach, *Ann. Inst. H. Poincaré Sect. B (N.S.)*, 10 (1974), 31–36.
- 16 isem17.unisa.it/w/index.php/17th-Internet-Seminar

Gunther Cornelissen

Mathematisch Instituut

Universiteit Utrecht

g.cornelissen@uu.nl

Onderzoek Vici-project

Differentialmeetkunde in de getaltheorie

Voor getaltheorie is geen enkel soort wiskunde te min; de koningin onder de wiskunde-disciplines heeft combinatoriek, algebra en algebraïsche meetkunde gebruikt, complexe analyse, representatietheorie, Lie-theorie, ergodentheorie, grootschalig rekenen, symbolisch rekenen, en het lijstje zou nog lang kunnen doorgaan. Getaltheorie is ook streng: de gebruikte methode moet iets voor je doen. In ieder geval had differentialmeetkunde nog niet veel voor getaltheorie gedaan. Gunther Cornelissen bespreekt zijn Vici-project, waar het precies om toepassingen in deze richting gaat.

Nog een slagje algemener dan differentialmeetkunde is niet-commutatieve meetkunde, en de feitelijke slogan van mijn Vici-project was: onderzoek of niet-commutatieve Riemannse meetkunde en getaltheorie iets voor mekaar kunnen betekenen. De sfeer is ietwat vertroebeld doordat hardcore niet-commutatieve meetkundigen overmatig enthousiast zijn over de mogelijke betekenis van hun vakgebied voor de getaltheorie, terwijl de droge *pauca sed matura*-getaltheoretici liever even de kat uit de boom kijken, of na vele jaren van niet ingeloste beloftes over de Riemann-hypothese of Hilberts 12de probleem het helemaal hebben afgeschreven. Ikzelf neem ergens een middenpositie in: ik heb een hekel aan grandioze beweringen, maar wil wel op zoek naar kruisbestuiving; de constructies en taal van het ene gebied leren en in verband brengen

met die van het andere gebied. En dan de daarbij passende beginnersfouten (mogen) maken... Dit project was mijn uitrusten van 'diamanten voor het kwantum', om het in typische Nederlandse clustertaal te zeggen.

De basis ontbreekt?

Het beginpunt van het onderzoek was de vaststelling dat er in de niet-commutatieve meetkunde aan de kant van de 'high-brow' toepassingen heel wat gebeurt, terwijl er aan de basis best nog werk is. Er is geen 'Graduate Text' waaruit de theorie van spectrale tripels (= niet-commutatieve variëteiten) kan worden geleerd op een droge, ontbeende manier (zonder natuurkunde, zonder een heel curriculum differentialmeetkunde en operatoralgebra, et cetera). Er zijn ook niet genoeg voorbeelden van objecten en bijbehorende

morfismen. En erger nog, het natuurlijke begrip van isomorfisme, 'Morita-equivalentie', blijkt in deze context geen equivalentierelatie te zijn. Kan getaltheorie voorbeelden opleveren?

Een interessante bijdrage kwam met het promotie-onderzoek van Jan Jitse Venselaar, die alle niet-commutatieve n -dimensionale tori classificeerde en hun equivalenties in kaart bracht [1]. Onder andere gaf hij de eerste voorbeelden van (niet-triviale) equivalenties die ook echt omkeerbaar waren [2]. Een hoogtepunt in zijn onderzoek kwam toen hij het classificatieprobleem had herleid tot een probleem in de lineaire algebra, en dat toen niet kon oplossen; waarop hij het oorspronkelijke probleem met meetkunde oploste, en de stelling in de lineaire algebra een gevolg werd. Het resultaat is een nieuwe methode, en uiteindelijk ook een redelijk grote verzameling voorbeelden waarvoor de equivalenties min of meer begrepen zijn.

Bram Mesland kwam als post-doc op het project terecht. Hij had in zijn proefschrift in Bonn een notie van 'correspondentie' ingevoerd voor spectrale tripels, die hij in Utrecht verder ging uitwerken [3]. Wij zijn nog steeds aan het werk om dit begrip te

Het Vici-project in feiten

NWO project 639.033.705

From Arithmetic Geometry to Non-commutative Riemannian Geometry, and back
Looptijd: 2008–2014.

Budget: 1,25 miljoen euro.

Output: circa. 25 publicaties, 500 pp., 40 noemenswaardige stellingen.

Twee postdocs:

- Bram Mesland, ging als postdoc naar Warwick.
- Jorge Plazas, ging als postdoc naar Granada.

Vier promovendi:

- Jan Willem de Jong, *Zeta function rigidity - a view from noncommutative geometry*, 2011, ging bij Collis werken.
- Jan Jitse Venselaar, *Classification and equivalences of noncommutative tori and quantum lens spaces*, 2012, ging naar Caltech als postdoc.
- Janne Kool, *Graphs, curves and dynamics*, 2013, ging naar Bonn als postdoc.
- Sebastian Klein, *Chow groups and intersection products for tensor triangulated categories*, promoveert hopelijk in september 2014, daarna postdoc in Antwerpen.



De eerste jaren kon je enkel promoveren binnen dit project als je voornaam met 'Jan' begon, maar later werd deze regel flexibeler.

veralgemeniseren, opdat er een (Gromov-Hausdorff-achtige) metriek ontstaat op de ruimte van spectrale triples op (gesymmetriseerde) Morita-equivalentie na. Dankzij deze theorie, die hopelijk in 2015 wordt opgeschreven, kan je bijvoorbeeld zinvol praten over het limietobject van een cirkel met een groepsactie als de straal van de cirkel naar nul gaat (en zodat het limietobject nog iets van de groepsactie weet).

Spectra, invarianten, en reconstructie

Het is de bedoeling van 'spectrale tripels' om meetkunde met spectrale invarianten te doen, en dan is het een natuurlijke vraag of er een complete set van spectrale invarianten is voor een gegeven ruimte, die hem uniek op 'isometrie' na karakteriseert. Het Laplace-spectrum zelf doet het niet altijd; dat is het probleem van de 'isospectraliteit', of, meer plastisch verwoord: "You cannot hear the shape of a drum." De spectrale invarianten worden samengepakt in zeta-functies, en daardoor voelt de getaltheoretiek zich meteen aangesproken. Ik had met Matilde Marcolli al een constructie gegeven van voldoende spectrale invarianten voor het karakteriseren van Riemann-oppervlakken, door gebruik te

maken van maat-theoretische rigiditeit à la Mostow, en in het proefschrift van Jan Willem de Jong wordt het voor grafen en Riemannse variëteiten gedaan [4]. Omdat spectra diffeomorfisme-invarianten zijn, lijkt dit resultaat ook relevant voor de kwantisatie van gravitatie. Per slot van rekening is alle 'waarneming' (geluid, licht, ...) intrinsiek spectraal, dus eigenlijk is een beschrijving met behulp van spectra in plaats van coördinaten veel natuurlijker.

Dit was de inspiratie voor wat ik het leukste deel van het onderzoek vond: kan zo iets ook voor getallenlichamen? Bost en Connes hadden een kwantum-statistisch mechanisch systeem opgesteld met als partitie-functie de Riemann-zeta-functie, en Ha en Paugam schreven begin deze eeuw een variant op voor een algemeen getallenlichaam, waarvan de partitie-functie de Dedekind-zeta-functie ζ_K van het getallenlichaam K is. Sinds oud werk van Gauss uit de jaren twintig weten we dat ζ_K het lichaam K bepaalt als K een normale lichaamsuitbreiding is van $\mathbb{Q}$. De eerste voor de hand liggende vraag wordt: als de systemen van twee getallenlichamen 'isomorf' zijn, zijn de zeta-functies dan gelijk? Dit was niet al te moeilijk, en met Marcolli had

ik het binnen een week uitgewerkt. Nu werd het ambitieuzer: zijn de lichamen dan ook isomorf? Dit is filosofisch interessant, omdat de systemen enkel informatie over abelse uitbreidingen van K gebruiken, terwijl de klassieke stellingen in deze richting (van Uchida) ook niet-abelse uitbreidingen nodig hebben.

Het werd een lang reconstructie-bewijs, vol verraderlijk gladde plekken [5]. Het is dan ook nog steeds niet af: ik heb het nu in vier stukken opgehakt die in 2015 uitkomen. Ondertussen heb ik het wel voor functielichamen (krommen over eindige lichamen) bewezen, waar het veel korter kan [6]. Omdat alles ook puur getaltheoretisch te formuleren is in termen van L -reeksen (die te voorschijn komen uit de evenwichtstoestanden van het systeem) was er aanvankelijk veel enthousiasme voor het resultaat, maar ondertussen hebben de rangen zich weer gesloten, en is onze ontdekking als 'odeloos ingewikkeld' weggezet [7].

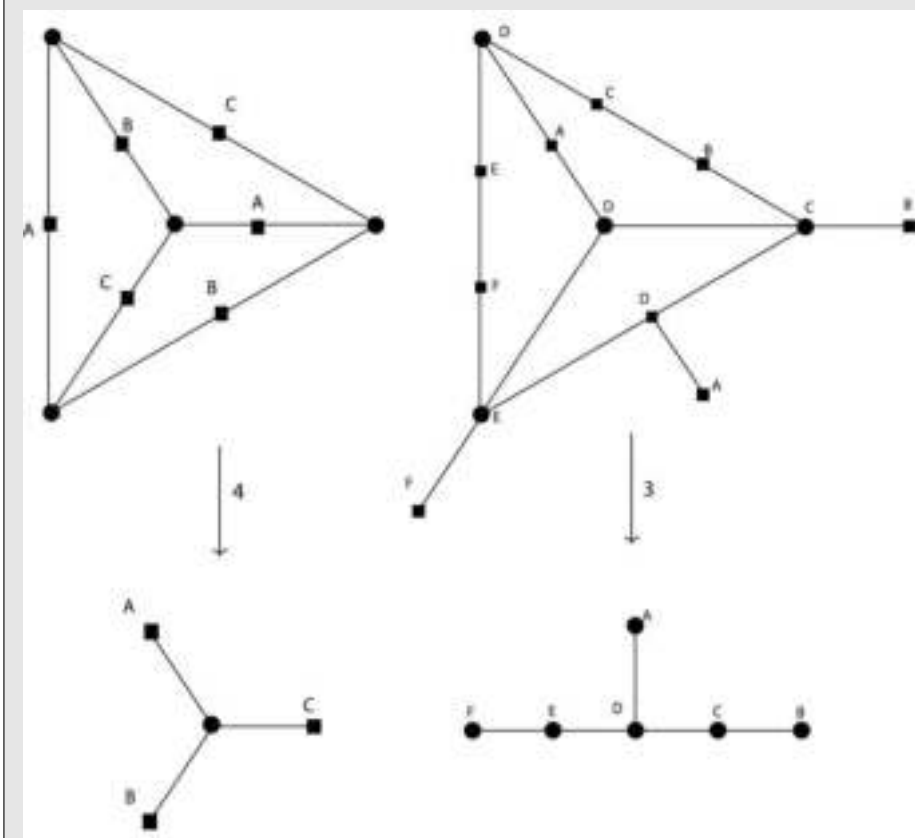
Ondertussen kwamen er, waarschijnlijk door deze combinatie van kwantumtheorie met getaltheorie, een paar natuurkundigen bij me langs met vragen over elliptische krommen, die ik ook nog eens kon oplossen, en zo komen in het Vici-project ook publicaties over membraanmodellen van het universum voor [8].

Een p -adische variant

Aldus komen we bij de p -adische variant van dit alles. Janne Kool schreef binnen het project een fascinerend proefschrift, waarin, na het invoeren van dynamica met p -adisch waardige maten, eerst maat-theoretische rigiditeit voor p -adische uniformiseerbare krommen werd bewezen [9]. Het hoogtepunt van dit deel van het onderzoek was het p -adische analogon van de Li-Yau-ongelijkheid voor gonaliteit van Riemann-oppervlakken [10]. Het oorspronkelijke resultaat, dat Li en Yau differentiaal-meetkundig bewezen in verband met de theorie van minimale oppervlakken ('zeepbellen'), geeft een ondergrens voor de minimale graad van een afbeelding van een Riemann-oppervlak X naar de Riemann-sfeer in termen van het volume en het Laplace-spectrum van X . In onze variant is het een ondergrens voor de graad van een harmonische afbeelding van een graaf (en zijn verfijningen) naar een boom in termen van invarianten van de graaf. Het bewijs lijkt in niets op het origineel, en de irregulariteit van de graaf speelt ons parten. Uiteindelijk kan je met deze 'differentiaalmeetkunde' bepaalde diophantische problemen op-

Brill–Noether voor grafen

Stel dat K_4 de complete graaf is met vier knopen. De minimale graad van een grafenmorfisme van K_4 naar een boom is 4, en links in de figuur staat een voorbeeld van een dergelijke afbeelding. Voor de minimale graad van een morfisme van een Riemann-oppervlak naar een sfeer bestaat de Brill–Noether-bovengrens: $\frac{g+3}{2}$, waarbij g het aantal onafhankelijke lussen op het oppervlak is. Dit heeft ook zin voor grafen, en K_4 heeft 3 onafhankelijke lussen, dus de bovengrens wordt 3. Maar de minimale graad was 4? De Brill–Noether-bovengrens blijkt wel degelijk ook te kloppen voor grafen, maar het grafenmorfisme mag van een *verfijning* van de graaf naar een boom gaan. Hier betekent ‘verfijnen’ het onderverdelen van kanten en het toevoegen van losse kanten. Rechts in de figuur staat een dergelijke verfijning van K_4 met een morfisme van graad 3 naar een boom. In het werk van Janne Kool gaat het om het vinden van een *ondergrens* voor deze minimale graad.



lossen. Interessant is ook een verband met ‘boombreedte’, een concept uit de theoretische informatica, en zandhoopmodellen uit de stochastiek.

Een categorische variant

Tenslotte is er een andere ‘niet-commutatieve’ kijk op meetkunde, namelijk, via categorietheorie. Het blijkt onmogelijk om een niet-commutatieve projectieve variëteit te maken door het ‘plakken’ van spectra van niet-commutatieve ringen, zoals dat commutatief gebruikelijk is. Maar een projectieve variëteit kan worden gecodeerd in de tensor-getrianguleerde categorie van zijn perfecte complexen. Je kan dus proberen niet-

commutatief rechtstreeks te werken met zulke categorieën. In de natuurkunde komt dit voor in de homologische variant van spiegelsymmetrie, als ‘intersecting D -branes’. In zijn proefschrift heeft Sebastian Klein intersectietheorie ontwikkeld voor dergelijke algemene tensor-getrianguleerde categorieën [11]. Zijn nieuwe theorie staat pas in de kinderschoenen, maar lijkt een functoriële constructie te zijn met veel potentieel — ze bevat misschien wel een goede intersectie-theorie voor singuliere variëteiten. In ieder geval heb ik nu geleerd dat een cykel *niet* een lineaire combinatie is van deelvariëteiten, maar een eindig rijtje elementen uit de K_0 -groepen van quotiëntcategorieën,

en voor gladde variëteiten zijn die groepen ‘toevallig’ de gehele getallen.

Conclusie

Hiermee is de inhoud van het project grosso modo gedekt. Het werd een interessante tocht die bij klassieke differentiaalmeetkunde begon en via meer natuurkunde-geïnspireerde ideeën uitkwam bij combinatorische en categorie-theoretische beschouwingen.

Het project had veel onverwachte wendingen en euforische momenten. Ik ben echt trots op de uitkomst, ook op het excellente werk van het hele team, en in het bijzonder de promovendi, die ieder hun eigen lijn en hun eigen wiskundige persoonlijkheid hebben ontwikkeld. Om een ‘school’ te maken, zoals de meeste wetenschappers doen, past helemaal niet bij mijn eigen springerigheid. Maar ik mis mijn oud-teamgenoten nu al; misschien is dat deel van mijn ontwenningssverschijnselen.

Voor en tegen de ‘Vernieuwingsimpuls’

Mijn houding ten opzichte van het Vernieuwingsimpuls-schema is erg ambivalent. Het is een unieke kans om riskant onderzoek te financieren, uitgevoerd in een voor wiskunde ongebruikelijke vorm: met tijdelijk een redelijk grote groep onderzoekers en bijbehorende focus. NWO kon hiermee, buiten het structurele onderzoeksgeld van de universiteiten om, *extra* onderzoek gaan financieren — heerlijk. Maar de afgelopen jaren heeft er een ‘aardverschuiving’ plaatsgevonden in de financiering van wetenschap. ‘Aard’ betekent hier ‘Geld’; in bijbelse taal ook bekend als ‘Slijk’. Het vernieuwingsimpuls-budget is niet meer ‘extra’ — wat het volgens mij zou moeten zijn, om echt riskant te ‘vernieuwen’ — maar het is de ruggengraat geworden van de financiering van de wetenschap; een overlevensnoodzaak voor departementen en universiteiten. Dit heeft allerlei nare gevolgen: bevorderingen en benoemingen hangen af van het binnenhalen van deze subsidies; en gedegen aanstellingsbeleid is vervangen door het pragmatisch aantrekken van de wetenschappers die dit soort geld hebben. De combinatie met het Mattheus-effect (“wie heeft, zal meer krijgen”) en steeds meer thematisch sturen door of via NWO is erg ongelukkig, want wie weet wat ‘belangrijk’ zal worden? Is ‘weinig, groot en gestuurd’ beter dan ‘velen, klein en vrij’? (Leest allen het interview dat Higgs gaf aan *The Guardian* nadat hij de Nobelprijs ontving [12].) Natuurlijk komt kwaliteit bovendien (zie mijzelf, ha-

Het Vici-project in stellingen en definities

Hierbij een aantal (meer technisch geformuleerde) resultaten van het project.

Stelling (C). *Twee globale functielichamen K en L zijn isomorf precies als er een groepsisomorfisme ψ bestaat tussen de groepen van lineaire karakters van hun absolute Galois-groepen, zodat er identiteiten van L -reeksen zijn $L(K, \chi) = L(L, \psi(\chi))$ voor alle χ .*

Stelling (Venselaar). *Iedere n -dimensionale equivariante niet-commutatieve torus is een isospectrale deformatie van een commutatieve n -torus.*

Stelling (C-de Jong). *Een diffeomorfisme φ tussen twee Riemannse variëteiten X en Y met enkelvoudig Laplace-spectrum is een isometrie precies als $\text{tr}(\varphi^*(a) \Delta_X^s) = \text{tr}(a \Delta_Y^s)$ voor alle functies $a \in C^\infty(Y)$.*

Stelling (C-Kato-Kool). *Als de intersectie-duale graaf G is van het stabiele model van een kromme X over een compleet niet-archimedisch lichaam k n knopen heeft, dan is de gonality van X beneden begrensd door $\lambda n / (5\lambda + 4)$, waarbij λ de kleinste niet-nul eigenwaarde is van de Laplace-operator van G .*

Definitie (Klein). *Een functoriële definitie van Chow groep en intersectieproduct in een tensorgetrianguleerde categorie.*

Definitie (C-Mesland). *Een afstand in de ruimte van spectrale triples, zodat afstand nul precies Morita-equivalentie betekent.*

hal), maar het is wel altijd *hetzelfde soort kwaliteit*. Voor een omstreden project kan je bij definitie geen vijf referenten vinden die het allemaal top vinden. Een onhandige aanvrager geeft een knullig interview, wat dan? Laat ons een stapje terugzetten en vragen: is dit alles nog een impuls voor vernieuwing? Waar is het radicale, baanbrekende onderzoek?

Er rest NWO nog een vervolgprogramma op het succesvolle 'Veni-Vidi-Vici' te lanceren, mag ik voorstellen onder de naam *Brutus*, waarvan de winnaars tot de peer group van 1 procent voormalig meest succesvolle wetenschappers dienen te behoren, en die na het verkrijgen van tenminste vijf A++ ('exemplary') evaluaties door een commissie bestaande uit niet-vakgenoten definitief op een zijspoor worden gerangeerd. Ook gij, mijn maecenas? 

Referenties

- J.J. Venselaar, Classification of spin structures on the noncommutative n -torus, *J. Noncommut. Geom.* 7 (2013), 787–816.
- J.J. Venselaar, Morita "Equivalences" of Equivariant Torus Spectral Triples, *Lett. Math. Phys.* 103 (2013), 131–144.
- B. Mesland, Unbounded Bivariant K -Theory and Correspondences in Noncommutative Geometry, *J. Reine Angew. Math.* 691 (2014), 101–172.
- G. Cornelissen en J.W. de Jong, The spectral length of a map between Riemannian manifolds, *J. Noncommut. Geom.* 45 (2012), 721–758.
- G. Cornelissen en M. Marcolli, Quantum statistical mechanics, L -series and anabelian geometry, preprint, arXiv:1009.0736.
- G. Cornelissen, Curves, dynamical systems, and weighted point counting, *Proc. Natl. Acad. Sci. USA* 110 (2013), 9669–9673.
- Vergelijk ook: M. Marcolli, *The Sombre Science (a theater play)*, beschikbaar op lulu.com (2013).
- N. Akerblom en G. Cornelissen, A compact codimension two braneworld with precisely one brane, *Phys. Rev. D* 81 (2010), 124025.
- G. Cornelissen en J. Kool, Measure theoretic rigidity for Mumford curves, *Ergodic Th. Dyn. Sys.* 33 (2013), 851–869.
- G. Cornelissen, F. Kato and J. Kool, A combinatorial Li–Yau inequality and rational points on curves, *Math. Ann.* (2014), 50 pp., arXiv: 1211.2681.
- S. Klein, *Chow Groups and Intersection Products for Tensor Triangulated Categories*, proefschrift (2014).
- Peter Higgs interview: 'I have this kind of underlying incompetence', *The Guardian*, posted online 6 December 2013 on <http://www.theguardian.com/science/2013/dec/06/peter-higgs-interview-underlying-incompetence>.

Bas Edixhoven

Mathematisch Instituut

Universiteit Leiden

bas@edixhoven.net

Onderzoek Vici-project

Aritmetische meetkunde

Bas Edixhoven vroeg in 2002 een Vici-subsidie aan voor het project 'Arithmetic geometry, motives: computational aspects'. Deze aanvraag werd *niet* gehonoreerd. In 2004 was dezelfde aanvraag *wel* succesvol. In dit artikel blikt hij terug op zowel de aanvraag- als op de uitvoeringsperiode, en geeft hij enkele adviezen aan NWO.

Verslag doen is een goede zaak. Zeker als er 1,25 miljoen euro aan publieke middelen is gestoken in een individueel onderzoeksproject. Natuurlijk worden er verslagen voor de grootste geldschieter, NWO, geschreven, elk jaar zolang het project loopt, *en* op het midden, *en* aan het eind. Maar die verslagen bereiken maar een zeer klein publiek. En het zijn grotendeels weinig inspirerende opsommingen van proefschriften, publicaties, voordrachten en andere vormen van 'output'. Zulke verslagen belanden al gauw in een digitale map, van waaruit ze dan hopelijk nog eens worden opgevraagd wanneer de uitvoerder een nieuwe aanvraag indient. Ik ben een groot voorstander van het beoordelen van aanvragers op prestaties uit het verleden, en niet op beloften voor de toekomst. Het is dan interessant (NWO-bestuurders, lezen jullie mee?) om te kijken hoeveel van de heldhaftige plannen uit de vorige aanvraag daadwerkelijk zijn gerealiseerd.

Ik neem dus nu graag mijn laptop op schoot om aan het verzoek van de redactie

van dit blad te voldoen en een verslag te schrijven over het door mij uitgevoerde Vici-project, niet voor *alle* belastingbetalers, maar wel voor alle lezers van het *Nieuw Archief voor Wiskunde* en, laten we zeggen, voor allen die zich wiskundigen kunnen noemen.

Het schrijven van de aanvraag

Het was niet mijn eigen idee om een Vici project aan te vragen bij NWO. Het idee kwam van de toenmalige directie van het Leidse Mathematisch Instituut (en met name van Gerrit van Dijk) in december van 2001, toen ik daar vanuit Frankrijk solliciteerde naar een hoogleraarspositie. Ook toen was dit soort geld al belangrijk voor het overleven van de Nederlandse wiskunde-instituten, die geteisterd werden door lage studentenaantallen. Aangezien het mijn ambitie was in Leiden een sterke groep op mijn vakgebied 'aritmetische meetkunde' op te zetten, zowel voor onderzoek als voor onderwijs, kwamen onze belangen overeen. Na enig onderhandelen kreeg ik een aanbod uit Leiden dat ik aannam, en begon ik met na-

denken over de aanvraag. Een eerste versie, vooraanmelding geheten, moest al per 1 april bij NWO zijn ingediend. Ik had al een goede onderzoeksvraag, gebaseerd op een vraag van René Schoof uit 1995. Over die vraag had ik al af en toe nagedacht, maar kwam pas weer verder na een cruciale suggestie van Jean-Marc Couveignes in 1999 (gebruik geen algebra, maar numerieke analyse!). In oktober 2000 had ik een kansrijke strategie gevonden, die ik samen met Couveignes zou uitwerken. Onze taken waren goed gescheiden: Jean-Marc werkte aan benaderingen met behulp van numerieke analyse, en ik aan afschattingen van de benodigde precisie. In december 2000 had ik over dit project gesproken tijdens een conferentie in Berkeley voor een publiek van aritmetisch meetkundigen (zie [22]), maar daarna had ik er nog niet verder aan gewerkt omdat het een meerjarenklus zou worden, en aan werk had ik geen gebrek.

Bij het schrijven van de vooraanmelding besteedde ik de meeste tijd aan de beschrijving van het voorgenomen onderzoek, in 300 + 800 woorden (waarover later meer; wie ongeduldig is *en* voldoende bekwaam is in de aritmetische meetkunde kan ook direct door naar [6] en [3], die samen gezien kunnen worden als het ultieme wetenschappe-

lijke verslag van het project). In overleg met Fred Bakker werd de begroting opgesteld: vijf jaar mijn gehele eigen salaris, acht postdoc-jaren, twee promovendi en wat bijkomstighe-den als bezoekers, reiskosten, computers en software, een programmeur, en wat geld voor het populariseren van de wiskunde (denk aan steun voor de stichting Vierkant voor Wiskunde en het opzetten van een WIMS-mirror, zie [21]). De universiteit Leiden zorgde voor een ‘inbeddingsgarantie’, waarin ze beloofde de onderzoekslijn van het project structureel in te bedden in haar toekomstplannen. Het gaat hier om een blijvende stevige invloed van de subsidie. In mijn geval was dat niet zo moeilijk, want ik had immers al de hoogleraarsplaats gekregen, met daarbij de belofte twee UD/UHD-posities in te kunnen vullen.

Op 2 juli 2002 kreeg ik van Lex Zandee het goede nieuws dat ik werd uitgenodigd een uitgewerkt Vici-voorstel in te dienen: 300+8000 woorden dit keer. De deadline was 1 september 2002. Ik herinner me nog dat ik een flink aantal dagen in augustus, na de verhuizing naar Leiden, op het instituut aan de aanvraag heb gewerkt. Uiteindelijk was ik zeer tevreden met het resultaat. In die 8000 woorden had ik uitgelegd welk probleem aangepakt zou worden, waarom het een interessant probleem was, hoe het aangepakt zou worden, en waarom de kans van slagen groot was.

Daarna was NWO weer aan zet, met het raadplegen van adviseurs en verzamelen van de reacties van de kandidaten op de adviezen. Op 23 oktober 2002 kreeg ik van Petra de Bont de rapporten van vijf referenten, waarop ik binnen zes dagen diende te reageren. Het lezen van de vijf rapporten was een spannende ervaring. Gelukkig kon ik tevreden zijn met het resultaat. Alle vijf referenten beoordeelden de aanvraag als excellent, ze vonden de plannen interessant en de aanpak overtuigend. Er was voor mij geen reden om te reageren.

Het interview, wat ging er mis?

De volgende stap in de aanvraagprocedure was een interview van vijftig minuten van de overgebleven kandidaten met een commissie ingesteld door het gebiedsbestuur van Exacte Wetenschappen (EW) van NWO, waarin wiskunde, informatica, sterrenkunde en toen ook nog natuurkunde vertegenwoordigd waren. Direct na de interviews, die op een of twee dagen in november plaatsvonden, maakte deze commissie een ‘ranking’ van de kandidaten, zodat het algemene NWO-bestuur (geleid door de excellente, nu legendarische en wel-

haast mythische topeconoom Peter Nijkamp) de uiteindelijke beslissing kon nemen. (Hoe kan zo iemand als Nijkamp zo hoog terecht komen? Dateert zijn fraude al van voor zijn prijzen en benoeringen? Extra controle van bovenaf, en extra cursussen integriteit lossen dit probleem niet op — bestuurders, lezen jullie mee? De controle moet van collega’s uit het vakgebied zelf komen, daar zit de expertise. Laten vooral degenen die verantwoordelijk zijn voor zijn prijzen en benoeringen zich eens bezinnen op de vraag hoe dit alles heeft kunnen gebeuren. De schuld voor de misdrijven ligt natuurlijk bij Nijkamp zelf.)

Als voorbereiding werd er voor mij in Leiden een proef-interview georganiseerd. Daar kreeg ik veel nuttige maar uiteenlopende suggesties. Het echte interview verliep stroef. Eigenlijk liep het uit op een clash, maar dat besef drong pas na enige tijd door. Na al die jaren nu terugkijkend zie ik twee oorzaken. Zelf had ik het belang van het interview onderschat. Ik verkeerde teveel in de veronderstelling dat de commissie haar oordeel grotendeels op de CV’s en de rapporten van de referenten zou baseren, en dat het interview meer een soort ‘sanity check’ was (zo ging dat toen in Frankrijk). Gezien de uiterst positieve rapporten dacht ik niet dat een andere uitkomst dan toekenning mogelijk was. Maar zo gaat het dus niet. De commissie gaf haar eigen oordeel over de kandidaten meer gewicht dan ik toen dacht. Mijn presentatie, waarmee het interview begon, bestond teveel uit intimidatie met grote namen, prijzen, en wiskundige objecten dan op inhoudelijke overtuiging. Bijvoorbeeld noemde ik belangrijke resultaten van Faltings, Wiles, Lafforgue en Voevodsky zonder die concreet te maken. Er kwam geen ‘klik’ met de commissie. Aan de andere kant begon de voorzitter van de commissie, H.A.M. van Eekelen, een natuurkundige die voor Shell had gewerkt (of werkte), na de presentatie met mij te vragen waarom ik maar zo weinig citaties had (hij had zijn huiswerk gedaan, zei hij). Was de groep van wiskundigen met interesse in mijn werk misschien heel klein? Ik gaf hierop het weinig diplomatieke antwoord dat er wel degelijk veel wiskundigen in mijn werk geïnteresseerd waren, dat de referenten toch duidelijk overtuigd waren, en dat hij een fout maakte met zijn citatie-argument. Ook liet Van Eekelen blijken dat hij cryptografie niet belangrijk vond, en niet geloofde dat mijn onderzoek relevant zou kunnen zijn voor cryptografie.

Ongeveer een maand na het interview werd mij de uitslag van de procedure meegegeeld. Niet toegekend, dus. Ondanks de ne-

gatieve sfeer tijdens het interview, die ik zelf kennelijk grotendeels verdrongen had, was ik toch nog verbaasd, en kwaad.

Tussen twee aanvragen

Natuurlijk was het de bedoeling om de aanvraag nog een keer in te dienen. Maar een periode van afkoeling kon geen kwaad. Vandaar het besluit om een jaar over te slaan, in 2004 zou ik een tweede poging doen.

Nu ik zo’n duidelijk onderzoeksplan had liggen, maar nog geen promovendi en geen postdocs, begon ik er zelf alvast maar aan te werken. Aan zijn kant maakte Jean-Marc Couveignes vorderingen, dus ik was wel verplicht om ook aan mijn kant aan de kar te trekken. Een andere goede reden om te beginnen was om een voordracht over dit onderwerp voor te bereiden die ik in een workshop ‘Future directions in algorithmic number theory’ in Palo Alto zou gaan geven.

Bij een voordracht in het Nederlandse Intercity Number Theory Seminar in April 2003 liet Robin de Jong, toen promovendus bij Gerard van der Geer, zijn interesse en deskundigheid in het onderwerp blijken. In de drie maanden daarna maakten we samen een goed begin met het project, we bewezen een deelresultaat (Stelling 9.2.5 in [6]). Met dat resultaat in de hand werd het duidelijker wat er allemaal nog te doen was. Een van deze taken was het afschatten van zogenaamde Arakelov–Green-functies op Riemann-oppervlakken. Voor mijzelf was dit probleem te analytisch, dus benaderde ik Peter Sarnak. Hij gaf de vraag door aan Jay Jorgenson, die er vanaf januari 2004 aan ging werken, samen met Jürg Kramer in Berlijn. Ook sprak ik in december 2003 met Franz Merkl over dit probleem, hij was dat jaar postdoc in de statistiegroep in Leiden. Franz zei meteen dat hij wist hoe hij dit probleem kon oplossen. En inderdaad kwam hij in februari 2004 met een tekst die met weinig aanpassingen geworden is tot hoofdstuk 10 in [6]. Jorgenson en Kramer losten het probleem wat later ook op, op een andere manier. Voor mij betekende dit dat het laatste serieuze obstakel in mijn hele project was weggenomen, en was ik er zeker van dat ik de rest zou kunnen afmaken. Het bleef nog wel een meerjarenklus.

De tweede aanvraag, wel succes

Inmiddels was het 2004, dus tijd om opnieuw een aanvraag bij NWO in te dienen. De eerste keer had de mislukking niet aan het geschreven voorstel gelegen, dus dit keer had ik weinig werk. Ik diende het voorstel in zoals het was, met toevoeging van een beschrijving van

het werk dat sinds de eerste keer was gedaan, en met een verandering van de begroting. Dit laatste punt verdient wel enige uitleg, aangezien er een conflict van belangen was tussen die van de aanvrager en die van zijn instituut en universiteit. De totale omvang van het project was 1,25 miljoen euro, waarvan NWO 67 procent voor haar rekening nam, en de overige 33 procent moest worden ‘gematcht’ door de Universiteit Leiden. Dit soort matching is later afgeschaft. In mijn eerste aanvraag had ik 100 procent van mijn eigen salaris in de begroting van het project gezet. Doordat ik in de jaren 2002–2004 voor NWO in commissies had gezeten waar projecten werden beoordeeld, had ik ook ingezien dat projecten aantrekkelijker waren naarmate er meer uitkwam, bijvoorbeeld in aantallen opgeleide promovendi. Door mijn eigen salaris (de universiteit moest het toch al betalen) voor maar 40 procent in de begroting op te nemen, kwam er ruimte voor een derde promovendus. Ook was het natuurlijk niet realistisch dat ik 100 procent van mijn tijd in het project kon gaan steken: er moest immers ook onderwijs worden gegeven, en ik was een van de twee managing editors van *Compositio Mathematica*. Mijn begroting was kostenneutraal voor de universiteit (het salaris van Johan Bosman, die in juni 2004 als promovendus was begonnen, zat er ook in). Natuurlijk zou de universiteit van mijn project enorm profiteren in de vorm van extra promovendi, postdocs en activiteiten. Ik kreeg wel een telefoontje van het bestuursbureau met de vraag of er niet een promovendus minder kon, maar het was niet moeilijk om daar nee op te zeggen.

Ook deze keer werd ik uitgenodigd om een uitgewerkt voorstel in te dienen. Het resultaat daarvan is [19], nagenoeg identiek aan het voorstel uit 2002. NWO zocht en vond vijf nieuwe referenten. Vier van hen beoordeelden het project met ‘excellent’. Referent nummer 5 schreef: “As the above report clearly shows, for me this is THE most important work presently being done in explicit arithmetic geometry. I have no doubt that the authors will achieve at least part of their goals, and that it will be an important landmark on the subject. In addition, the cryptographic applications are immediately clear, even if they are not the main motivation for the research. I am surprised that an earlier proposal of the applicant was not accepted 2 or 3 years ago: of course the research was not as advanced as it is now, but I am sure that the referees must have been unanimous in saying that the potential of the work was outstanding. I give the highest possible marks to this proposal.”

Maar referent nummer 4 vond het maar niets dat ik voltijds zou werken aan computationele aspecten, want ik zou er mijn intuïtie voor ‘bona fide theorems’ mee verliezen. Ook vond hij of zij het maar niets dat ik wat samenwerking had met een bedrijf, Canon Recherche France, en met het Franse CELAR (Centre Electronique de l’Armement, een afdeling van het Franse ministerie van defensie). Hij ging ervan uit dat de in die samenwerking verkregen resultaten geheim zouden zijn. Zijn rapport eindigde aldus: “As far as I am concerned, I feel that Edixhoven is basically lost for number theory, and I cannot recommend him for your fellowship.”

Dit keer schreef ik dus wel een weerwoord. Ik schreef dat mijn project bijna geheel bestond uit het bewijzen van ‘bona fide theorems’, dat zijn conclusies over de bovengenoemde samenwerking die ik had, gebaseerd waren op onjuiste aannamen (in het contract voor de samenwerking stond bijvoorbeeld dat ik alle daarin door mij verkregen resultaten op mijn eigen homepage moest publiceren), en ik eindigde met: “Finally, to think that I would be lost for number theory just proves that this report cannot be taken seriously.”

Nu is het zo dat zo’n weerwoord niet naar de referenten gaat, maar naar de commissie die de kandidaten moet ‘ranken’. Die commissie moet dan beslissen of het weerwoord de bezwaren van de referent voldoende weerlegt. Maar als het een technische kwestie wordt, heeft ze vaak de daarvoor benodigde expertise niet (NWO-bestuurders, kan dit beter?).

Deze keer nam ik het interview serieuzer. Door mijn ervaring als lid van andere beoordelingscommissies snapte ik beter dat je als kandidaat op *inhoudelijke* zaken echt overtuigen moet zijn. Dat je de commissie moet overtuigen juist aan *jou* die enorme pot geld toe te kennen, door te laten zien dat zij *waar* voor haar geld krijgt door de *meerwaarde van het project* duidelijk te maken.

Het interview, dat aan het eind van de middag plaatsvond, begon met een presentatie van 25 minuten, waarvan de slides (voor overheadprojector, en inclusief aantekeningen voor mijzelf — tussen de slides) te vinden zijn in [20]. De sfeer was ontspannen. De voorzitter, Emile Aarts, heette mij hartelijk welkom. Ik had mij de hele dag mentaal zitten voorbereiden op mijn presentatie, die daardoor liep als een trein. Ik wist precies wat ik allemaal wilde zeggen, en het kwam er zo vloeiend uit dat ik adem tekortkwam. Daarna volgde de discussie, waarin de voorzitter begon met de mededeling dat ook de commis-

sie het rapport van referent nummer 4 terzijde had geschoven. Van de 25 minuten discussie herinner ik me weinig, behalve dat aan het eind er de vraag kwam, nu van Annejet Meijler (NWO, directeur gebied EW, met een achtergrond in de medische fysica), die ook bij het eerste interview aanwezig was geweest, waarom mijn werk relevant zou zijn voor de cryptografie. Kennelijk waren de twijfels van Van Eekelen toch nog blijven hangen. Nu had ik echter mijn antwoord klaar. Ik haalde even diep adem, ging *rustig* een aantal slides terug (naar slide 4, om precies te zijn) en liet zien dat het daar stond, en dat ik het had uitgelegd.

Na het interview volgde een spannende periode van wachten. De ranking van de commissie blijft natuurlijk een proces met een kans-aspect, want het is als appels en peren vergelijken. Er zijn veel aanvragen en maar weinig toekenningen, en je weet zelf niet wie je concurrenten zijn. Voor je eigen gezondheid is het dan maar beter om ervan uit te gaan dat je de subsidie *niet* krijgt. En dat is ook de meest realistische houding. Uiteindelijk kwam op 16 december 2004 het goede nieuws in de vorm van een email (normaal word je gebeld, maar ik was juist bij Couveignes in Toulouse) van Petra de Bont: bij EW (wiskunde, informatica en sterrenkunde; de natuurkunde was eruit gestapt) werden drie aanvragen gehonoreerd, en het mijne was daar één van.

De wiskunde dan, eindelijk; context

Nu kon ik medewerkers gaan aanstellen. De eersten waren Johan Bosman, die al promovendus was, en Robin de Jong die direct na zijn promotie als postdoc in dienst kwam. Ik had al twee andere promovendi, Gabor Wiese en Theo van den Bogaart, maar die werkten aan andere zaken. Met Peter Bruin en Arjen Stolk had ik twee heel goede kandidaten voor de overige twee promotieplaatsen. Zij moesten nog wel eerst afstuderen. Een voordeel daarbij was dat ze in hun afstudeerscripties al werden voorbereid op het latere werk.

Laten we dan nu eindelijk naar de *wiskunde* in het voorstel kijken. (NWO-medewerkers in EW en andere bèta-bestuurders: haak nu nog niet af! Als u het volgende niet groten-deels kunt begrijpen, bent u aan wat bijscholing toe. Er zijn vast wiskundigen in uw omgeving die u daar graag bij helpen, en zo niet, dan bent u welkom bij mij.) Eerst een schets van het landschap waarin het onderzoek plaatsvond: de algebraïsche meetkunde, en Grothendiecks étale cohomologie. Laat $n \geq 0$ een geheel getal zijn, en laat $X \subset \mathbb{C}^n$

de oplossingsverzameling zijn van een systeem van veeltermvergelijkingen met complexe coëfficiënten:

$$\begin{aligned} f_1(x_1, x_2, \dots, x_n) &= 0 \\ f_2(x_1, x_2, \dots, x_n) &= 0 \\ &\vdots \\ f_r(x_1, x_2, \dots, x_n) &= 0. \end{aligned}$$

Zulke deelverzamelingen van $\mathbb{C}^n$ heten *complex affien algebraïsch*. We zijn met name geïnteresseerd in de topologische eigenschappen van X , waarbij we X voorzien van de geïnduceerde topologie als deelverzameling van $\mathbb{C}^n$, die zelf de gebruikelijke (euclidische) topologie heeft. Een voorbeeld is de vergelijking $x_1 + x_2 = 0$; dan is de oplossingsverzameling X gelijk aan $\{(z, -z) : z \in \mathbb{C}\}$, een complexe lijn, dus homeomorf met $\mathbb{C}$. Een ander voorbeeld is de vergelijking $x_1^2 + x_2^2 = 0$, waarbij X gelijk is aan de vereniging van twee complexe lijnen die snijden in de oorsprong (want $x_1^2 + x_2^2 = (x_1 + ix_2)(x_1 - ix_2)$). Iets interessanter is de vergelijking $x_1^2 + x_2^2 = 1$, waarbij X homeomorf is met $\mathbb{C}$ minus één punt: schrijf de vergelijking als $(x_1 + ix_2)(x_1 - ix_2) = 1$, dan zie je dat de afbeelding $X \rightarrow \mathbb{C}$ die (a, b) naar $a + ib$ stuurt injectief is, met beeld $\mathbb{C} - \{0\}$. De inverse afbeelding stuurt t naar $((t + t^{-1})/2, (t - t^{-1})/2i)$, een continue afbeelding. Topologisch gezien is deze X interessanter dan de voorgaande, want deze X is niet samentrekbaar. Sterker, deze X is homotopie-equivalent met de cirkel S^1 .

Nog interessanter wordt het met vergelijkingen van de vorm $x_2^2 = x_1^3 + ax_1 + b$, met a en b in $\mathbb{C}$ complexe parameters (elliptische krommen!). Als de veelterm $x_1^3 + ax_1 + b$ geen meervoudige nulpunten heeft (hetgeen equivalent is met $4a^3 + 27b^2 \neq 0$), dan is X homeomorf met een torus ($S^1 \times S^1$) minus één punt. Dit is minder eenvoudig in te zien, maar al wel minstens 150 jaar standaardwiskunde (denk aan Gauss, Jacobi, Riemann, ...).

In het begin van twintigste eeuw hebben algebraïsch topologen (Henri Poincaré (intuïtief), onze eigen Luitzen Egbertus Jan Brouwer (precies)) voor alle topologische ruimten X cohomologiegroepen $H^j(X, \mathbb{Z})$ gedefinieerd, voor j in $\mathbb{Z}$ (die met $j < 0$ zijn nul). (Dit lijkt me een redelijk punt om even af te haken, voor degenen die niet het equivalent van een bachelor wiskunde hebben gedaan. Maar lees vooral weer door vanaf de voorlaatste paragraaf.) Deze groepen geven niet alleen interessante informatie over de topologische complexiteit van X , maar zijn ook nuttig

voor het tellen van vaste punten van continue afbeeldingen $f: X \rightarrow X$ via de spoorformule van Lefschetz (onder zekere voorwaarden op X en f).

Een van de mijlpalen in het werk van Alexander Grothendieck is een *algebraïsche definitie* van $H^j(X, \mathbb{Z}/m\mathbb{Z})$, voor $m \neq 0$ en j geheel, en $X \subset \mathbb{C}^n$ complex affien algebraïsch. Zelfs voor elliptische krommen X als hierboven kunnen cohomologiegroepen $H^1(X, \mathbb{Z})$ niet algebraïsch gedefinieerd worden. Als groep zijn al deze $H^1(X, \mathbb{Z})$ isomorf met $\mathbb{Z}^2$. Voor de kenner: neem X met 'complexe vermenigvuldiging', zie die cohomologiegroep als moduul over de endomorfismenring, de cohomologiegroep heeft dan een klasse in de Picard-groep van de endomorfismenring, deze klassen zouden dan behouden moeten zijn door automorfismen van $\mathbb{C}$ die de identiteit induceren op de endomorfismenring, quod non.

Wat is dat precies, in dit geval, een *algebraïsche definitie*? Het antwoord is: een definitie die compatibel is met algebraïsche isomorfismen. Dat betekent dat we moeten zeggen wat de algebraïsche isomorfismen zijn tussen complexe affiene algebraïsche X en Y . Welnu, terwijl ik dit schrijf, realiseer ik me ineens dat zelfs dat in eenvoudige termen uit te leggen is, zonder sjoemelen!

Voor $X \subset \mathbb{C}^n$ complex affien algebraïsch, laat $A(X)$ de verzameling van functies $f: X \rightarrow \mathbb{C}$ zijn, die de beperking tot X zijn van complexe veeltermfuncties op $\mathbb{C}^n$. Deze verzameling $A(X)$ is gesloten onder het puntsgewijs optellen en vermenigvuldigen van functies: het is een commutatieve ring, met een eenheidselement, namelijk de constante functie met waarde 1. Ieder element x van X geeft een evaluatie-afbeelding $\text{ev}_x: A(X) \rightarrow \mathbb{C}$, $f \mapsto f(x)$. David Hilbert liet al zien (zijn Nullstellensatz) dat de kernen van deze evaluatie-afbeeldingen precies de maximale idealen van $A(X)$ zijn (de afbeelding $x \mapsto \ker(\text{ev}_x)$ is een bijectie tussen de betreffende verzamelingen). Dus als verzameling kunnen we X terugvinden uit $A(X)$.

Voor $X \subset \mathbb{C}^n$ en $Y \subset \mathbb{C}^m$ complex affien algebraïsch, is dan een algebraïsch isomorfisme van X naar Y hetzelfde als een isomorfisme van ringen van $A(Y)$ naar $A(X)$. Wat Grothendieck heeft laten zien (met veel medewerking van Michael Artin), is dat er voor ieder geheel getal $m \neq 0$ en ieder geheel getal j een functor is van ringen naar abelse groepen, $A \mapsto H_{\text{et}}^j(A, \mathbb{Z}/m\mathbb{Z})$, zodat voor X complex affien algebraïsch $H_{\text{et}}^j(A(X), \mathbb{Z}/m\mathbb{Z})$ hetzelfde is (isomorfisme van functoren...) als de door de topologen gedefinieerde $H^j(X, \mathbb{Z}/m\mathbb{Z})$. Voor

de volledigheid is het goed te melden dat Grothendieck zijn functor definieerde (hoe kan het ook anders) voor *willekeurige ringen*. En eigenlijk is die definitie tegenwoordig geen verrassing meer; zozeer zijn Grothendiecks technieken gemeengoed geworden. Wat wel verrassend is, is dat die definitie redelijke resultaten oplevert (dat was het werk met Artin).

Laten we nu eens kijken naar de automorfismen van $\mathbb{C}$. Let wel, dit gaat om automorfismen van $\mathbb{C}$ als *lichaam*, we moeten (en dat is voor iemand die dat voor het eerst doet niet zo makkelijk) de topologie van $\mathbb{C}$ vergeten. De enige continue automorfismen van $\mathbb{C}$ zijn de identiteit en de complexe conjugatie (makkelijke opgave voor eerstejaars studenten). Laten we nu degenen die denken dat e en π speciale getallen zijn eens wat plagen. De getallen e en π zijn beide transcendent over $\mathbb{Q}$ (Hermite, Lindemann), dus zijn er (transcendentiebases, Zorn...) automorfismen σ en τ van $\mathbb{C}$ met $\sigma(\pi) = e$ en $\tau(e) = \pi$. Dus voor een algebraïcus zijn e en π niet verschillend. Het schijnt niet bekend te zijn of men τ en σ aan elkaar gelijk kan nemen. Men verwacht dat e en π algebraïsch onafhankelijk over $\mathbb{Q}$ zijn, en dan is $\sigma = \tau$ mogelijk.

De cruciale opmerking is nu dat ieder automorfisme σ van $\mathbb{C}$ een algebraïsch isomorfisme geeft van X , oplossingsverzameling van $f_1, \dots, f_r$, naar $\sigma(X)$, de oplossingsverzameling van $\sigma(f_1), \dots, \sigma(f_r)$ (pas σ toe op de coëfficiënten van $f_1, \dots, f_r$), als volgt. Voor $(a_1, \dots, a_n)$ in $\mathbb{C}^n$ is het nul zijn, voor alle j , van $f_j(a_1, \dots, a_n)$, equivalent met het nul zijn, voor alle j , van $\sigma(f_j(a_1, \dots, a_n)) = \sigma(f_j)(\sigma(a_1), \dots, \sigma(a_n))$. Kortom, σ coördinaatsgewijs toepassen geeft een bijectie tussen X en $\sigma(X)$, en een isomorfisme van ringen $A(\sigma(X)) \rightarrow A(X)$, $h \mapsto \sigma^{-1} \circ h \circ \sigma$.

Laten we vanaf nu aannemen dat alle coëfficiënten van alle f_j in $\mathbb{Q}$ liggen. Dan is $\sigma(X)$ gelijk aan X , en $A(\sigma(X))$ is gelijk aan $A(X)$. We concluderen dat de automorfismengroep van $\mathbb{C}$ werkt op alle $H^j(X, \mathbb{Z}/m\mathbb{Z})$. Dit heet de *Galois-actie* van $\text{Aut}(\mathbb{C})$, en het maakt de cohomologiegroepen tot zogenaamde *Galois-representaties*.

Laten we dit concreet maken. Voor iedere X , m en j is $H^j(X, \mathbb{Z}/m\mathbb{Z})$ eindig, en is er een polynoom f in $\mathbb{Q}[t]$, en een bijectie b tussen $H^j(X, \mathbb{Z}/m\mathbb{Z})$ en de verzameling nulpunten van f in $\mathbb{C}$, die compatibel is met de Galois-acties aan beide kanten: voor alle elementen h van $H^j(X, \mathbb{Z}/m\mathbb{Z})$ en voor alle σ in $\text{Aut}(\mathbb{C})$ geldt dat $b(\sigma(h)) = \sigma(b(h))$. Echter, in niet-triviale gevallen is het meestal ongelooflijk moeilijk om zo'n f te vinden. Voorbeelden

van triviale tot conceptueel niet zo erg moeilijke gevallen zijn:

- die waar $H^j(X, \mathbb{Z}/m\mathbb{Z})$ cyclisch is (rang één motieven),
- die waar $j = 0$,
- die waar X een rationale of elliptische kromme is (gebruik delingspolynomen),
- die waar X een Riemann-oppervlak van begrensd geslacht minus een eindig aantal punten is (in dit geval kijken we naar een oneindige rij van X^n en),
- die waar het beeld van de Galois-representatie (een eindige groep) oplosbaar is (geïtereerde klasselichamentheorie).

De wiskunde, het project

Het project bestond eruit om het vinden van een f zoals aan het eind van de vorige sectie in het eenvoudigste niet-triviale geval aan te pakken: het geval van rang twee motieven, dat wil zeggen, Galois-stabiele ondergroepen van $H^j(A, \mathbb{Z}/m\mathbb{Z})$ die als commutatieve groep isomorf zijn met $(\mathbb{Z}/m\mathbb{Z})^2$, waar f dus graad m^2 heeft. Sinds werk van Hecke, Eichler, Shimura, Deligne (ongeveer van 1920 tot 1970) en nog veel anderen is het bekend dat modulaire vormen (we gaan dit begrip nu niet uitleggen) een bron zijn voor dit soort Galois-representaties. En sinds het werk van Khare-Wintenberger en Kisin (en veel werk dat daar weer aan ten grondslag ligt, denk aan Wiles en Taylor, en laten we Fontaine en ook Serre niet vergeten) weten we precies welke tweedimensionale Galois-representaties van modulaire vormen komen: de determinant van de actie van complexe conjugatie moet -1 zijn.

Kort samengevat heeft het project opgeleverd dat zulke f komend van modulaire vormen, berekend kunnen worden in een rekentijd begrensd door een vaste macht van de som van m , het 'gewicht' en het 'niveau' van f . Het geval van niveau 1 is in groot detail opgeschreven in [6]. Peter Bruin generaliseerde het in zijn proefschrift [3] naar algemenere niveaus (Ariyan Javanpeykar bewees de nodige afschattingen in Arakelov theorie voor *alle* niveaus in zijn proefschrift [7]). Arjen Stolk begon met een analoog geval: functioneel lichamen, maar de klus was groter dan redelijk. Onder begeleiding van Joost Batenburg en in mindere mate van mij paste hij zijn verworven kennis in de algebra toe op de discrete tomografie in [13].

Naast de net genoemde theoretische resultaten over de asymptotiek van de rekentijd zijn er in 2004–2008 ook echte berekeningen gedaan door Johan Bosman, zie hoofdstukken 6 en 7 van [6], en ook zijn proefschrift [1]. Zie vooral ook zijn eigen verslag [2] in dit tijd-

schrift. Kort geleden zijn Johans berekeningen uitgebreid door Nicolas Mascot, een promovendus van Couveignes, in [10] en [11]. En ook door Maarten Derickx, Mark van Hoeij en Jinxiang Zeng, en Peng Tian: zie [4], [16], en [14].

Grothendiecks algebraïsche definitie van $H^j(X, \mathbb{Z}/m\mathbb{Z})$ voor $j > 1$ is niet geschikt om direct ermee te kunnen rekenen, laat staan er *snel* mee te kunnen rekenen. Standaardtechnieken uit de étale cohomologie maken het mogelijk om berekeningen te reduceren naar gevallen met $j = 1$, en uiteindelijk ook $j = 0$, waarin Grothendiecks definitie *wel* geschikt is om mee te rekenen. Maar de prijs die daarvoor wordt betaald is een toename van de dimensie van X met een factor ongeveer gelijk aan m^2 in de gevallen die in het project bestudeerd werden. Exacte berekeningen (computer algebra) van oplossingen van stelsels veeltermvergelijkingen in zoveel variabelen kosten een rekentijd die exponentieel in m groeit (dit is een manifestatie van de 'curse of dimensionality'). Hier had Couveignes het idee om numeriek te werken, met een voldoende grote precisie zodat de gezochte f exact bepaald kon worden. Inderdaad zijn de coëfficiënten van dergelijke f rationale getallen, dus van de vorm a/b met a en b geheel en onderling ondeelbaar. Als men een a priori bovengrens kent voor $|a|$ en $|b|$, zeg M , dan is een benadering x (reëel, zeg) van a/b met $|x - a/b| < 1/(2M^2)$ voldoende om a/b uit te bepalen.

Couveignes' idee splitst dan het probleem in twee deelproblemen. Het eerste is om te laten zien dat de aantallen cijfers van tellers en noemers van de coëfficiënten van de f niet harder groeien dan een vaste macht van m . Dit is uitgevoerd door Robin de Jong en mij, gebruikmakend van Franz Merkl's bovengrenzen voor Greense functies (hoofdstukken 8–11 in [6]). Het tweede deelprobleem is te laten zien dat de benaderingen met de nodige precisie uitgerekend kunnen worden in rekentijd die niet harder groeit dan een vaste macht van m . Dat is uitgevoerd door Couveignes (hoofdstukken 5, 12 en 13 van [6]). Hij behandelt daar benaderingen met complexe getallen, maar ook benaderingen met behulp van veel eindige lichamen. Peter Bruin generaliseerde die laatste methode in zijn proefschrift en ook het begrenzen van de benodigde precisie. Alles samengevoegd hebben we op die manier de 'curse of dimensionality' overwonnen, door hem te omzeilen.

Kort geleden, zie [12] en [9], is aangetoond dat, ook voor $j > 1$, $H^j(X, \mathbb{Z}/m\mathbb{Z})$ inclusief Galois-actie berekenbaar is. Maar de technieken die daar gebruikt worden, berusten op af-

tellen van alle mogelijkheden in aftelbare verzamelingen, dus redelijke bovengrenzen voor de rekentijd zijn nog ver te zoeken. Jinbi Jin werkt in Leiden aan directere technieken.

Tastbare gevolgen

Coëfficiënten van modulaire vormen komen veel voor in oplossingen van telproblemen. Eenvoudige telproblemen leiden tot machtsfuncties, of binomiaalcoëfficiënten, en lineaire combinaties en multiplicatieve combinaties daarvan, en de bijbehorende genererende functies zijn dan rationale functies, algebraïsche functies, of hypergeometrische functies. Het volgende niveau van moeilijkheid leidt dan tot modulaire vormen en hun coëfficiënten. Natuurlijk zijn er ook weer moeilijkere telproblemen. In ieder geval is het zo dat het hier besproken Vici-project de berekening in polynomiale tijd van coëfficiënten van modulaire vormen mogelijk heeft gemaakt, door, behalve de interne symmetrie van de modulaire vormen zelf, óók de symmetrieën in de getaltheorie te gebruiken (Galois-representaties). Voor een hele klasse van telproblemen kan (in theorie) het antwoord nu heel snel worden uitgerekend.

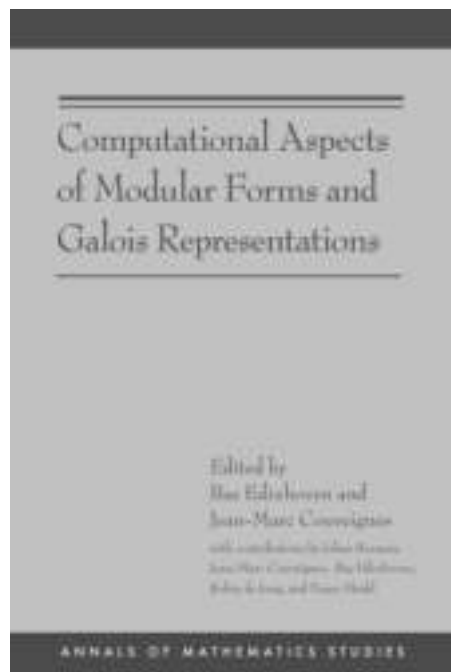
Laat ik hier twee voorbeelden geven, die beide als mijlpalen bekend staan: aantallen punten in $\mathbb{Z}^{2n}$ op gegeven afstand van de oorsprong, en Ramanujans τ -functie. Het eerste voorbeeld wordt in meer detail behandeld in [5], van waaruit ik me nu ga bezondigen aan een beetje zelfplagiat, en het tweede in [2].

Het eerste probleem dan. Voor $d \geq 0$ en $n \geq 0$ geheel, laat $r_d(n)$ het aantal punten $(x_1, \dots, x_d)$ in $\mathbb{Z}^d$ zijn met $x_1^2 + \dots + x_d^2 = n$, dat wil zeggen, het aantal punten waarvan het kwadraat van de afstand tot $(0, \dots, 0)$ gelijk is aan n .

Beroemde wiskundigen zoals Diophantus, Fermat, Legendre, Gauss, Jacobi, Eisenstein en Liouville hebben voor d gelijk aan 2, 4, 6, 8 of 10 formules gegeven waarmee deze aantallen snel berekend kunnen worden. Daarna is zonder succes geprobeerd dit uit te breiden naar grotere even getallen. Door ons werk begrijpen we nu dat er dan geen dergelijke formules meer bestaan (zie [15]), maar dat de gezochte aantallen *toch* snel kunnen worden uitgerekend. Even snel als wanneer de formules *wel* hadden bestaan. Een algoritmische kijk op dit probleem geeft dus een bevredigender antwoord.

Het tweede probleem. We bekijken het oneindig product

$$x \prod_{n \geq 1} (1 - x^n)^{24} = \sum_{n \geq 1} \tau(n) x^n.$$



Omslag van het boek dat uit het project is voortgekomen [6]

De zo gedefinieerde functie $\tau: \mathbb{N} \rightarrow \mathbb{Z}$ is bekend als Ramanujans τ -functie. De bovenstaande machtreeks is een typisch voorbeeld van een niet-triviale modulaire vorm. In [6] is bewezen dat voor priemgetallen p , men $\tau(p)$ kan uitrekenen in een tijd begrensd door een vaste macht van $\log(p)$. Daarvóór was de benodigde rekentijd minstens een positief getal keer $p^{1/2}$.

Eindsituatie, aanbevelingen, dank

De belangrijkste van de in de aanvraag beoogde resultaten zijn behaald. De beoogde aanpak heeft gewerkt. Ik ben bijzonder trots op de

publicatie van de resultaten in [6], in de prestigieuze boekenreeks *Annals of Mathematics Studies*, waaraan dit de eerste Nederlandse bijdrage is (zie [18]). In Leiden is er nu een sterke groep voor onderzoek en onderwijs in de algebraïsche en aritmetische meetkunde, getaltheorie en algebra. Dit laatste is niet alleen te danken aan het Vici-project, denk bijvoorbeeld ook aan het Akademiehoooglerarschap van Hendrik Lenstra, de Veni's van Robin de Jong, Lenny Taelman en Peter Bruin, de Vidi van Ronald van Luijk, en aan promovendi, studenten en bezoekers gefinancierd door de Erasmus Mundus master- en PhD-programma's 'ALGANT'. Het gaat goed met het Mathematisch Instituut in Leiden als geheel. De nabije toekomst ziet er florissant uit. Op de langere termijn is de belangrijkste vraag of de vaste staf mee kan groeien. Voor een goed onderwijsprogramma is dat zeker nodig.

Heeft het project mijn status verhoogd? Buiten Nederland niet, denk ik, maar binnen Nederland waarschijnlijk wel, en dan met name buiten de wiskunde, want binnen de wiskunde weten we zelf meestal wel wat iemand waard is. In dit themanummer van het NAW staan veel mooie zaken die bereikt zijn door succesvolle Vernieuwingsimpuls-kandidaten. Het is dan verleidelijk te concluderen dat het programma goed heeft gewerkt. Maar om *echt* te evalueren moet je het vergelijken met wat degenen die *niet* succesvol waren hebben bereikt, en met wat ze misschien zouden hebben bereikt als ze succesvol waren geweest.

Graag eindig ik met wat gedachten over de huidige trend in subsidieerland, voor zover het de wiskunde betreft. Die trend is om steeds

grotere subsidievormen op te zetten, waarbij natuurlijk steeds minder projecten gehonoreerd kunnen worden. Dit verstoort het hele ecosysteem. Maar als dat dan toch moet, dan pleit ik voor maar één project in de wiskunde in Nederland, namelijk de wiskunde zelf, als geheel. Dat heeft het bijkomende voordeel dat er geen selectie meer hoeft plaats te vinden bij NWO. De wiskundegemeenschap in Nederland is prima in staat om zelf het geld te verdelen, en daarvoor verantwoording af te leggen. De globale verdeling van de middelen van NWO over de verschillende wetenschapsgebieden kan gedaan worden in een jaarlijks overleg tussen uit de wetenschapsgebieden afgevaardigde wetenschappers (laat vooral ook de universiteitsbestuurders erbij, het moet om de wetenschap gaan). Mijn gevoel is dat zo'n systeem betere resultaten zal opleveren dan wat er nu is: directeuren en politici die zich laten adviseren door 'beleidswetenschappers' (dat *is* geen wetenschap). In een groter en meer direct overleg zoals ik voorstel komen de grootverbruikers van NWO-middelen directer in confrontatie met de kleinere maar meer talrijke en ook meer diverse gebruikers, waarvoor ik zelf meer sympathie heb.

Leest u vooral ook Klaas Landsmans artikel [8] in het vorige nummer van dit tijdschrift over de problematiek van de financiering van wetenschappelijk onderzoek. Ik ben het van harte met hem eens!

Ten slotte dank aan NWO voor de subsidie die me is toegekend, en aan mijn medewerkers voor hun bijdragen aan het project, en voor de fijne tijd die ze me hebben gegeven. 

Referenties

- J.G. Bosman, *Explicit Computations with Modular Galois Representations*, proefschrift, Universiteit Leiden, 2008, online onder [17].
- J.G. Bosman, Modulaire vormen en berekeningen in Galoistheorie, *Nieuw Archief voor Wiskunde* 5/9(3) (2008), 184–187.
- P.J. Bruin, *Modular Curves, Arakelov Theory, Algorithmic Applications*, proefschrift, Universiteit Leiden, 2010, online onder [17].
- M. Derickx, M. van Hoeij en Jinxiang Zeng, Computing Galois representations and equations for modular curves $X_H(\ell)$, arxiv.org/abs/1312.6819.
- S.J. Edixhoven, Snelle algoritmen in de getaltheorie, Vacantiecursus PWN/CWI, 2011, pub.math.leidenuniv.nl/~edixhovensj/talks/2011/2011-08-26.vacantiecursus/text.pdf.
- S.J. Edixhoven en J.-M. Couveignes, eds., *Computational Aspects of Modular Forms and Galois Representations*, met bijdragen van Johan Bosman, Jean-Marc Couveignes, Bas Edixhoven, Robin de Jong en Franz Merkl, *Annals of Mathematics Studies*, Vol. 176, Princeton University Press, 2011, www.math.u-bordeaux1.fr/~jcouveig/book.htm; versies 1 en 2 op arxiv.org/abs/math/0605244 hebben een interessant 'personal historical account'.
- A. Javan Peykar, *Arakelov Invariants of Belyi Curves*, proefschrift, Universiteit Leiden, 2013, online onder [17].
- N.P. Landsman, Wetenschap en welvaart, een paradoxaal krachtenveld, *Nieuw Archief voor Wiskunde* 5/15(2) (2014), 89–95.
- D. Madore en F. Orgogozo, Calculabilité de la cohomologie étale modulo ℓ , arxiv.org/abs/1304.5376.
- N. Mascot, Computing modular Galois representations, arxiv.org/abs/1211.1635.
- N. Mascot, Tables of modular Galois representations, arxiv.org/abs/1312.6418.
- B. Poonen, D. Testa en R. van Luijk, Computing Néron-Severi groups and cycle class groups, arxiv.org/abs/1210.3720.
- A.P. Stolk, *Discrete Tomography for Integer-Valued Functions*, proefschrift, Universiteit Leiden, 2011, online onder [17].
- P. Tian, Computations of Galois representations associated to modular forms of level one, *Acta Arithm.* 164 (2014), 399–411.
- I. Varma, Finding elementary formulas for theta functions associated to even sums of squares, *Indag. Math. (N.S.)* 22 (2011), 12–26, www.math.leidenuniv.nl/nl/theses/196.
- J. Zeng en L. Yin, On the computation of coefficients of modular forms: the reduction modulo p approach, arxiv.org/abs/1211.1124.
- openaccess.leidenuniv.nl.
- press.princeton.edu/catalogs/series/am.html.
- pub.math.leidenuniv.nl/~edixhovensj/FormVlCldetail.2004.pdf.
- pub.math.leidenuniv.nl/~edixhovensj/talks/2004/vicipres2.pdf.
- wims.math.leidenuniv.nl/wims.
- www.msri.org/realvideo/ln/msri/2000/arithgeo/edixhoven/1/index.html

Ronald Meester

*Department of Mathematics
Vrije Universiteit Amsterdam
r.w.j.meester@vu.nl*

Research Vici project

Longe range stochastic dynamics

In the Vici project ‘Longe range stochastic dynamics’ Ronald Meester and his team worked on sandpile models and the Bak–Sneppen model. In this article Meester describes these two systems. However, their research was certainly not restricted to these two subjects. They also investigated dependent percolation models with long range interactions, models for forest fires, invasion percolation, self-destructive percolation, divide and colour models, and more.

If I remember correctly my own Vici story began with Jan van Mill stepping into my office with the Vici call in his hands, simply saying: “Ronald, I think this is something for you.”

And well, yes, it was something for me. Applying for so much money of course required a big and ambitious program. Although I had been (and still am) interested in many other things as well, it was rather obvious that such a big and ambitious program should centre around some aspect of spatial random processes. Much of my research until that point had been devoted to percolation theory in a classical, continuum, and fractal setting. Percolation theory is also of obvious interest to many theoretical physicists and as such it was not unusual for me to participate in conferences where mathematicians and physicists actually talk to each other. As such, I had come across the notion of so called ‘Self-Organised Criticality’ (SOC). The phrase was coined by physicists like Per Bak, and referred in some vague sense to models that behaved

as classical systems (like percolation) at the critical point, but without any tuning of parameters.

Let me elaborate on this point. Suppose you take classical percolation on the d -dimensional lattice $\mathbb{Z}^d$, which means that every nearest neighbour bond is retained with probability p , and deleted with probability $1 - p$. For small values of p , all connected components of the resulting graph will be finite, while for large p , infinite components will arise (in fact, at most one infinite component will be formed but this is not important for my purposes here). In the former case, spatial correlations decay exponentially fast, while in the latter case, correlations do not decay to zero at all. It is precisely at the critical value for p , denoted by p_c , which separates the two regimes, where the correlations do decay, but according to a power law, rather than exponentially fast. Hence, power law behaviour is associated with criticality, and in this example, p must be tuned to p_c precisely

in order to observe this power law behaviour. (How much of this can be demonstrated rigorously is another matter, I will not go into that direction here.)

In many physical, ecological and biological systems, power law behaviour is observed, but apparently without any tuning parameter. The systems ‘organise’ themselves into this apparent critical behaviour, hence the name Self-Organised Criticality. Examples are models for earthquakes, avalanches, evolutionary systems, forest fires and many more. For instance, when you plot the energy released in an earthquake versus the frequency of occurring, you will observe a power law, the basis for Richter’s scale.

Much of this is rather attractive from a physics point of view, and there are many, many publications in the physics literature describing systems that are supposedly self-organised critical in the above, rather vague sense. For mathematicians, there are other things at stake. Even the precise mathematical formulation of some of these concepts is rather unclear, let alone proving them. This is not to say that the models that were introduced by the physicists would not be interesting from a mathematical point of view. In fact, they are very interesting, exactly because of

the fact that standard and classical methods seem to break down completely. In my Vici project, I took up the challenge to study some of these models. I already had some experience with some of them, and the Vici project seemed a very good opportunity to carry this further. The project was certainly not restricted to sandpiles and the Bak–Sneppen model: we also investigated dependent percolation models with long range interactions, models for forest fires, invasion percolation, self-destructive percolation, divide and colour models, and more. The general nature of the project was reflected in the title: ‘Long range stochastic dynamics’. This encompasses a lot, and I thought it wise not to restrict myself too early.

In this article, I will of course not be able to discuss all the work done in the project. I will therefore restrict myself to two specific systems, namely sandpile models and the Bak–Sneppen model, which are easy to explain and hopefully interesting for a broader audience.

The Abelian sandpile model

The Abelian sandpile model (ASM) is a finite state discrete time Markov process, supposed to model avalanches. It is defined on a finite connected subset Λ of $\mathbb{Z}^d$. It starts with a so called *configuration*, that is, every site in Λ contains a non-negative integer-valued number of particles, or *sand grains*. This number is typically called the *height* of the site. A site is *stable* if its height is at most $2d - 1$. When all sites in Λ are stable we call the configuration stable. The state space of the Markov chain is the collection of stable configurations. The dynamics is as follows. We start with a stable configuration. Every discrete time step, an addition of one sand grain is made to a randomly chosen site. If this site becomes *unstable*, i.e., it has at least $2d$ grains, it *topples*, that is, it simply gives one grain to each neighbour. Hence the height of the toppled site decreases by $2d$, and the height of each of its neighbours increases by 1. When a site at the boundary of Λ topples, then the number of neighbours may be less than $2d$. This simply means that the corresponding grains leave the system. This is not the end of a time step, because the resulting configuration may not be stable. Indeed, a toppling may cause a neighbouring site to become unstable. Hence, we continue with toppling unstable sites until every site is stable again. The total of all necessary topplings is called an *avalanche*. After the avalanche we have reached the new configuration, and this

finishes one time step of the Markov process.

It is not hard to see that a new stable configuration is reached after finitely many topplings. It is also not very difficult to show that the order in which topplings are executed has no effect on the final stable configuration. Although not too difficult, this simple fact already caused some discussion between the mathematical and the physics community. The physicists insisted that it was enough to observe that if you perform two topplings, one at site x and one at site y , then the order in which you do this does not matter, hence the name *Abelian* sandpile model. However, this obviously does not settle the issue, because you have to prove that when you topple x first, say, then the collection of sites that topples until stabilization, is the same as when you topple y first. I am not sure I have been able to convince my physics friends on this issue.

This sandpile model is said to exhibit self-organised critical behaviour, for the following reason. As the model evolves in time, it reaches a stationary distribution that is characterized, in the large-volume limit, by long-range height correlations and power law statistics for avalanche sizes. What I mean by this is that when Λ is large, it seems that the probability to observe an avalanche which involves at least k sites, decays with a power law in k , and similarly for the number of topplings of a randomly chosen avalanche (this must be made precise of course). As indicated above, this reminds one of critical behaviour in statistical mechanical models, like percolation. In percolation, one sees power law behaviour of cluster sizes only at the critical point, so one must choose parameters very, very carefully in order to observe this. For the sandpile however, it seems that this is achieved in a natural way, without apparent tuning of any parameters. Hence the model organises itself into behaviour which is associated with criticality, hence the name SOC.

One may wonder whether or not this mathematical model is suitable for describing anything which looks like a real avalanche. Indeed, isn't it more natural to let height *differences* decide whether or not an avalanche takes place? I would say yes, but the problem is that a sandpile model based on height differences is a lot more difficult to study since it is not Abelian. As a result, very little has been done in this direction.

Preceding my Vici project, I had already worked on the ASM with Dmitri Znamenski, a PhD student, and Frank Redig. Among other things, we had written a paper in which we

gave rigorous proofs of various claims by the physicist.

The Bak–Sneppen model

The Bak–Sneppen model was originally introduced as a very simple model for evolution by Per Bak and Kim Sneppen [2]. I had already worked on it with Dmitri Znamenski in the years preceding the Vici grant. The model is as simple as one can imagine, but at the same time very difficult to study in a rigorous mathematical way. It is defined as follows. Let N vertices (‘species’) be arranged regularly on a circle, and denote this structure by Λ_N . Assign a *fitness* to each vertex, that is, independent random variables, uniformly distributed on $(0, 1)$. At each discrete time step the system is updated by locating the vertex with the lowest fitness and replacing this fitness *and those of its two neighbours* by independent and uniform $(0, 1)$ random variables. The Bak–Sneppen model is again a discrete time Markov process. In some vague sense, the dynamics should remind us of evolutionary processes in which species with the lowest fitness disappear. Other species which somehow depend on the one with lowest fitness, run into trouble then, hence the rule that also neighbours obtain new fitnesses.

This neighbour interaction makes this model very interesting but also very difficult. One may wonder why this model is interpreted as a model for SOC. The reason for this is that one can define *avalanches* in a very natural way, as follows. An *avalanche at threshold* $0 < b < 1$ (also called a *b-avalanche*) is said to occur between times s and $s + t$ if at time s all the fitnesses are equal to or greater than b , and time $s + t$ is the next time after s at which this occurs. Note that if we have a minimum fitness value of b , then we can choose any value up to (and including) b to be our avalanche threshold. Furthermore, it is the threshold and not the exact initial values of the model that determines the behaviour of an avalanche. Once we have used the initial fitnesses to find out the minimal fitness and its location, all other information can be discarded for the purposes of analysing individual avalanches.

The notion of an avalanche helps to explain the self-organised critical nature of the model. Indeed, when b is small, avalanches appear to be (exponentially) short, both in the time of duration as in the number of sites involved. When b is large, avalanche durations are not uniformly bounded in the system size N . The critical threshold b_c is the threshold values separating these two

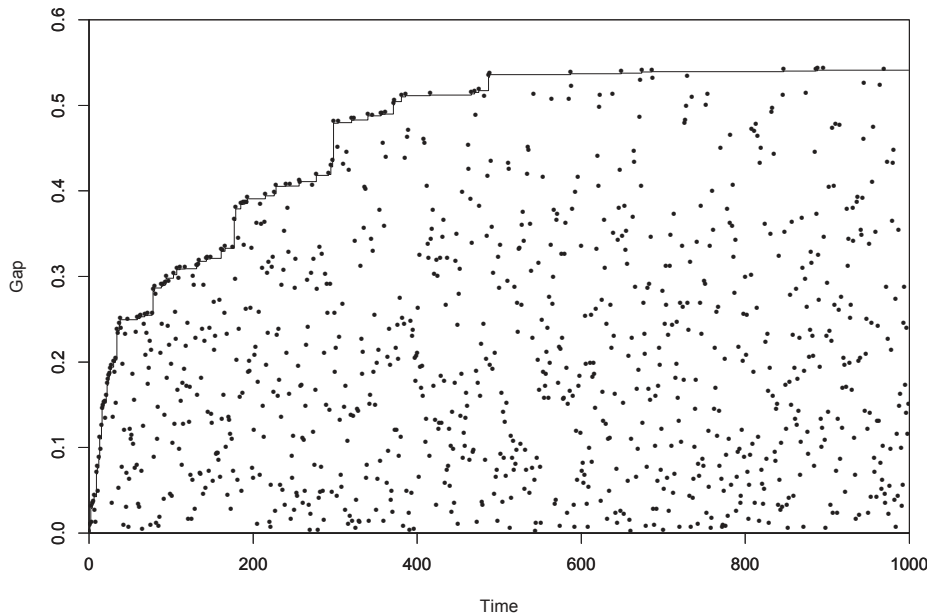


Figure 1 A snapshot of the Bak-Sneppen model in stationarity.

regimes. Running the model on a computer (this is really simple; I do not think that there are many models which are so simple to describe, and at the same time so deep from a mathematical point of view) there seems to be a threshold b_c , close to $\frac{2}{3}$, such that after a while, the dynamics appear to consist of consecutive avalanches at b_c , and in addition, these avalanches seem to exhibit power law behaviour in the sense that both duration and range can be described by power laws [2]. The threshold b_c is not set beforehand; the model seems to organise *itself* into this state. See Figure 1 for a typical snapshot of the Bak-Sneppen model in stationarity, with $N = 300$. On the horizontal axis we have the 300 vertices, with the dots representing the fitnesses of the vertices.

Some philosophical issues

I will discuss some progress in understanding these models later. Before that, it is perhaps interesting to elaborate on the claim that these processes indeed organise themselves into a critical state. How self-organised are these systems, really? And how realistic is the implicit or explicit claim that power law behaviour in spatial or temporal quantities can or should be interpreted as being the result of self-organised criticality? Power law behaviour is abundant, and probably for a variety of reasons. In this connection it is useful to read Per Bak's book *How nature works* on the subject. The title of the book of course already gives away what seems to be at stake: self-organised criticality as the leading principle in many physical, ecological and

biological processes. Ignoring the obvious self-satisfaction displayed by Bak, reading his book it is hard to avoid the conclusion that they had great difficulties to formulate a model which in fact showed power law behaviour as desired. Especially the description of the Bak-Sneppen model did not come for free. Isn't this careful formulation in itself slightly at odds with the claim that everything goes 'by itself'? One has to define a model very cautiously in order to see critical behaviour. The tuning of parameters has been replaced by careful selection of the model, perhaps. In addition, claiming that SOC is the way nature works is claiming that a power law behaviour can be explained by SOC which, in my opinion, is not well founded. When you have a hammer, everything looks like a nail.

There have been philosophical attempts to explain the fact that sandpile models behave like a critical classical system. These attempts involve the definition of parametrized sandpiles in infinite volume, and since we will need this later anyway, this is the right moment to introduce them.

Consider the Abelian sandpile described above, but this time in infinite volume, let us say on $\mathbb{Z}$. In this situation, we cannot choose a site uniformly any more. Hence, this system has no additions, only topplings. Starting from an initial configuration of heights, one step of the ensuing Markov process is to simply topple all unstable sites once. In this context, the question is whether or not the configuration converges (in the usual product topology) to a limiting configuration. Clearly this depends on the initial configuration, and

in order to formulate this as a classical parametric model, we let the heights in the initial configuration be distributed as independent Poisson- ρ random variables. In this set-up, we expect a phase transition in ρ : when ρ is small, not many sand grains are present, and probably all motion will stop locally after a transient period, that is, all sites topple only finitely many times. If ρ is large, then there is no limiting configuration since there will not be enough space to accommodate all particles in a stable way, that is, all sites will topple infinitely many times. The critical point of this system separating the two regimes is denoted ρ_c ; the similarity between this critical density and the critical probability p_c in percolation is clear.

With this infinite volume model in place, we can look at the connection between the original Abelian sandpile and this infinite-volume system. In a widely cited series of papers [6–7, 23, 25–26], Dickman, Muñoz, Vespignani and Zapperi developed the following heuristic argument. If the density of particles in the finite volume system is larger than ρ_c , one 'typically' should have topplings, and as a result particles might leave the system. If this density of particles is smaller than ρ_c , then 'typically' one should only have addition of particles. Hence the density of particles should always change in the direction of ρ_c and therefore the finite volume sandpile resides, when the volume is large, around the density ρ_c , and as such, its behaviour should be close to the behaviour of the infinite-volume system at criticality. According to this reasoning, for n large, the finite volume ASM should behave very similarly to the infinite volume model *at its critical point*, so it would be reasonable to expect critical behaviour in the finite volume sandpile.

In the above situation, that is, the Abelian sandpile on the line, one can actually prove that the above intuition is correct [19]. However, when we change the graph, this need not be true any more. As an example (taken from [8]), consider the *bracelet graph*. This graph is similar to the line, except for the fact that there are two edges between neighbouring vertices (this can be done both in finite and infinite volume). The ASM on the bracelet graph closely resembles the one-dimensional ASM described above. In fact, we can repeat the entire description, except for two differences: first, sites are called stable if their height is 0, 1, 2 or 3, and second, in a toppling occurring at site x , the height of x decreases by 4 and the height of both its neighbours increases by 2.

In this model, the parity of a given site is invariant under topplings. Indeed, the height changes that occur in a toppling are all even. This simple observation allows one to calculate explicitly the various critical densities. For a configuration in the bracelet ASM, we write

$$\eta = 2\eta_e + \eta_o,$$

where $\eta_e(x) = \lfloor \eta(x)/2 \rfloor$ is the number of pairs of particles at x , and $\eta_o(x) = \eta(x) \bmod 2$ is the indicator that $\eta(x)$ is odd. Let us look at the infinite volume model, where we only have topplings. Topplings have no influence on η_o , therefore the expected value of $\eta_o(x)$ is constant in time, and for every x equal to the probability that a Poisson- ρ random variable is odd. We denote this probability as $P_\rho(\text{odd})$. Topplings influence η_e as follows: only sites x where $\eta_e(x) > 1$ are unstable, and in a toppling, $\eta_e(x)$ decreases by 2 and the number of pairs of the neighbours increases by 1. In other words, η_e in the bracelet ASM evolves in precisely the same way as η in the one-dimensional ASM. We can conclude immediately that there is a phase transition when the ‘pair density’ is 1. A simple computation now yields that ρ_c is the solution of $\rho = P_\rho(\text{odd}) + 2$. However, a rather elementary analysis of the finite-volume version leads to the conclusion that the average density of sand grains converges to $\frac{5}{2}$, as the system size grows to infinity, so the finite volume will not reside around the critical value from the infinite volume model, and the picture of Dickman et al. breaks down.

The situation is, therefore, not so clear. One of the ways to get rid of local toppling invariants, is to let the topplings themselves being random in the sense that each particle randomly chooses a neighbour. In this model, the so called *Manna model*, a lot of structure is lost, and the picture sketched by Dickman is still a possibility; we do not know.

Progress in the Bak–Sneppen model

Maximal avalanches

Prior to the Vici project, we had concentrated on the expected duration of an avalanche at a fixed and non-random threshold b [22].

Results include a number of useful monotonicity results, as well as an explicit differential equation relating the expected duration of avalanches to their expected range. During the project we studied the avalanches at random thresholds which appear in, or are strongly related to, the thresholds in the

so called *maximal avalanche decomposition*. Here the first avalanche threshold is defined to be the minimum fitness value from the initial fitness values. After this and every subsequent avalanche, another avalanche begins with the threshold chosen to be the new minimal value of the model; this is the maximal threshold choice. It is clear that this will lead to the Bak–Sneppen model being seen as a series of avalanches at strictly increasing thresholds. The *gap function* at time s , $G(s)$, is defined to be the avalanche threshold at time s . The gap function is a stepwise increasing random function which jumps to a new value each time an avalanche finishes. Note that for all finite systems the gap function tends to 1 almost surely. Figure 2 shows a realisation of the gap function represented by the line, with the dots being the minimum fitness values at each time step. The initial fitnesses were independent and uniform $(0, 1)$ distributed.

One reason for looking at the maximal avalanche decomposition is to gain insight into how the Bak–Sneppen model tends towards criticality.

On Λ_N the threshold is the only variable needed in order to determine the distribution of an avalanche’s duration. By this we mean that the durations of two avalanches on a transitive graph are identically distributed if their thresholds are the same. Consider the Bak–Sneppen model on Λ_N . Concentrating first on the *initial* avalanche in the maximal decomposition, we see that the initial threshold is the minimum of N independent uniform $(0, 1)$ random variables. To be more explicit, we

have an avalanche with random threshold B whose density $h_N(b)$ is given by

$$h_N(b) = N(1 - b)^{N-1}, \quad 0 \leq b \leq 1.$$

Letting D_N denote the duration of the initial avalanche on Λ_N , we have the following theorem.

Theorem 1 [12]. *The expected duration of the first avalanche on Λ_N is infinite, i.e. $\mathbb{E}(D_N) = \infty$.*

One consequence of this result is that any subsequent avalanche also has infinite expected duration, as its threshold is stochastically larger. Hence the gap function consists of a sequence of steps, each of which has infinite expected length.

The usual way to analyse the Bak–Sneppen model has been to run computer simulations. Compared to these simulations, our result seems somewhat surprising, since divergent behaviour is not typically noticeable under numerical simulations of the model, especially when N is large. This is because the long avalanches that are behind this result occur when the (random) threshold B is high, which is exponentially unlikely in N . If one were to run computer simulations of the initial avalanche in order to estimate its expected duration, it would still be possible to detect this, but only from the dramatic variability of these estimations (even when a very large number of simulations are used). Theorem 1 is, therefore, an example of the value of an-

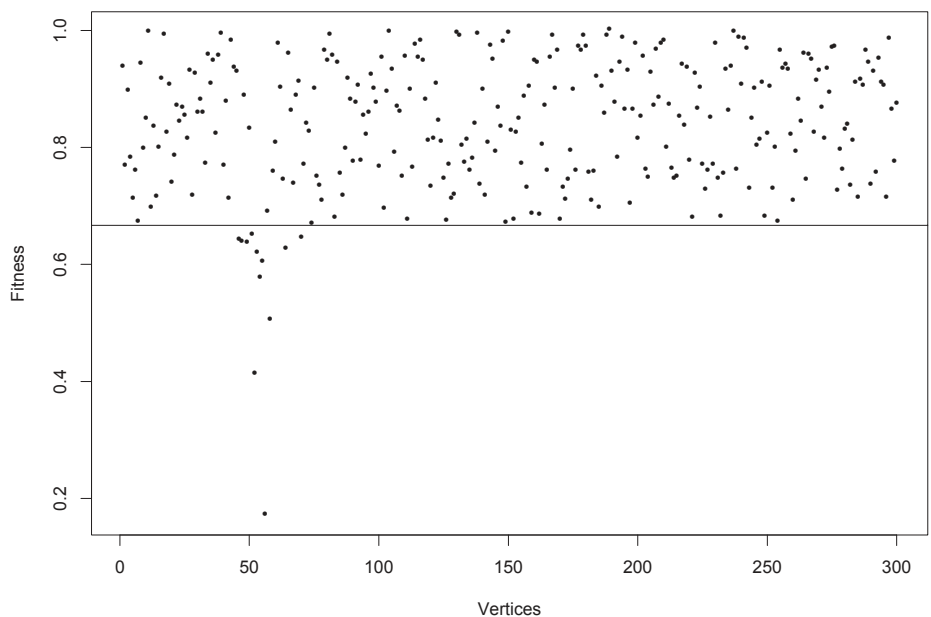


Figure 2 A realisation of the gap function when $N=100$.

alytic methods, as only very careful interpretation of computer simulations would lead one to suspect this result.

We decided to perturb the avalanche threshold by making it stochastically smaller and see whether this would lead to convergence. It turns out that $\mathbb{E}(D_N)$ is ‘barely infinite’ in the sense that making the threshold a tiny bit stochastically smaller yields finite expected durations. To be precise, we denote by D_N^n the duration of an avalanche at a threshold which is set by the minimum of n uniform $(0, 1)$ random variables on Λ_N . In this notation, $D_N^n = D_N$, with Theorem 1 now stating that $\mathbb{E}(D_N^n) = \infty$. We proved the following result.

Theorem 2 [12]. *An avalanche from a threshold chosen as the minimum of $n > N$ independent uniform $(0, 1)$ random variables has finite expectation, i.e. $\mathbb{E}(D_N^n) < \infty$ for all $n > N$.*

So just adding one uniform random variable when setting the threshold is enough to get a finite expected duration, no matter the size N of the system.

However, it is possible to show that under certain conditions all *further* avalanches have infinite expected duration. Recall that on Λ_N , setting the threshold as the minimum of N independent uniform $(0, 1)$ random variables, gives infinite expected duration. If all the fitnesses (except the minimum) are independent and uniformly distributed above the threshold at the start of the avalanche, then at the end of the avalanche all the vertices will again be independent and uniformly distributed above the threshold. So even if you fix b and choose your fitnesses to be uniform above it, it follows from Theorem 1 that the next avalanche will have infinite expected duration.

A more general, but weaker form of this result applies when we drop the condition that the fitnesses had to be nicely distributed at the start of the avalanche. All the vertices updated by the avalanche will be independent and uniformly distributed above the threshold at the end of the avalanche. So once we have had a spanning avalanche (one that updates every vertex in the system during its duration) all subsequent avalanches (from maximal thresholds) will have infinite expected duration, no matter what initial fitness values are taken.

The critical value

We already noticed that a sandpile model in

infinite volume can be defined, without additions and only topplings. Obviously, there is also a problem if we want to define the Bak–Sneppen model on an infinite graph, since every time step requires the choice of the vertex with minimal fitness. Nevertheless, for certain initial configurations we can define the model on an infinite graph, at least for a certain number of time steps. For instance, choose a threshold $b \in (0, 1)$, and consider a configuration of fitnesses with exactly one vertex, x say, having fitness below b , and all other fitnesses above b . In this situation we can start the system and run it at least until the first time that all fitnesses are above b again (if this happens). In other words, the notion of a b -avalanche makes perfect sense in infinite volume. As such it is very natural to define the critical threshold b_c as the infimum over all thresholds b for which the probability of an infinite b -avalanche is positive. In fact, we can do this on any infinite graph G .

The question then is what we can say about the critical value b_c . Computing it seems beyond reach, but interesting lower and upper bounds can be computed. A non-trivial lower bound is obtained by comparing the Bak–Sneppen model to a branching process. This is not very demanding and a very common technique. In this case this quickly leads to the following result.

Proposition 3 [13]. *On any locally finite transitive graph G with common vertex degree Δ , we have*

$$b_c(G) \geq \frac{1}{\Delta + 1}.$$

A non-trivial upper bound, however, is another matter. One of the most satisfactory things in mathematics is to relate two models to each other which did not have an obvious connection from the outset. In this direction, we were able to relate the Bak–Sneppen model on a graph G to independent site percolation on the same graph. In independent site percolation, we independently colour the vertices black or white with probability p and $1 - p$ respectively, and $p_c^{\text{site}}(G)$ is the infimum over all p for which the probability that an infinite black component arises is positive. It turns out that the following is true.

Theorem 4 [13]. *On any locally finite transitive graph G , we have*

$$b_c(G) \leq p_c^{\text{site}}(G).$$

This result implies that on many locally fi-

nite transitive graphs, b_c is non-trivial. For the Bak–Sneppen avalanche on $\mathbb{Z}$, Theorem 4 gives a trivial upper bound, but in this case we know from [21] that $b_c(\mathbb{Z}) \leq 1 - \exp(-68)$.

The following heuristics make Theorem 4 plausible. If a vertex’s fitness is not minimal, then its conditional distribution based on this information is stochastically larger than its original uniform $(0, 1)$ distribution. So if a vertex is updated by a neighbour having minimal fitness, this makes its fitness stochastically smaller, making the vertex more likely to be active and therefore, intuitively at least, the avalanche is more likely to continue. This means that on average the interference from the non-extremal vertices of the Bak–Sneppen model on the extremal vertices should be beneficial to the spread of the avalanche.

A proof is another matter. We are interested in comparing the open cluster at the origin of site percolation to a Bak–Sneppen avalanche. Typically, site percolation is considered to be static, but it is also possible to build up the open cluster at the origin dynamically. This can be done as follows. To begin with, consider the origin to be open and look at its neighbours. Decide which of these vertices are open. Then look at the new neighbours of the open cluster and iterate.

The growth of both a Bak–Sneppen avalanche and the open cluster at the origin is driven by the *extremal* vertices. These are those vertices that are contained within the avalanche and have neighbours outside the avalanche. It is only through one of the extremal vertices having the minimal fitness that the range of the avalanche can increase. For site percolation, the extremal vertices are those having a neighbour in the open cluster at the origin, but that are themselves unknown as to be open or closed. These are exactly the vertices at the edge of the cluster that will increase the size of the cluster by being open. Since it is the extremal vertices that drive the spread of both processes, the task is to relate the two sets of extremal vertices to each other.

The major difficulty to overcome is that in the Bak–Sneppen model an extremal vertex may be updated by neighbouring activity before having minimal fitness itself, whereas in site percolation a vertex is just either open or closed. This means that it is not useful to couple the two models in the naive way by realising the fitness and determining if the vertex is open and closed immediately with the same random variable, and suggests that the coupling needed is rather subtle and requires great care.

Since the critical value of site percolation on T_Δ , the regular tree with common degree Δ , equals $1/(\Delta - 1)$, the following corollary holds.

Corollary 5. *The critical value of the Bak–Sneppen model on a regular tree with common degree Δ , T_Δ , satisfies*

$$\frac{1}{\Delta + 1} \leq b_c(T_\Delta) \leq \frac{1}{\Delta - 1}.$$

A power law

One may wonder whether any progress has been made on power law behaviour in the Bak–Sneppen model. During the course of the Vici project we have not addressed this issue, but some years later, we realised that power law behaviour of avalanches can be rigorously demonstrated in a modified version of the Bak–Sneppen model [24]. This modification is defined as follows. At each discrete time step, the particle with the lowest fitness is chosen, together with one other particle, chosen uniformly at random among all remaining particles. (The restriction to update only one extra particle is rather arbitrary. The proof – suitably reformulated – goes through for multiple choices as well.) The fitnesses of both chosen particles are replaced by new fitnesses, according to independent uniform random variables on $(0, 1)$.

We define the *duration* of an *avalanche* at level $t \in (0, 1)$, also referred to as a *t-avalanche*, as follows. Consider an initial configuration of fitnesses in which one particle has fitness 0 and all other particles have fitnesses strictly larger than t . Let A_t^N denote the first time at which all fitnesses are strictly larger than t . The random variable A_t^N is the duration of a typical avalanche at level t . The number of particles updated in such an avalanche is called the *size* of an avalanche, and the corresponding random variable is denoted S_t^N .

Theorem 6 [24]. *In the modified Bak–Sneppen model, the following hold.*

(a) *For $t < \frac{1}{2}$, we have for all N ,*

$$P(A_t^N \geq k) \leq e^{-c_1(t)k},$$

for some positive constant $c_1(t)$ independent of N .

(b) *For $t > \frac{1}{2}$ and all k , we have*

$$\lim_{N \rightarrow \infty} P(A_t^N \geq k) \geq c_2(t),$$

for some positive constant $c_2(t)$.

(c) *For $t = \frac{1}{2}$, we have*

$$\lim_{k \rightarrow \infty} \lim_{N \rightarrow \infty} \sqrt{k} P(A_t^N \geq k) = 2/\sqrt{\pi}.$$

The statements in (a)–(c) remain valid when we replace A_t^N with S_t^N .

A rigorous power law at last; the proof of this result proceeds through coupling with a branching process, in combination with the known power law behaviour of a branching process at criticality. At least this result shows a proof of principle. The critical threshold is $\frac{1}{2}$ in this case, and one can understand why power law behaviour is observed now. Indeed, if the minimal threshold is below $\frac{1}{2}$, then the avalanche at that threshold is exponentially short. Only when the minimal threshold is close to $\frac{1}{2}$, one notices the power law statistics, and the system seems to organise itself, roughly, around consecutive avalanches at level $\frac{1}{2}$.

Progress on sandpile models

Stabilization in infinite volume

I already mentioned the stabilization problem in infinite volume. Above, we simply toppled all unstable sites once, but there are many other ways to organise the topplings in infinite volume. We mention some of them.

- *Markov toppling processes.* These are examples of random stationary toppling procedures and are defined as follows. Each site $x \in \mathbb{Z}^d$ has a Poisson clock (different clocks are independent) with rate one. When the clock at site x rings at time t and in the configuration η_{t-} , x is unstable, then x is toppled.
- *Toppling in nested volumes.* Choose a sequence $V_1 \subset V_2 \subset \dots$ of subsets of $\mathbb{Z}^d$ such that $\cup_n V_n = \mathbb{Z}^d$, but all V_n contain finitely many sites. We start toppling all the unstable sites in V_0 until the configuration in V_0 has no unstable sites left, then we do the same with V_1 , et cetera.
- *Topplings in waves.* This procedure is only used for initial configurations having a single unstable site, say at $x \in \mathbb{Z}^d$. In the first step, we topple x once and subsequently all *other* sites that become unstable. All these topplings form the first wave. If after these topplings, x is still unstable, then we perform the second wave, et cetera. In each wave, no site topples more than once.

Now the question about an infinite-volume analogue of the Abelian property arises: how do we know that the order in which we ap-

ply the topplings has no effect on the final stable configuration, or, for that matter, on the very question whether or not stabilization occurs? We formulated the following answer to this question. We call a toppling procedure T *finite* for initial configuration η if starting from η , every site topples at most finitely many times. We call it *stabilizing* for initial configuration η if it is finite for η and eventually leads to a stable configuration. We call a configuration η *stabilizable* if there is at least one stabilizing toppling procedure for η .

Theorem 7 [10].

1. *If T and T' are two stabilizing toppling procedures for η , then for all $x \in \mathbb{Z}^d$, x topples the same number of times under T and T' . In particular, this means that for stabilizable η , the limit configuration η_∞ is well-defined.*
2. *For stabilizable η , there does not exist a non-finite toppling procedure.*
3. *If T is stabilizing for η , then there is at least one site x that does not topple.*

Strictly speaking, the above is only true under a very weak technical condition, which is empty in case the topplings evolve in discrete time, and satisfied for Markov topplings. The upshot of this result is that we can talk about stabilizable initial configurations since it essentially does not matter which toppling procedure we use.

Another interesting question is the behaviour of the infinite volume sandpile at its critical density ρ_c . Does the system stabilize at ρ_c or not? The behaviour at criticality is in general one of the most difficult things to understand and to prove, but for the infinite-volume ASM in dimension 1, it turns out to be within reach. We say that a probability measure μ on initial configurations is stabilizable if μ -almost all configurations are stabilizable. The following result is not the most general result we obtained, but it has a short and elegant proof which I sketch below.

Theorem 8 [10]. *Let μ be a translation invariant probability measure such that $E_\mu(\eta(0)) = 1$ and such that $\frac{1}{\sqrt{n}} \sum_{x=-n}^n (\eta(x) - 1)$ converges in distribution, as $n \rightarrow \infty$, to a non-degenerate normal random variable. Then μ is not stabilizable.*

Proof. The toppling matrix Δ is defined as the matrix indexed by sites $x, y \in \mathbb{Z}$, with entries

$$\Delta_{x,y} = 2\mathbf{1}_{x=y} - \mathbf{1}_{|x-y|=1}.$$

Suppose now that μ is stabilizable. Then

the only final stable configuration can be the configuration which is constant and equal to 1. Denote by $N(x)$ the number of topplings needed at x to stabilize η . From the way topplings are defined, we then must have

$$\eta - \Delta N(x) = \bar{1}. \quad (1)$$

where $\bar{1}$ denotes the configuration with height 1 everywhere. By stationarity of the toppling mechanism, the joint distribution of $N(x)$ is stationary under translations. From (1) we obtain

$$\begin{aligned} & \frac{1}{\sqrt{n}} \sum_{x=-n}^n (\eta(x) - 1) \\ &= \frac{1}{\sqrt{n}} \left(\sum_{x=-n}^n \Delta N(x) \right) \\ &= \frac{1}{\sqrt{n}} (N(-n-1) - N(n) \\ &\quad + N(n+1) - N(-n)). \end{aligned}$$

The right hand side converges to 0 in probability as $n \rightarrow \infty$. This leads to a contradiction since, by assumption, the left hand side converges in distribution to a non-degenerate normal random variable. $\square$

Zhang's sandpile model

A less well known sandpile model was introduced by Zhang [27]. Instead of discrete sand grains, he uses continuous height variables, as follows.

Consider a finite connected subset $\Lambda \subset \mathbb{Z}^d$. Initially, every lattice site $x \in \Lambda$ is given an energy $0 \leq E_x < E_c$, where E_c is the so called *critical threshold*, and often chosen to be equal to 1. Then, at each discrete time step, one adds a random amount of energy, uniformly distributed on some interval $[a, b] \subset [0, E_c]$, at a randomly chosen lattice site. If the resulting energy at this site is still below the critical value then we have arrived at the new configuration. If not, an *avalanche* is started, in which all unstable sites (that is, sites with energy at least E_c) 'topple' in parallel, i.e., give a fraction $1/(2d)$ of their energy to each neighbour in Λ . Hence, after toppling of site x , $E_x = 0$. For boundary sites, energy leaves the system in complete analogy to the Abelian sandpile model. As in the ASM, the stabilization of an unstable configuration is performed instantaneously, i.e., one only looks at the final stable result of the random addition, and the transition from one stable configuration to the other comprises one step of the Markov process.

For this process, it is not even obvious that a (unique) stationary distribution exists, and one of our contributions is to prove precisely this in the special case of the Zhang model on the line, with N sites.

Theorem 9 [9, 11]. *For every $0 \leq a < b \leq 1$, and $N \geq 2$, Zhang's sandpile model $(N, [a, b])$ has a unique stationary distribution which we denote by $\mu^{a,b,N}$. Moreover, for every initial distribution on $[0, 1]^N$, the distribution of the process at time t converges exponentially fast in total variation to $\mu^{a,b,N}$, as $t \rightarrow \infty$.*

This result was proved in a number of papers, with special proofs for various special cases first. The proof technique is to find a coupling between the evolution of the process starting from different initial configurations in such a way that the processes eventually coalesce. Conceptually this proof method is classical, but to carry it out is not always so easy. It quickly becomes rather technical.

It is not so easy to obtain specific information about the stationary distribution. Here I state one result in this direction. Obviously the one-dimensional marginals have an atom at 0. Apart from this, the marginals turn out to be absolutely continuous with respect to Lebesgue measure on $(0, 1)$. This is of some independent interest, since in [4], a version of Zhang's sandpile model is discussed in which additions are deterministic and this model behaves radically different.

Theorem 10 [11]. *Let ν be the stationary distribution for Zhang's model on N sites. Every one-site marginal of ν is on $(0, 1)$ absolutely continuous with respect to Lebesgue measure.*

There are interesting connections between the ASM and Zhang's sandpile model, and I discuss one of them. In his original paper, Zhang observes from numerical simulation, that for large lattices, the energy variables in the stationary state tend to concentrate around discrete values of energy. He calls this the emergence of energy 'quasi-units'. Furthermore, he argues that in the thermodynamic limit, that is, when the volume tends to infinity, the stationary dynamics should behave as in the discrete ASM, with the grains of sand replaced by the discrete values of the energy.

One of the things we proved is that these quasi-units do indeed appear when $a \geq \frac{1}{2}$, in the following sense: as $N \rightarrow \infty$, all one-site marginals of the stationary distribution

concentrate on a single, non-random value. (We believe that the same is true for $a < \frac{1}{2}$ but we cannot prove this.) This is consistent with the behaviour of the ASM in one dimension, since the stationary distribution of the ASM is uniform over all configurations with at most one site with no sand grains. Hence, also in the ASM, the one-site marginals concentrate, in the limit as the system size tends to infinity, on a single value.

To state our result, we introduce the notation μ_N for the stationary distribution for the model on N sites, with expectation and variance $\mathbb{E}_N$ and Var_N , respectively.

Theorem 11 [11]. *Consider the $(N, [a, b])$ model with $a \geq \frac{1}{2}$, and write U for the random addition quantity. For the unique stationary measure μ_N we have*

$$\lim_{N \rightarrow \infty} \mu_N = \delta_U \quad (2)$$

where $\delta_{\mathbb{E}(U)}$ is the Dirac measure concentrating on the (infinite-volume) constant configuration $\eta_i = \mathbb{E}(U)$ for all $i \in \mathbb{N}$, and where the limit is in the sense of weak convergence of probability measures.

We proved this theorem by showing that for η distributed according to μ_N , in the limit $N \rightarrow \infty$, for every sequence $1 \leq j_N \leq N$,

1. $\lim_{N \rightarrow \infty} \mathbb{E}_N(\eta_{j_N}) = \mathbb{E}U$,
2. $\lim_{N \rightarrow \infty} \text{Var}_N(\eta_{j_N}) = 0$.

The proof of the first item is not difficult. However, the proof of the second part is rather complicated.

Finally ...

Many people have asked me at some point what the effect of the Vici grant has been on my career. On this point I can be brief: of course a grant like the Vici helps a lot and it is a wonderful feeling to be financially independent for a number of years. But there are other effects as well.

Supervising so many students in such a short time is rather demanding, certainly when you take the postdocs also into account. The grant was supposed to run over a rather limited period, and was not supposed to be extended too easily. Hence one should find good students on a rather short notice which has not been so easy.

Furthermore, we all know that in mathematics, one cannot advise too many PhD students at the same time. The way I dealt with it, was to ask other people to help me supervising some students. However, the point of

discussion remains: is the Vici grant system, with at least for mathematics a very substantial amount of money, the best way to finance mathematical research? Or would it be better to give less money to more researchers? I have the impression that the mathematics community would in majority vote for the latter and I tend to agree. This point be-

comes even more important these days, with even more concentration, for instance with the *Zwaartekracht* call. It is great, really, that so much money flows into mathematics, but I feel that mathematics would even be better off if that amount of money would be spread out more evenly over various disciplines within mathematics.

Acknowledgments

It is a pleasure to take this opportunity to thank everybody who participated in this project. Thanks to the PhD students Alexis Gillett, Anne Fey-den Boer, Andras Balint and Balint Vagvolgyi. Many thanks to Rob van den Berg and Frank Redig to help me supervising some of these students. Working with the postdocs Erik Broman, Misja Nuyens, Corrie Quant and Pieter Trapman was a pleasure. In addition to this, many co-authors participated in one way or another.

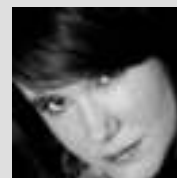
References

- 1 P. Bak, *How Nature Works*, Copernicus Press, 1996.
- 2 P. Bak and K. Sneppen, Punctuated equilibrium and criticality in a simple model of evolution, *Physical Review Letters* 71 (1993), 4083–4086.
- 3 P. Bak, K. Tang and K. Wiesenfeld, Self-organized criticality, *Physical Review A* 38 (1988), 364–374.
- 4 P. Blanchard, B. Cessac and T. Krüger, A Dynamical System Approach to SOC Models of Zhang's Type, *Journal of Statistical Physics* 88 (1997), 307–318.
- 5 D. Dhar, The abelian sandpile and related models, *Physica A* 263 (1999), 4–25.
- 6 R. Dickman, M. Muñoz, A. Vespignani and S. Zapperi: Paths to self-organized criticality, *Brazilian Journal of Physics* 30 (2000), 27–42.
- 7 R. Dickman, A. Vespignani and S. Zapperi, Self-organized criticality as an absorbing-state phase transition, *Physical Review E* 57 (1998), 5095–5105.
- 8 A. Fey, L. Levine and D. Wilson, The approach to criticality in sandpiles, *Physical Review E* 82 (2010), 031121.
- 9 A. Fey, H. Liu and R. Meester, Uniqueness of the stationary distribution and stabilizability in Zhang's sandpile model, *Electronic Journal of Probability* 14 (2009), 895–911.
- 10 A. Fey, R. Meester and F. Redig, Stabilizability and percolation in the infinite volume sandpile model, *Annals of Probability* 37 (2009), 654–675.
- 11 A. Fey, R. Meester, F. Redig and C. Quant, A probabilistic approach to Zhang's sandpile model, *Communications in Mathematical Physics* 280 (2008), 351–388.
- 12 A. Gillett, R. Meester and P. van der Wal, Maximal avalanches in the Bak–Sneppen model, *Journal of Applied Probability* 43 (2006), 840–851.
- 13 A. Gillett, M. Nuyens and R. Meester, Bounds for critical values of the Bak–Sneppen model on transitive graphs, *Markov Processes and Related Fields* 12 (2006), 679–694.
- 14 G. Grimmett, *Percolation*, Springer, 1999, 2nd edition.
- 15 T. Hara and G. Slade, The self-avoiding-walk and percolation critical points in high dimensions, *Combinatorics, Probability and Computing* 4 (1995), 197–215.
- 16 W. Kager, H. Liu and R. Meester, Existence and uniqueness of the stationary measure in a continuous sandpile, *Markov Processes and Related Fields* 16 (2010), 185–204.
- 17 C. Lee, X. Zhu and K. Gao, Avalanche dynamics in Bak–Sneppen evolution model observed with standard distribution width of fitness, *Nonlinearity* 16 (2003), 25–34.
- 18 W. Li and X. Cai, Analytic results for scaling function and moments for a different type of avalanche in the Bak–Sneppen evolution model, *Physical Review E* 62 (2000), 7743–7747.
- 19 R. Meester and C. Quant, Connections between 'classical' and 'self-organised' criticality, *Markov Processes and Related Fields* 11 (2005), 355–370.
- 20 R. Meester, F. Redig and D. Znamenski, The Abelian sandpile; a mathematical introduction, *Markov Processes and Related Fields* 7 (2001), 509–523.
- 21 R. Meester and D. Znamenski, Limit behavior of the Bak–Sneppen evolution model, *Annals of Probability* 31 (2003), 1986–2002.
- 22 R. Meester and D. Znamenski, Critical thresholds and the limit distribution in the Bak–Sneppen model, *Communications in Mathematical Physics* 246 (2004), 63–86.
- 23 M.A. Muñoz, R. Dickman, R. Pastor-Satorras, A. Vespignani and S. Zapperi, Sandpiles and absorbing-state phase transitions: recent results and open problems, in *Proceedings of the 6th Granada Seminar on Computational Physics*, J. Marro and P. L. Garrido (eds.), American Institute of Physics, 2001.
- 24 A. Sarkar and R. Meester, Rigorous self-organised criticality in the modified Bak–Sneppen model, *Journal of Statistical Physics* 149 (2012), 964–968.
- 25 A. Vespignani, R. Dickman, M.A. Muñoz and S. Zapperi, Driving, conservation and absorbing states in sandpiles, *Physical Review Letters* 81 (1998), 5676–5679.
- 26 A. Vespignani, R. Dickman, M.A. Muñoz and S. Zapperi, Absorbing-state phase transitions in fixed-energy sandpiles, *Physical Review E* 62 (2000), 4564–4582.
- 27 Y.-C. Zhang, Scaling theory of Self-Organized Criticality, *Physical Review Letters* 63 (1989), 470–473.

Ionica Smeets

wetenschapsjournalist, Leiden

i@ionica.nl



Het keerpunt van Paul van Meenen

Docenten moeten meer opkomen voor zichzelf en hun studenten

Paul van Meenen (1956) is Tweede Kamerlid en de onderwijswoordvoerder van D66. Als scholier wilde hij maar één ding worden: leraar. Dat hij voor wiskunde koos was min of meer toevallig, maar de studie in Leiden beviel hem prima. Daarna werkte hij op allerlei scholen, in allerlei functies. Tot zijn buurman Alexander Pechtold hem de politiek in praatte. Van Meenen combineerde de Leidse gemeenteraad met zijn baan in het onderwijs. Het grote keerpunt in zijn carrière kwam toen hij besloot om voltijds politicus te worden: "Ik was zo boos over hoe het kabinet Rutte I over onderwijs sprak, er moest iets gebeuren."

Waarom wilde u vroeger zo graag leraar worden?

"Het leek me een mooi beroep. Op mijn school zag ik leraren met een leven dat me erg aansprak: vrij, geen 9-tot-5-baan en veel contact met jonge mensen. Dat leek me wel wat. Wat misschien ook meespeelde is dat mijn broer gehandicapt is. Vanaf mijn jongste jeugd voelde ik me verantwoordelijk voor hem. Ik zag toen al wat het betekent als je mensen een kans geeft, hoe ze zich verder kunnen ontwikkelen. Ik wilde een beroep waarin je iets doet voor anderen, en als er één beroep is waar dat kan, dan is het leraar. Voor het vak waarin ik les wilde geven, twijfelde ik tussen wiskunde en klasieke talen. Uiteindelijk werd het wiskunde, vooral omdat twee vrienden dat ook gingen studeren in Leiden."

Waarom vielen andere vakken af als optie?

"Dat kan ik niet helemaal terughalen. Tegen-



Paul van Meenen

woordig wordt er geprobeerd om meer ratio in de studiekeuze te brengen, maar volgens mij kiezen de meeste scholieren uiteindelijk nog steeds met hun hart. En dat is maar goed ook."

U studeerde zuivere wiskunde, was dat niet zwaar als u eigenlijk docent wilde worden?

"Welnee, ik had helemaal geen beeld van wat een wiskundedocent wel en niet moest weten. Ik vond topologie en getaltheorie bijvoorbeeld prachtig. Het is een verrijking om zoiets te doen, ook al doe je er nooit meer iets mee. Wat me ook inspireerde was dat er bij wiskunde heel gedreven docenten waren. Tijdens mijn studie had ik voortdurend dat docentenbestaan in beeld."

Kreeg u iets van didactiek tijdens uw studie?

"Dat zat helemaal niet in de opleiding. Ik kreeg mijn lesbevoegdheid nadat ik vijftig uur bij iemand anders achterin de klas had gezeten om te kijken hoe het moest. In die tijd begon net de experimentele lerarenopleiding van de universiteit en het leek me verstandig om die te volgen. Daar leerde ik over de psychologische, didactische en pedagogische kanten van het vak."

Hoe beviel het toen u eindelijk voor het eerst zelf voor de klas stond?

“Dat was geweldig mooi. Na mijn studie was ik een jaar ziek, maar ik wilde toch graag werken. Ik zocht een baan dichtbij huis en kwam terecht op een vhbo. Dat was een schakelopleiding tussen het toenmalige vbo, de huishoudschool of technische school, en het hbo. De studenten waren ongeveer even oud als ik en grepen de kans om naar het hbo te kunnen. Het was heel emanciperend onderwijs. Ik begon omdat ik leraar voor mezelf een mooi beroep vond, maar al snel zag ik hoeveel het voor mensen kon betekenen.”

Waarom ging u er weg?

“Na zes jaar zag ik in de krant een vacature bij de hogeschool in Breda. Ik besloot eens een briefje te schrijven om te kijken wat er gebeurde. Ik werd aangenomen en het was daar fantastisch. Je kreeg er als docent enorm veel ruimte om samen met collega's je eigen vak in te vullen. Er was in je werkweek ook echt voldoende tijd om daar goed over na te denken. Zo kon je steeds inspelen op wat de studenten nodig hadden. Die vrijheid was een enorm verschil met mijn eerdere baan en vooral met wat ik later zag in het voortgezet onderwijs. Inmiddels zijn docenten in alle takken van het onderwijs veel van die vrijheid kwijtgeraakt, terwijl ze die nodig hebben om goed te functioneren. Daar wijs ik vaak op in de Tweede Kamer, we moeten ervoor vechten om docenten die ruimte terug te geven.”

Hoe belandde u vanuit het onderwijs in de politiek?

“Het begon toen Alexander Pechtold naast me kwam wonen, hij was in Leiden wethouder voor D66. Alexander vroeg me in de aanloop naar de verkiezingen van 2002 om mee te denken over onderwijsbeleid. Die samenwerking beviel goed. En als je Alexander een beetje kent, dan weet je dat ik daarmee nog niet klaar was. Voor ik het wist stond ik op een lijst voor de gemeenteraadsverkiezingen. En ook dat bleek enorm leuk. In de gemeentepolitiek leer je je stad zo goed kennen.”

Wat kan onderwijs van de politiek leren?

“In het onderwijs zijn we erg consensusgericht, we kunnen eindeloos ergens over praten en alsmaar geen besluit nemen. Dat is in de politiek heel anders, het hele proces is gericht op besluitvorming. Je spreekt van tevoren af dat je op een bepaald moment

een besluit zult nemen. In de tussentijd verzamelt je zoveel mogelijk informatie, maar op het afgesproken moment hak je de knoop ook echt door. Bovendien is er in de politiek volstrekt helder wat het genomen besluit inhoudt, dat is ondubbelzinnig opgeschreven. Als het in de onderwijswereld eindelijk lukt om met zes mensen aan tafel een besluit te nemen, dan kan iedereen weglopen met een volkomen eigen beeld van wat het besluit nu precies is.

Andersom is het voor de politiek goed als er mensen uit de praktijk in komen: mensen die echt weten waar ze het over hebben. Dat gebeurt in mijn ogen te weinig. Ik maakte me vroeger enorm druk over hoe Den Haag besluiten over onderwijs nam.”

Gaf dat de doorslag om in 2012 naar de landelijke politiek te vertrekken?

“Alexander Pechtold had me al jaren eerder gevraagd, maar ik wilde eigenlijk niet van de politiek mijn werk maken. Ik hield van het onderwijs. Bovendien leek het me vervelend dat je in de politiek niet puur op je eigen werk wordt afgerekend, je kunt uitglijden over de bananenschil van een ander. En zo kon ik nog wel een paar redenen verzinnen om niet naar de Tweede Kamer te willen.

Maar ik was echt boos over hoe het kabinet Rutte I over onderwijs sprak. De steen des aanstoots was de urennorm. De toenmalige minister van onderwijs kreeg klachten van ouders dat hun kinderen zo vaak onverwachts thuis waren omdat er lessen uitvielen. Toen bleek er nog ergens een oud wetsartikel te liggen met een urennorm, wat nooit actief was geweest. Uiteindelijk kwam daar de norm uit dat middelbare scholieren per jaar minstens 1040 uur les moesten krijgen. Dat was zo de verkeerde manier van denken over onderwijs: alsof tijd hetzelfde is als kwaliteit. Iedereen in het onderwijs vroeg zich af waar dit over ging. Langzaam ontwikkelde zich een soort woede in me. Ik ben niet snel kwaad, maar ik voelde dat er iets moest gebeuren. Ik heb er drie weken slecht van geslapen, maar uiteindelijk besloot ik dat ik er in de politiek echt iets aan kon doen. *(En dat is overigens gelukt, in mei dit jaar is besloten dat de 1040-urennorm vervalt – red.)*”

Heeft u in de Tweede Kamer nog iets aan uw studie?

“Met wiskunde heeft het allemaal niet zoveel te maken. Al is het fijn dat ik heb geleerd om analytisch te denken. Iedereen zit hier de hele dag conclusies te trekken. Zeker

in de onderwijshoek komen er redeneringen voorbij die logisch gezien niet helemaal correct zijn. Er wordt ook enorm veel met getallen gegooid. Ik vind het fijn dat ik kan kijken wat getallen betekenen en vooral wat ze niet betekenen.”

Mist u het onderwijs?

“Ik kom gelukkig nog steeds veel op scholen en een deel van mijn werk is in zekere zin ook nog steeds lesgeven. Sommige collega's zien me wel eens een beetje als een schoolmeester. *(Van Meenens voorlichter op de achtergrond grinnikend: ‘Nóóit.’)* De Tweede Kamer is ook echt een bijzondere omgeving. Iedereen in het gebouw heeft het gevoel dat we ergens voor staan: van beveiligers tot de kantine. We doen het samen en er zit hier zoveel kwaliteit.”

Wat wilt u vanuit de politiek zeggen tegen wiskundigen?

“Je beroep is meer dan je vak. Juist wij wiskundigen zitten dicht bij dingen die aantoonbaar zijn. Beperk het onderbouwen van stellingen niet tot je vak, maar doe het ook in de rest van je leven. Zeker docenten moeten meer voor zichzelf opkomen en voor degenen voor wie ze hun beroep uitoefenen. Als het belang van je leerlingen in het geding is, dan kun je niet zeggen dat jij alleen van de wiskunde bent. Je bent ook van de rest. Docenten hebben te snel een meegaande houding: ‘De politiek wil dit, we doen het wel weer.’ Nee! Wees altijd kritisch en blijf zelf nadenken. Het klinkt heftig, maar ik meen het wel.”

Heeft u een goede suggestie voor een (Nederlandse) wiskundige met een bijzonder keerpunt in zijn of haar carrière? Stuur dan een e-mail naar i@ionica.nl.

Herman de Lang

redacteur Nederlands Tijdschrift voor Natuurkunde
hndelang@gmail.com

Ken uw klassieken

Wiskunde en fysica

E.P. Wigner, The unreasonable effectiveness of mathematics in the natural sciences, Communications on Pure and Applied Mathematics 13 (1960), 1–14. In deze nieuwe rubriek worden klassiek geworden artikelen besproken die een blijvend stempel hebben gedrukt op de wiskunde. De navolgende bespreking van Wigners artikel door Herman de Lang is eerder verschenen in het Nederlands Tijdschrift voor Natuurkunde.

Volgens Albert Einstein is “das ewig Unbegreifliche an der Welt ihre Begreiflichkeit”. Die begrijpelijkheid komt voort uit de ontdekking dat “het boek der natuur geschreven is in de taal der wiskunde”. Galileo zei het 400 jaar geleden reeds: “De natuurfilosofie staat beschreven in het onvoorstelbaar grote boek dat doorlopend open voor onze ogen staat, ik bedoel het universum, maar men kan het niet lezen wanneer men niet eerst de taal en de tekens kent waarmee het geschreven is. Het is geschreven in de taal der wiskunde.” En meer dan 2000 jaar vóór hem verklaarde Pythagoras: “Het getal is de maat aller dingen.” Maar, aldus weer Einstein: “Wie ist es möglich, dass die Mathematik, die doch ein von aller Erfahrung unabhängiges Produkt des menschlichen Denkens ist, auf die Gegenstände der Wirklichkeit so vortrefflich passt?”

Dat fysische verschijnselen zo precies wiskundig beschreven konden worden, was ook Werner Heisenberg reeds als scholier opgevallen. “Diesen Gedanken, dass die Mathematik in irgendeiner Weise auf Gebilde unserer Erfahrung passt, empfand ich als ausserordentlich merkwürdig und aufregend”, herinnerde hij zich uit zijn middelbare schooltijd. Maar wat Eugene Wigner (Nobelprijswinnaar 1963) in zijn artikel formuleerde was de vraag naar de oorzaak van dat ‘unreasonable’ succes. Hoe komt het, aldus Wigner, “that the mathematical formulation of the physicist’s often crude experience leads in an uncanny number of cases to an amazingly accurate description of a large class of phenomena?” Voorbeelden daarvan zijn onder andere de bewegingswetten en de gravitatiewet van Newton waarmee de beweging van zon,

maan, planeten en sterren konden worden verklaard en de Maxwell-vergelijkingen waarmee in vier wetten alle elektrische, magnetische en optische verschijnselen konden worden begrepen.

Wiskunde: effectief of ineffectief?

Het antwoord op zijn vraag kon Wigner zelf niet leveren. Zijn onmacht blijkt uit het feit dat hij de samenhang tussen wiskunde en fysica als een soort mysterieus raadsel beschouwde. “The enormous usefulness of mathematics in the natural sciences is something bordering on the mysterious and there is no rational explanation for it”, aldus Wigner. “The appropriateness of the language of mathematics for the formulation of the laws of physics is a wonderful gift which we neither understand nor deserve.”

Het probleem dat Wigner aan de orde stelde, ontlokt nog steeds reacties, ook van paus Benedictus XVI. In een Engelstalige brief aan de rector magnificus van de Pauselijke Lateraanse Universiteit, aartsbisschop Fisichella, schreef hij ter gelegenheid van het internationale congres ‘From Galileo’s telescope to evolutionary cosmology’ (Rome, 26 november 2009): “Yet the human mind invented mathematics in order to understand creation, but if nature is really structured with a mathematical language and mathematics invented by man can manage to understand it, this demonstrates something extraordinary. The objective structure of the universe and the intellectual structure of the human being coincide; the subjective reason and the objectified reason in nature are identical.”

Anderen wezen er echter op dat in wetenschapgebieden zoals economie, meteorologie, biologie de effectiviteit van de wiskunde veel te wensen overliet. De bekende moleculair bioloog Israel Gelfand verklaarde in een reactie op Wigners artikel: “There is one thing which is more unreasonable than the unreasonable effectiveness of mathematics in physics and that is the unreasonable ineffectiveness of mathematics in biology.” De mathematische ineffectiviteit in die andere wetenschappen is vaak te wijten aan de complexiteit van de aldaar heersende verschijnselen — complexiteit die zich alleen laat vangen in waarschijnlijkheidsrekening en statistiek.

Dit gebeurt ook in de fysica zoals bij de conceptie van de emergente thermodynamische begrippen en bij de dataverwerking van experimenten van de elementaire deeltjesfysica. Ook kan het gebeuren dat bepaalde wiskundige vergelijkingen — zoals de Navier–Stokes-vergelijkingen uit de stromingsleer — niet analytisch kunnen worden opgelost en numeriek moeten worden bewerkt. Maar een veel dieper liggende oorzaak



Eugene Paul Wigner (1902–1995)

is het feit dat, met uitzondering van de fysica, in de andere (natuur)wetenschappen de wiskunde slechts een instrumentele rol vervult, louter als toepassing, als numerieke manifestatie van kwantitatieve gegevens. Steeds kan men daarbij een strikte scheiding aanbrengen tussen de conceptuele begrippen uit de betreffende wetenschap en de mathematische bewerking ervan.

Daarentegen bestaat in de fysica een veel dieper, zelfs inherent verband tussen de wiskundige en fysische concepten. Snelheid en versnelling zijn niet te scheiden van differentiaalafgeleiden, het elektromagnetisch veld niet van het vectorveld, de algemene relativiteitstheorie niet van de niet-euclidische meetkunde, de tensorrekening en de differentiaalmeetkunde, de elementaire-deeltjesfysica niet van de transformatiegroepen en kwantummechanica niet van de Hilbert-ruimte, om maar enkele voorbeelden te noemen. Zo werd door Newton de differentiaalrekening specifiek uitgevonden om de continue verandering en instantane snelheid van een lichaam in beweging te kunnen beschrijven. De wiskunde is medebepalend voor de vormgeving van de fysica, is daarmee ‘verinwendigd’ en daarom onafscheidelijk en onscheidbaar ermee verbonden.

Wiskunde als taal

“Toutes les lois physiques,” aldus Henri Poincaré, “sont tirées de l’expérience, mais pour l’énoncer, il faut une langue spéciale; le langage ordinaire est trop vague, pour exprimer les rapports si délicats, si riches et si précis. Voilà donc une première raison pour laquelle le physicien ne peut se passer des mathématiques; elles lui fournissent la seule langue qu’il puisse parler.” Gezien haar constituerende en formatieve rol echter, is wiskunde méér dan de taal van de fysica. Wiskunde is in de fysica niet louter descriptief, maar vormt onderdeel van de fysische gedachte. De (theoretische) fysicus denkt de fysische verschijnselen mede in mathematische concepten. Die samenhang is subtiel. De wiskunde is niet een skelet waaromheen het fysische vlees wordt opgebouwd, noch is het een abstract idee dat met de fysische werkelijkheid concrete vorm wordt gegeven. De samenhang is dynamisch, waarbij men twee vormen kan onderscheiden: een *actieve* en een *passieve*.

De actieve vorm betreft de wiskunde die speciaal werd ontwikkeld met de toepassing op een specifiek fysisch probleem voor ogen. Ogenscheinlijk lijkt de effectiviteit dan voor de hand te liggen, maar toch is verbazingwekkend dat de effectiviteit veel groter blijkt te

zijn dan voor het doel waarvoor die oorspronkelijk werd ontworpen. Toen Newton zijn gravitatiewet opstelde, die inhoudt dat de kracht tussen twee massa’s omgekeerd evenredig is met het kwadraat van hun onderlinge afstand, bleek die wet tot op 4 procent nauwkeurig, op grond van de experimentele data die hem toen ter beschikking stonden. In 1950 bleek de experimentele nauwkeurigheid van de wet beter dan 0,001 procent. Vanwege de snaartheorie en de hypothese van meerdere opgerolde dimensies ontstond recent het vermoeden dat op hele korte afstanden de wet van Newton niet meer zou gelden. Met ingenieuze metingen toonde Dan Kapner van de universiteit van Washington (Seattle) in 2007 echter aan dat tot op een afstand van 0,056 mm de wet nog steeds geldt. Aldus blijkt dat een wet, die meer dan 300 jaar geleden op grond van summiere gegevens wiskundig werd geformuleerd, thans nog met uiterste nauwkeurigheid geldt, zelfs in een gebied waarbinnen tot voor kort niet eens gemeten kon worden.

Zo groot was ook in het verleden het vertrouwen in de precisie van de wet van Newton, dat kleine afwijkingen ervan niet aan de wet zelf werden toegeschreven, maar aan de invloed van een storend object. Op die manier werd in 1840 de planeet Neptunus door Urbain Le Verrier ontdekt en in 1930 de dwergplaneet Pluto door Clyde Tombaugh van de Lowell Observatory in Arizona. Een ander voorbeeld is het magnetisch moment van het elektron dat in de kwantumelektrodynamica men zowel theoretisch kan berekenen als experimenteel meten. Beide resultaten bleken overeen te stemmen met een precisie van 10^{-8} procent. Volgens Richard Feynman is het alsof je de afstand tussen New York en San Francisco tot op een haarbreedte hebt kunnen bepalen.

Hoe dieper men in de fundamenteën van de fysica doordringt, hoe meer men merkt dat de fysica door de wiskunde wordt beheerst. De wiskunde die men daar vindt is bovendien niet van het eenvoudige uit te rekenen soort, maar betreft wiskunde van een diepgaand, subtiel en complex karakter dat men niet bij de minder fundamentele fysica aantreft. Nog verbazingwekkender is de effectiviteit van de passieve vorm, die bestaat uit volledig abstracte, zonder enig toepassingsoogmerk ontwikkelde wiskunde, maar die later blijkt een precies passend model voor een fysisch gebied te vormen. Zo bleek de in 1924 door Heisenberg opgestelde kwantummechanica, zonder dat hij er erg in had, te berusten op de matrix- en determinanttheorie die reeds in

de achttiende en negentiende eeuw was ontwikkeld. De in 1831 de dag voor zijn dood opgeschreven groepentheorie van Evariste Galois, louter om de oplosbaarheid van algebraïsche vergelijkingen te bepalen, bleek een uitstekende toepassing te zijn voor de classificatie, representatie en transformatie van elementaire deeltjes. Ook Einstein vond in de tensorrekening en differentiaalmeetkunde van Bernhard Riemann (1826–1866) een kant-en-klaar mathematisch apparaat voor zijn algemene relativiteitstheorie van 1915.

Een ander aspect is de pluriformiteit van het wiskundig gebruik in de fysica. Hetzelfde fysische verschijnsel kan op verschillende, maar equivalente wiskundige manieren beschreven worden. De beweging van een massapunt in een conservatief krachteveld bijvoorbeeld, kan worden beschreven volgens Newton, Hamilton of Lagrange. De kwantummechanica kan worden geformuleerd volgens Heisenberg/Dirac, Schrödinger of Feynman. Niet alleen de wiskunde daarbij is verschillend, ook de onderliggende fysica is anders. Dit is een van de redenen waarom de fysica zich niet laat axiomatiseren. (Vanwege het onvolledigheidstheorema (1931) van Kurt Gödel is dat in de wiskunde ook niet meer mogelijk gebleken, ondanks pogingen daartoe van David Hilbert en van de école Bourbaki onder leiding van André Weil.)

Wiskunde en de werkelijkheid

De welhaast pijnlijke nauwkeurigheid van de wiskunde bij de beschrijving en voorspelling van fysische verschijnselen doet de vraag rijzen of de werkelijkheid volledig door de wiskunde wordt bepaald. “Is God a mathematician?”, vraagt de astrofysicus Mario Livio zich af. Max Tegmark, een fysicus van MIT, lijkt die vraag te beamen. In een artikel uit 2007 in de *Foundations of Physics* met als titel ‘The Mathematical Universe’, poneert hij twee hypothesen, de External Reality Hypothesis (ERH): *There exists an external physical reality completely independent of us humans*, en de Mathematical Universe Hypothesis (MUH): *Our external physical reality is a mathematical structure*. Hij adstrueert zijn hypothesen als volgt. Fysische theorieën streven ernaar om de werkelijkheid te beschrijven. De huidige theorieën echter bestrijken slechts beperkte gebieden van de werkelijkheid. De Heilige Graal van de fysica is een complete beschrijving van alles — een ‘Theory of Everything’ (TOE).

De ERH impliceert dat voor zo’n complete allesomvattende beschrijving de gebruikte ‘taal’ welgedefinieerd en begrijpelijk moet

zijn, ook voor niet-menselijke intelligente wezens zoals buitenaardse bewoners ('aliens') of toekomstige computers. Zo'n taal moet dus vrij zijn van 'menselijke bagage', dat wil zeggen van concepten en uitdrukkingen die tijdens de menselijke evolutie zijn ontstaan, zoals 'deeltje', 'observatie', enzovoorts, ja zelfs van ieder woord in iedere taal.

De enige taal zonder die menselijke bagage en daarom geschikt om de gehele werkelijkheid compleet te beschrijven is de wiskunde. Dat impliceert weer dat de werkelijkheid een wiskundige structuur moet hebben, zoals gesteld in MUH. Waar men nu nog zegt dat de externe werkelijkheid door de wiskunde wordt *beschreven*, kan men zeggen als de TOE is voltooid, dat de wiskunde de externe werkelijkheid *is*.

De vraag van Wigner naar de oorzaak van de raadselachtige effectiviteit van de wiskunde is daarmee volgens Tegmark beantwoord. De wiskundig geformuleerde benaderingen waaruit onze fysische theorieën bestaan zijn effectief omdat die eenvoudige wiskundige formuleringen een goede benadering vormen van bepaalde aspecten van meer complexe wiskundige structuren. "In other words," aldus Tegmark, "our successful theories are not mathematics approximating physics, but mathematics approximating mathematics."

De mathematische structuur van de werkelijkheid verklaart ook dat vanuit de wiskunde nieuwe fysische verschijnselen kunnen worden voorspeld, beter gezegd: nieuwe mathematische verbanden kunnen worden ontdekt. Reeds in 1931 verklaarde Paul Dirac: "The most powerful method of advance that can be suggested at present is to employ all the resources of pure mathematics in attempts to perfect and generalize the mathematical formalism that forms the existing basis of theoretical physics and after each success in this direction, to try to interpret the new mathematical features in terms of physical entities."

In zijn boek *The Road to Reality* (2004) echter, verdiept de bekende (nu emeritus) hoogleraar mathematische fysica van de universiteit van Oxford, Roger Penrose, de vraag van Wigner. Penrose onderscheidt drie werelden: de wereld van het mentale bewustzijn of de menselijke geest, de wereld van de materiële fysische realiteit en de platonische (ideële) wereld van de wiskunde. Die drie werelden zijn volgens hem verbonden door drie mysteries, namelijk: hoe kan het dat de menselijke geest uit de materiële wereld is ontstaan, hoe kan het dat de fysische wereld door de mathematische wereld wordt beheerst en hoe kan het dat de menselijke geest weet heeft

van de wiskundige wereld en daarmee ook de fysische wereld kan omvatten? De drie werelden vallen niet samen, maar vormen toch een eenheid. Daaraan is echter ook de vraag verbonden of wiskunde wordt ontdekt of uitgevonden. Met andere woorden, bestaat er inderdaad een ideële wiskundige wereld onafhankelijk van de mens, waarin we stukje bij beetje binnendringen of is de wiskunde niet meer dan een menselijke constructie? Daarover bestaat nog geen consensus.

De toekenning van een wiskundige structuur aan de fysische werkelijkheid werpt ook de vraag op welke waarheidscriteria men op een mathematische beschrijving van die werkelijkheid moet toepassen, mede in verband met de pluriformiteit van zo'n beschrijving. Tot nog toe geldt daarvoor het criterium van de experimentele verificatie, of sinds Karl Poppers boek *Die Logik der Forschung* (1935), van de experimentele falsifieerbaarheid. Maar wat te doen wanneer een theorie zich bijna principieel aan een experimentele toetsing onttrekt, zoals bijvoorbeeld het geval is met de snaartheorie? Is op grond van het postulaat van een mathematisch gestructureerd universum de wiskundige zelfconsistentie of niet-tegenstrijdigheid van zo'n theorie voldoende waarborg voor de realiteit ervan?

Einstein en, met name, Dirac bepleitten een esthetisch criterium, namelijk de eenvoud, elegantie en schoonheid van de wiskundige formulering als mede-keurmerk voor het fysisch waarheidsgehalte van de beschrijving. In zijn boek *Experiment and Theory in Physics* (1943) schrijft Max Born daarover: "I have not endeavoured to analyse the idea of beauty or perfection or simplicity of a natural law which have often guided the correct divination. I am convinced that such an analysis would lead to nothing; for these ideas are themselves subject to development. We learn something new from every new case, and I am not inclined to accept final theories about invariable laws of the human mind. My advice to those who wish to learn the art of scientific prophecy is not to rely on abstract reason, but to decipher the secret language of Nature from Nature's documents, the facts of experience." En reeds in de inleiding van zijn eerste hoofdstuk van zijn befaamde *The Feynman Lectures on Physics* (1963) verklaart Richard Feynman: "The principle of science, the definition almost, is the following: The test of all knowledge is experiment. Experiment is the sole judge of scientific truth."

Over de hypothese dat de fysische werkelijkheid volledig isomorf is met een wiskundige structuur bestaat trouwens geen consen-



Roger Penrose

sus. In navolging van de filosoof Immanuel Kant valt volgens de Kopenhaagse School (Bohr, Heisenberg) de werkelijkheid als zodanig niet te kennen, ook niet volgens wiskundig geformuleerde theorieën of experimentele metingen. Wat wij kunnen weten is alleen het verband tussen de werkelijkheid en onze zintuigen en meetapparatuur. "Die Vorstellung von der objektiven Realität der Elementarteilchen", aldus Werner Heisenberg, "hat sich also in einer merkwürdigen Weise verflüchtigt... in die durchsichtige Klarheit einer Mathematik, die nicht mehr das Verhalten des Elementarteilchens, sondern unsere Kenntnis dieses Verhalten darstellt. Der Atomphysiker hat sich damit abfinden müssen, dass seine Wissenschaft nur ein Glied ist in der endlosen Kette der Auseinandersetzungen des Menschen mit der Natur, dass sie aber nicht einfach von der Natur an sich sprechen kann."

Hoe het ook zij, laten we ons aansluiten bij Eugene Wigner, die zijn artikel over de effectiviteit van de wiskunde in de natuurkunde met de volgende zin besluit: "We should be grateful for it and hope that it will remain valid in future research and that it will extend, for better or for worse, to our pleasure, even though perhaps also to our bafflement, to wide branches of learning."

Deze nieuwe rubriek is geïnspireerd op een soortgelijke rubriek in het *Nederlands Tijdschrift voor Natuurkunde*. Wij danken de redactie van dit tijdschrift voor hun enthousiaste reactie op onze suggestie de rubriek te openen met de hierboven afgedrukte bespreking van Wigners klassieke artikel. Graag wijzen we de geïntereseerde lezer ook op een interessant artikel van Robbert Dijkgraaf in het NTvN, 'De onredelijke effectiviteit van de fysica in de moderne wiskunde' (NTvN, 62/11, 1996), dat Wigners artikel in omgekeerd perspectief beziet.

Frans Oort

Mathematisch Instituut

Universiteit Utrecht

f.oort@uu.nl

Geschiedenis

The Weil conjectures

As of 2003, the Abel Prize has been awarded yearly to one or more mathematicians. Up to 2014, fourteen laureates have received this prize, which has often been described as the mathematician's 'Nobel prize'. In 2013 it was awarded to Pierre Deligne. This event was celebrated by a presentation during a WONDER meeting in Delft, in December 2013. The present note of Frans Oort aims to give a part of that presentation, in particular a contemplation on the 'flow of mathematics' which led to this great success: the main topic will be on the 'pre-history' of the Weil conjectures.

The fundamental problem in number theory is surely how to solve equations in integers. Since this question is still largely inaccessible, we shall content ourselves with the problem of solving polynomial congruences modulo p .

Nick Katz in [20]

The Riemann Hypothesis (RH) has been in the focus of mathematical research ever since Bernhard Riemann stated this conjecture in 1859. However, this problem will not be considered here. From 1924 onward an analogue of the RH has been studied, usually called *the characteristic p formulation*. In order to avoid any confusion we will refer to this by pRH (although this is not standard). Basically, this problem concerns solving equations over finite fields. We will see that the pRH answers the question of counting the number of solutions to polynomial equations over all finite fields of the same characteristic at one stroke. This will be illustrated by an easy example, to be followed throughout the paper.

After fifty years Pierre Deligne placed the crown on this impressive series of developments by proving the pRH in its full generality.

Below, we will discuss the history of this flow of ideas.

Remark. Does this provide any progress for the solution of the classical RH? The answer is negative in the strict sense: there is no implication $\text{pRH} \Rightarrow \text{RH}$ (and also no argument the reverse way). However, it may give us confidence of being on the right track. Moreover, tools have been developed, several technical steps have been made, and above all the deep insight in arithmetic aspects of geometry have proved to be a powerful aspect of modern mathematics.

We discuss:

- Formulation of the (equivalent of the) RH by Emil Artin, and results by F.K. Schmidt, Hasse and Weil proving this conjecture in special cases (algebraic curves and abelian varieties defined over finite fields).
- We indicate how this motivated André Weil to formulate his conjectures.
- In short sections we give references for results proved by Grothendieck with many of his co-workers, and finally by Deligne, proving the Weil conjectures.

I expect that the first four pages can be understood by a general audience; the next two pages will convey some of the thrill of this daring conjecture by Weil; the last two pages give ample references about recent work on the Weil conjectures. Excellent surveys are [20, 26, 33, 40], also see [8].

Counting points on varieties over finite fields

This was considered by Gauss, DA 357 (*Disquisitiones Arithmeticae*), and in his famous 'Last Entry' 146 in 1814 in his Tagebuch: the



Photo: IHES

Pierre Deligne during his time at IHES

number of rational points on several elliptic curves (in our terminology) over a prime field $\mathbb{F}_p$ were computed [11–12]. Also other mathematicians considered such cases.

Let me take one simple example, which we will follow throughout our journey. Try to solve the equation

$$Y^2 - Y = X^3 - X^2, \quad \text{with } x, y \in \mathbb{F}_{2^m}.$$

It is clear that over $\mathbb{F}_2$ there are exactly four solutions given by $x = 0, 1$ and $y = 0, 1$; note that $-1 = +1 \in \mathbb{F}_2$. We can embed the affine plane into the projective plane by $(x, y) = [x:y:1]$. We know that, adding the ‘point at infinity’ $[0:1:0]$ (the unique point at ‘infinity’ on the line $X = 0$) we obtain an elliptic curve $D \subset \mathbb{P}_K^2$ defined over $K = \mathbb{F}_2$ by the homogeneous equation

$$Y^2 Z - Y Z^2 = X^3 - X^2 Z.$$

We write our modest result as

$$\#(D(\mathbb{F}_2)) = 5.$$

How do we compute $N_m := \#(D(\mathbb{F}_{2^m}))$ for all $m \in \mathbb{Z}_{>0}$? We will show that abstract theory gives a complete (and easy) answer to this question (and in fact, the same method answers this question over any finite field).

Explanation. A *finite field* is a field with a finite number of elements. An example is the residue class ring $\mathbb{Z}/p$, where p is a prime number (and indeed, as is easily proved, this is a field). However $\mathbb{Z}/4$ is not a field: it has zero-divisors, the element $2 \bmod 4$ does not have an inverse. General theory says that for any prime power $q = p^n$, where p is a prime number and $n \in \mathbb{Z}_{>0}$, there exists a finite field with q elements, and this field is unique up to isomorphism; it will be denoted by $\mathbb{F}_q$, in particular $\mathbb{F}_p = \mathbb{Z}/p$.

An *elliptic curve* E over a field K is a non-singular algebraic curve $E \subset \mathbb{P}_K^2$ given by a cubic equation having at least one K -rational point. The curve $D \subset \mathbb{P}^2$ given by the homogeneous equation $ZY^2 - Z^2Y = X^3 - ZX^2$ (over a field in which $11 \neq 0$) is an example of an elliptic curve.

Side remark: This equation considered over $\mathbb{F}_{11}$ defines a curve on which $(x = 8 \bmod 11, y = 6 \bmod 11)$ is the (only) singular point (a node).

First, we will follow a different line of development in history.

Euler series and the Riemann zeta function

Euler studied in 1740 infinite series defined as an infinite sum of positive numbers, and later Chebyshev studied this as a function of a real variable s :

$$\sum_{n=1}^{\infty} \frac{1}{n^s} = \prod_p \frac{1}{1 - p^{-s}}, \quad s \in \mathbb{R},$$

where p runs through the set of all prime numbers. Both sides converge for $s > 1$.

Riemann, who knew work by Euler and who knew the relation of this function with the theory of prime numbers, wrote in 1859 his masterpiece *Über die Anzahl der Primzahlen unter einer gegebenen Grösse* [31]. Riemann considered the function

$$\zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n^s} = \prod_p \frac{1}{1 - p^{-s}}, \quad s \in \mathbb{C},$$

convergent for the real part of s greater than one, and he proved that this complex function has an analytic continuation. He showed that (the analytic continuation of) this function has zeros at all negative, even, integral values of s (the ‘trivial zeros’). Riemann then stated his famous conjecture that for this function (called the *zeta function* by Riemann) (continued across the pole at $s = 1$) all ‘non-trivial zeros’ should have real part with absolute value equal to $\frac{1}{2}$ (in this case ‘non-trivial zeros’ can be understood as zeros with imaginary part not equal to zero). It is impressive to read this paper by Riemann: concise, a masterpiece of technical skill. This conjecture, if true, would give a insight in the distribution of prime numbers. His idea, his conjecture, now indicated by RH, has had an enormous impact on mathematics, and it still has this influence.

Remark. These series were considered by Euler, already in 1740, for positive integral values of s . As far as I know Euler did not consider this as a ‘function’ in s , therefore I will not use the terminology ‘the Euler zeta-function’. Dirichlet and Chebyshev studied such series as a function (of a complex or a real variable).

The Dedekind and E. Artin zeta functions

At the moment we have no idea how to prove (or disprove?) the Riemann Hypothesis for the Riemann zeta function.

Remarkably enough, it might help to study a generalization. Let R be an *algebra of finite type over $\mathbb{Z}$* . This means that there is



Emil Artin (1898–1962)

an ideal $I \subset \mathbb{Z}[T_1, \dots, T_m]$ such that $R \cong \mathbb{Z}[T_1, \dots, T_m]/I$. Here are some examples: $\mathbb{Z}$, $\mathbb{Z}[T]$, $\mathbb{F}_p$ (where $\mathbb{F}_p = \mathbb{Z}/p$), $\mathbb{F}_p[T]$, etc.

Lemma. Let R be an algebra of finite type over $\mathbb{Z}$. For any maximal ideal $M \subset R$ the residue class ring R/M is a finite field.

For a ring R as above we define its ‘zeta function’ by

$$\zeta_R(s) = \prod_M \frac{1}{1 - \#(R/M)^{-s}},$$

where this (Euler) product ranges over all maximal ideals $M \subset R$, and where s is a complex variable. E.g. see [38].

Examples. 1. In case $R = \mathbb{Z}$ we have the classical Riemann zeta function

$$\zeta_{\mathbb{Z}}(s) = \zeta(s) :$$

any maximal ideal $M \subset R = \mathbb{Z}$ is of the form $M = (p) \subset \mathbb{Z}$, where p is a prime number, and

$$\begin{aligned} \zeta_{\mathbb{Z}}(s) &= \prod_M \frac{1}{1 - \#(R/M)^{-s}} \\ &= \prod_p \frac{1}{1 - p^{-s}} = \sum_1^{\infty} \frac{1}{n^s}. \end{aligned}$$

2. For the ring of integers in a number field we obtain what is now called the Dedekind zeta function.

3. For a ring like $R = \mathbb{Z}[T]$, or $\mathbb{F}_p[T]$, we obtain a new type of zeta function.

For these zeta functions (e.g. where $\mathbb{Z}$ is a subring of R) we hope we can extend classi-

cal properties of the Riemann zeta function: they should extend to a meromorphic function over the complex plane and they should satisfy a functional equation similar to that of the classical Riemann zeta function. We can ask for their non-trivial zeros (the extended Riemann hypothesis). See [39]. Later, these definitions and questions were considered for L -functions (not discussed here).

In his description of the RH as Millennium Problem Bombieri writes: “Not a single example of validity or failure of a Riemann hypothesis for an L -function is known up to this date. The Riemann hypothesis for $\zeta(s)$ does not seem to be any easier than for Dirichlet L -functions (except possibly for non-trivial real zeros), leading to the view that its solution may require attacking much more general problems, by means of entirely new ideas.” [48]

We seem to have made no progress for the classical RH in this way. However, we can derive some hope (or perhaps any hint?) from studying a *special case* of this more general situation:

Examples. For a given prime number p we study rings of finite type over the finite field $\mathbb{F}_p$ (the prime field of characteristic p).

4. We take $R = \mathbb{F}_q$, and obtain $\zeta_R = 1/(1 - q^s)$.
5. Emil Artin proposed in 1924 in his PhD thesis [1] a definition of the zeta function for an algebraic curve over a finite field and he proposed a RH for this kind of zeta function. The definition and properties of such zeta functions were further studied by F.K. Schmidt [34] and by H. Hasse [18–19]. Rationality was proved by F.K. Schmidt and Hasse proved the (analogue pRH of the) RH for elliptic curves over a finite field.

From now on all varieties are defined over a finite field of characteristic p , and we study the pRH, an analog/special case of the extended Riemann Hypothesis (below we give formulas).

Proof of the pRH by Hasse

In 1934 Hasse proves the pRH for elliptic curves over finite fields.

Reminder. We write RH for the classical Riemann Hypothesis (and generalizations in characteristic zero). In order to avoid confusion we write pRH for the equivalent of the RH about solving equations in positive characteristic.

Here we set up notation. As base field we choose $K = \mathbb{F}_q$, where q is a power of p . For any $m \in \mathbb{Z}_{>0}$ we write $K_m := \mathbb{F}_{q^m}$, i.e. $K \subset K_m$ is the extension of degree m (unique up to a K -isomorphism).

Reminder. In a basic course on algebra we learn that for every prime power $q = p^n$ there exists, up to an isomorphism, exactly one field K with q elements; this field we denote by $K = \mathbb{F}_q$. Note that $\mathbb{F}_p \cong \mathbb{Z}/p$, however for $n > 1$ the field $\mathbb{F}_q$ is not isomorphic with $\mathbb{Z}/p^n$.

From now on all base fields will be in characteristic $p > 0$.

This theory, started by Emil Artin, gives rise to the following definition, in analogy with the Dedekind zeta function for number fields. Let V be a non-singular, projective variety defined over K , i.e. an algebraic variety defined as a closed set in some projective space $\mathbb{P}_K^d$. For a field L containing K we write $V(L)$ for the set of points on V with coordinates in L , the set of points ‘rational over L ’. We write

$$N_m = N_m(V/\mathbb{F}_q) := \#(V(K_m)),$$

the number of points on V with coordinates in $K_m := \mathbb{F}_{q^m}$. This results in the (Hasse–Weil) zeta function

$$\begin{aligned} Z(T) &= Z(V, T) = Z_{V/K}(T) \\ &= \exp \left(\sum_{m=1}^{\infty} \frac{N_m}{m} T^m \right). \end{aligned}$$

Below we will see that this definition generalizes the notion of zeta functions $\zeta_R(s)$ as in the previous section from rings to varieties. In fact, Emil Artin introduced this zeta functions over a finite field, only for curves.

Example. Let V be just one point, rational over $K = \mathbb{F}_q$, hence $N_m = 1$ for every $m > 0$. We see:

$$Z(T) = \exp \left(\sum_{m=1}^{\infty} \frac{1}{m} T^m \right) = \frac{1}{1-T}.$$

Example. Let us consider $V = \mathbb{A}_K^d$, the affine space of dimension d over K ; this is defined by: for any ring R containing K we have $\mathbb{A}_K^d(R) = R^d$. We see

$$N_m = \#((\mathbb{F}_{q^m})^d) = q^{md}.$$

We can show:

$$Z_V(T) = \frac{1}{1 - q^d T}.$$

Example. For $V = \mathbb{P}_K^1$, the projective line, we have $N_j = q^j + 1$ and we see that

$$Z(\mathbb{P}_K^1, T) = \exp \left(\sum_{j=1}^{\infty} \frac{q^j + 1}{j} T^j \right).$$

This can be rewritten as

$$Z(\mathbb{P}_K^1, T) = \frac{1}{(1-T)(1-qT)}.$$

Surprisingly, the above examples give a rational function in the variable T . In an analogous way we can easily show:

$$Z(\mathbb{P}_K^n, T) = \frac{1}{(1-T)(1-qT) \cdots (1-q^n T)}$$

for all $n \in \mathbb{Z}_{>0}$ and all $K = \mathbb{F}_q$. Note that $\mathbb{P}^n$ can be written as disjoint union of $\mathbb{A}^0, \dots, \mathbb{A}^n$; from this observation the formula follows. A survey can be found in [25, Chapter 6].

Theorem (F.K. Schmidt, 1931). *For a (non-singular, irreducible, projective) algebraic curve C over a finite field $\mathbb{F}_q$, its zeta function $Z(C, T)$ is a rational function in T , having the precise form*

$$Z(C, T) = \frac{P}{(1-T)(1-qT)},$$

where $P \in \mathbb{Z}[T]$ is a polynomial of degree $2g$, where $g = \text{genus}(C)$, and

$$P = P(T) = \prod_{i=1}^{2g} (1 - \alpha_i T), \quad \alpha_i \in \mathbb{C}.$$

The map $\alpha \mapsto q/\alpha$ is a permutation of $\{\alpha_1, \dots, \alpha_{2g}\}$.

F.K. Schmidt proved in [34] the Riemann–Roch theorem for curves in positive characteristic, and in the second part of that paper Schmidt uses this to prove the theorem above, in particular the rationality of the zeta function of a complete, nonsingular curve of genus g over $\mathbb{F}_q$, with numerator a polynomial of degree $2g$.

Remark. We see that $Z(C, T)$ admits an analytic continuation. The substitution $T = q^{-s}$ gives

$$Z_E(T) = Z_E(q^{-s}) =: \zeta_E(s).$$

We see that $\alpha \mapsto q/\alpha$ yields $s \mapsto 1-s$, and this is the (analogue of the) ‘functional equation’.

Theorem (Hasse, 1934). *For an elliptic curve E over $K = \mathbb{F}_q$ the algebraic integers $\alpha, \beta \in \mathbb{C}$, defined by*

$$Z(E/K, T) = \frac{(1 - \alpha T)(1 - \beta T)}{(1 - T)(1 - qT)}$$

satisfy

$$(\text{pRH}) \quad |\alpha| = \sqrt{q} = |\beta|.$$

Hasse proves in [18, §11] the Riemann Hypothesis for elliptic curves over a finite field, see also [19, III, §4].

Remark. The numerator $P_1(T)$ of $Z(E/K, T)$ in case of an elliptic curve E is the eigenvalue polynomial of the action of the Frobenius $\pi \in \text{End}(E)$, as Hasse remarked and used. We will see that this insight will be generalized.

Explanation. As already has been noted, we write RH for the *classical Riemann Hypothesis*, and we write pRH for the special case of a generalization, studying an *equivalent question over finite fields*. The property $|\alpha| = \sqrt{q} = |\beta|$ above implies that the zeros of $\zeta_E(s)$ have their real part equal to $\frac{1}{2}$ here we see the resemblance with the classical RH.

We have seen that $Z_V(T)$ encodes the sequence $\{N_m \mid m \in \mathbb{Z}_{>0}\}$. Conversely these numbers can be retrieved via the logarithmic derivative (f'/f) :

$$\frac{TZ'(T)}{Z(T)} = \sum_{m>0} N_m T^m.$$

The Hasse bound

It follows that for any elliptic curve E over $\mathbb{F}_q$ we have

$$\begin{aligned} N_m(E/\mathbb{F}_q) &:= \#(E(\mathbb{F}_{q^m})) \\ &= 1 - (\alpha^m + \beta^m) + q^m. \end{aligned}$$

We see that such a theorem gives the number of rational points over all finite extensions of K , once α and β are known. This proves that for any elliptic curve E over $\mathbb{F}_q$ we have the ‘Hasse bound’:

$$|\#(E(\mathbb{F}_q)) - 1 + q| = |\alpha + \beta| \leq 2\sqrt{q}.$$

See below.

Remark. As an elliptic curve is a double cover of the projective line (ramified in at least one point) for an elliptic curve E over $\mathbb{F}_q$ we immediately see the bound

$$\#(E(\mathbb{F}_q)) \leq 2q + 1.$$

As $2\sqrt{q} < q + 1$ for all q and $2\sqrt{q} < q$ for $4 < q$ we see the Hasse bound agrees with this bound and in many cases it is sharper.

Elliptic curve

We return to our example $D \subset \mathbb{P}_K^2$, the elliptic curve given by the equation

$$Y^2Z - YZ^2 = X^3 - X^2Z$$

over the field $K = \mathbb{F}_2$.

As we have seen we have $\#(D(\mathbb{F}_2)) = 5$ (an easy computation, solving an equation modulo 2). By

$$\#(D(\mathbb{F}_2)) = 5 = 1 - (\alpha + \beta) + 2,$$

$$\beta = \frac{2}{\alpha}, \quad \alpha + \frac{2}{\alpha} = 2,$$

we see

$$\alpha, \beta = -1 \pm \sqrt{-1}.$$

We conclude that for every $m \in \mathbb{Z}_{>0}$ we have

$$\begin{aligned} \#(D(\mathbb{F}_{2^m})) &= 1 - ((-1 \pm \sqrt{-1})^m \\ &\quad + (-1 \pm \sqrt{-1})^m) + 2^m. \end{aligned}$$

(I find it astonishing that this theory after an easy computation gives this complete result.)

Let us see how this works out in simple examples. As the group $D(\mathbb{F}_4)$ has $D(\mathbb{F}_2) \cong \mathbb{Z}/5$ as a subgroup, and $\#(D(\mathbb{F}_4)) \leq 2 \cdot 4 + 1 = 9$ we conclude $\#(E(\mathbb{F}_4)) = 5$ (this can also be seen by an easy computation), and indeed:

$$\begin{aligned} \alpha^2, \beta^2 &= \mp 2\sqrt{-1}, \\ \#(E(\mathbb{F}_4)) &= 1 - (\alpha^2 + \beta^2) + 4 = 5. \end{aligned}$$

Something you would not like to compute without the preceding theory ($\alpha^{10}, \beta^{10} = 15 \mp 8\sqrt{-1}$):

$$\#(D(\mathbb{F}_{1024})) = 1 - 30 + 1024 = 995.$$

I hope this convinces the reader that for any elliptic curve E over $\mathbb{F}_q$ after computing $\#(E(\mathbb{F}_q))$ this theory gives access to all $\#(E(\mathbb{F}_{q^m}))$.

An amusing example: we see that $\alpha^4, \beta^4 = (2\sqrt{-1})^2 = -4$; we obtain:

$$\#(D(\mathbb{F}_{16})) = 1 - (-4 - 4) + 16 = 25.$$

Here $|\#(D(\mathbb{F}_{16})) - 1 - 16| = 8 = 2\sqrt{16}$, a case where the Hasse bound is reached.

However, note that any result of the type pRH, the Riemann hypothesis in characteristic p , does not give any new result for the classical RH, for example:

$$\zeta_{\mathbb{Z}}(s) = \prod_p \zeta_{\mathbb{F}_p}(s) = \prod_p \frac{1}{1 - p^{-s}}$$

(and it seems we have gained nothing in the direction of the classical RH).

Remark. Instead of the definition given above of $Z_V(T)$ one can give the equivalent definition:

$$Z_V(T) = \sum_{\delta} \frac{1}{1 - T^{\deg(\delta)}},$$

where δ runs over all effective divisors of V defined over $\mathbb{F}_q$.

What is the structure behind such theorems, and how can these results be generalized to curves of higher genus, and to varieties of higher dimensions?

Gauss

In DA 358 [11] Gauss computes for certain elliptic curve the number of rational points over a prime field $\mathbb{F}_p$; in the last entry in his *Tagebuch* [12], Gauss discusses these results as a conjecture. In [30] on page 73 G.J. Rieger writes: “Diese Tatsache wurde ... übersehen und ist erst in neuere Zeit bemerkt worden. Damit ist auch die Richtigkeit der *Riemannschen Vermutung* für denjenigen Funktionenkörper nachgewiesen.” This claim puzzles me; it is not clear how computations by Gauss imply the pRH in case you do not know rationality, functional equation or something like that for the zeta function considered.

Proof of the pRH by Weil

André Weil had the insight for the correct approach to generalizations. He started to write foundations necessary for proofs. In the period 1946–1948 he proved the pRH for *algebraic curves of arbitrary genus* and for *abelian*

varieties. His proof starts with a simple, but fundamental observation.

For a variety V over $K = \mathbb{F}_q$ with $q = p^n$ the map which sends coordinates x_i of a point to x_i^q is a morphism

$$\text{Frob}_{V/K} = \pi_{V/K} : V \rightarrow V.$$

Important (and obvious) remark. Fixed points of the map $\pi^m : V \rightarrow V$ are exactly the $K_m = \mathbb{F}_{q^m}$ -rational points:

$$\left(V(\mathbb{F}_q) \right)^{(\text{fix } \pi^m)} = V(\mathbb{F}_{q^m}).$$

Let us compare this with the result (for an elliptic curve) mentioned earlier:

$$\#(E(\mathbb{F}_{2^m})) = 1 - (\alpha^m + \beta^m) + 2^m.$$

What is an ‘interpretation’ of this formula, and how can we generalize this to arbitrary varieties (defined over a finite field)?

Further explanation. For a projective algebraic curve C over any field K one can define its *genus*, $g(C) \in \mathbb{Z}_{\geq 0}$; for a curve over $\mathbb{C}$ there is a topological definition; in algebraic geometry this can be extended to curves over any base field. A curve of genus zero is called a rational curve; a curve of genus one with a K -rational point is called an elliptic curve.

A projective, irreducible non-singular variety A such that this is a group variety is called an *abelian variety*.

An abelian variety of dimension one is an elliptic curve. Any curve C of genus g gives

rise to an abelian variety of dimension g , and many properties of C can be read off from properties of this abelian varieties. This abelian variety is called the Jacobian of C , or the Picard variety of C or the Albanese variety of C ; these notions coincide in case C has at least one point rational over the base field. It is not deep (although it requires some work) that proving pRH for all curves amounts to the same as proving pRH for all abelian varieties. An abelian variety A is called simple if there is no non-zero proper sub-abelian variety $0 \neq B \subsetneq A$.

The terminology ‘abelian variety’ stems from the fact that Niels Henrik Abel studied values of path-integrals of differentials on a Riemann surface; their values naturally lie in the related abelian variety, once you fix the end points of the path.

Remark. An abelian variety A over K is a group-object, the endomorphism algebra $\text{End}(A)$ is a ring, and the Frobenius $\text{Frob}_{A/K} \in \text{End}(A)$. In case A is simple, this ring has no zero divisors, is of characteristic zero, and is finitely generated as a $\mathbb{Z}$ -module: its field of fractions is a number field (a field of finite degree over $\mathbb{Q}$). Hence $\text{Frob}_{A/K}$ is (can be considered) as an algebraic integer. Here we see access to (pRH) in the case of abelian varieties, and hence in the case of algebraic curves.

Here are a version and a corollary of results by Weil (1948):

Theorem. For a simple abelian variety A defined over $K = \mathbb{F}_q$ its Frobenius homomorphism

$$\text{Frob}_{A/K} = \pi : A \rightarrow A$$

is an algebraic integer, and under every embedding $\psi : \mathbb{Q}(\pi) \rightarrow \mathbb{C}$ we have

$$|\psi(\pi)| = \sqrt{q}.$$

An amazing result: a ‘nature given’ endomorphism of a difficult object in positive characteristic turns out to be an algebraic integer having easy properties. It is easy to characterize and to produce such numbers (e.g. any zero of $T^2 + bT + q$ with $b \in \mathbb{Z}$ and $b^2 < 4q$; many more examples can easily be given).

Remark (details not explained nor discussed here). Conversely, an algebraic integer π with properties as in the theorem determines (an isogeny class of) an abelian variety A over $\mathbb{F}_q$ such that $\text{Frob}_{A/K} = \pi$ (Honda-Tate the-

ory): abelian varieties over a finite field can be constructed by just computing an algebraic integer having easy properties.

This theorem by Weil also proves the pRH for algebraic curves defined over a finite field. Reminder: a proof for the pRH for algebraic curves defined over a finite field implies the pRH for abelian varieties over a finite field.

Weil had two proofs. One proof relies on an analogue of a classical inequality (Castelnuovo-Severi) for correspondences on algebraic curves. Another proof (in this case for abelian varieties) uses the result that the Frobenius $\pi = \pi_{A/K} : A \rightarrow A$ for an abelian variety over $\mathbb{F}_q$ and its ‘transpose’ π^t (the image of π under the Rosati involution) satisfy $\pi \cdot \pi^t = q$. As π^t equals the complex conjugate of π , under any embedding ψ into $\mathbb{C}$, we easily conclude $|\psi(\pi)| = \sqrt{q}$.

In order to achieve such results Weil developed many aspects of algebraic geometry over an arbitrary field (in this case a field of characteristic p). Note that Pierre Deligne was born in 1944.

Corollary (The Hasse–Weil bound). For a non-singular, projective algebraic curve C of genus g over $K = \mathbb{F}_q$ we have

$$|\#(C(\mathbb{F}_q)) - 1 - q| \leq 2g\sqrt{q}.$$

Indeed, $\#(C(\mathbb{F}_q)) - 1 - q = -\sum_i \alpha_i$ and $|\alpha_i| \leq \sqrt{q}$.

Remark. For elliptic curves, $g = 1$, we find this in [19, III, p. 206].

The Weil conjectures

We will especially look into the RH for varieties over finite fields.

Reminder. For a curve C defined over $K = \mathbb{F}_q$, the pRH is just a statement on the asymptotic behavior of $\#(C(\mathbb{F}_{q^m}))$ for $m \rightarrow \infty$.

As we have seen, for a variety V over $K = \mathbb{F}_q$, with $q = p^n$, the map which sends coordinates x_i of a point to x_i^q is a morphism

$$\text{Frob}_{V/K} = \pi_{V/K} : V \rightarrow V$$

and $V(\mathbb{F}_{q^m})$ is the set of fixed points of $\text{Frob}_{V/K}^m$.

André Weil made in 1949 the following conjecture:

Conjecture. Let V be a non-singular, projective variety of dimension d defined over the



André Weil (1906–1998)

finite field $K = \mathbb{F}_q$ having q elements. Then:

1. Rationality. The zeta function is a rational function with coefficients in $\mathbb{Z}$ in $T := q^{-s}$:

$$Z(V/K, T) = \frac{P_1 \times P_3 \times \cdots \times P_{2d-1}}{P_0 \times P_2 \times \cdots \times P_{2d}}$$

with

$$P_j \in \mathbb{Z}[T], \quad P_0 = 1 - T, \quad P_{2d} = 1 - q^d T.$$

2. Analog of the classical Riemann Hypothesis. The polynomials $P_1, \dots, P_{2d-1}$ factor over $\mathbb{C}$ as

$$(\text{pRH}) \quad P_k(T) = \prod_j (1 - \alpha_{k,j} T),$$

$$\text{with } |\alpha_{k,j}| = \sqrt{q^k}.$$

Moreover there should be a functional equation, Poincaré duality and an explanation of the degrees of the polynomials P_k in terms of geometry of V : they should be (the analogues of) the ‘Betti numbers’; if V is the reduction mod p of a complex variety, these numbers should be the Betti number in the complex-topological sense. These together are called the ‘Weil conjectures’.

We have seen this conjecture to be true for $\mathbb{P}^d$, for algebraic curves and for abelian varieties. The conjecture above is a daring generalization. How did Weil come to this insight? We will see that methods of algebraic topology have their counterpart in arithmetic geometry.

Cohomology as predicted by Weil

- Weil used in his proofs an interpretation and generalizations of the notion of correspondences as studied in the classical Italian algebraic geometry. Also aspects of the theory of abelian varieties were generalized to properties over arbitrary fields.
- It might very well be that Weil originally had from the beginning a deeper motivation behind his ideas.
- In 1949 Weil stated his famous conjectures,
- and in the ICM in 1954 he describes why these should be true, and what could be a way to prove these.

His idea how to proceed is of a great beauty, of deep insight and of daring courage. Note that Pierre Deligne graduated from high school in Brussels in 1962. This insight by Weil started a new chapter in arithmetic algebraic geometry, a revolution, and a whole new setup of



Solomon Lefschetz (1884–1972)

algebraic geometry with new insights and new conjectures.

Here is that idea. We try to compute the number of rational points on a variety V defined over $\mathbb{F}_q$ over any finite field containing $\mathbb{F}_q$. The zeta function encodes

$$N_m = \#(V(\mathbb{F}_{q^m})) \quad \text{for all } m > 0.$$

We have seen that N_m is the number of fixed points under the operator $(\text{Frob}_{V/K})^m$.

In a completely different branch of mathematics Lefschetz has indicated how to compute the number of fixed points of an operator:

The Lefschetz fixed-point theorem (first stated in 1926). *For a continuous map $f: X \rightarrow X$ from a compact triangulable space X to itself, such that f has a finite set $\mathcal{F} = X^{\text{fix } f}$ of fixed points, and such that the graph of f intersects the diagonal in $X \times X$ transversally the trace formula computes the number of fixed points:*

$$\#(\mathcal{F}) = \sum_{k \geq 0} (-1)^k \text{Tr}(f_* | H_k(X, \mathbb{Q})).$$

Let us compare this with the result for an algebraic curve mentioned earlier:

$$\#(C(\mathbb{F}_{q^m})) = 1 - \sum_{i=1}^{2g} \alpha_i^m + q^m.$$

“Je gaat het pas zien als je het doorhebt”, as Johan Cruijff says. I would paraphrase: “Once you see it you understand it.”

This is the *Lefschetz fixed point formula* in

the following disguise:

- Show the graph of Frobenius is transversal to the diagonal (and this is easy).
- Find some (co)homology theory (?!!) such that the traces of $(\text{Frob}_{V/K})^m$ on H^k for all $k \in \{0, 1, \dots, 2 \cdot \dim(V)\}$ give the zeta-function of V/K . We should have $H^k = 0$ for $k < 0$ and $k > 2 \cdot \dim(V)$.

In the case of an algebraic curve this should be:

- The trace of the Frobenius on the one-dimensional H^0 should be 1.
- The trace of $(\text{Frob}_{C/K})^m$ on H^1 should be $\sum_{i=1}^{2g} \alpha_i^m$.
- The trace of the Frobenius on the one-dimensional H^2 should be q .

For an algebraic curve of genus g the degree of P_1 should be equal to $2g$. For algebraic varieties of higher dimension the polynomials $P_1, \dots, P_{2d-1}$ should be given in an analogous way. If so, we conclude (!):

$$\begin{aligned} \#(C(\mathbb{F}_{q^m})) &= \text{Tr}(f^* | H^0) - \text{Tr}(f^* | H^1) \\ &\quad + \text{Tr}(f^* | H^2) \\ &= 1 - \sum_{i=1}^{2g} \alpha_i^m + q^m \end{aligned}$$

with $H^k = H^k(X, ?)$ and $f = \text{Frob}_{C/K}$.

I hope you see that earlier results by E. Artin, Schmidt, Hasse and Weil have a natural, geometric interpretation and generalization once you see this geometric approach, and once you find this elusive cohomology theory.

After this became clear, *once you see it you understand it*, we “only” had to find this mysterious cohomology theory, and prove it has the right properties. Then the Weil conjectures would follow.

Completely independent from these ideas Dwork (1923–1998) proved in 1960 rationality of the zeta function of a variety over a finite field [9]. Also Monsky/Washnitzer and Lubkin contributed.

Alexandre Grothendieck

In 1958 Grothendieck told us he was putting algebraic geometry on a new footing with the main goal (for the time being) to prove the Weil conjectures, see [13]. I remember I was present at his presentation. I did not understand his explanation, however there was one person in the audience who was very much ‘au courant’; then I did not not know yet the influence Serre would have on mathematics and also upon on me. Note that Pierre Deligne was 14 years old at that time.

Serre made several attempts to construct a ‘Weil cohomology’. His cohomology with values in the Witt vectors [35], 1958, did not bring this success.

His attempt to use ‘étale topology’ turned out to be fruitful. In Serre [36], 1958, we find the idea. In order to have the analogue of fiber spaces in algebraic geometry one should introduce a *new notion of covering*. Suppose $G \rightarrow H$ is a homomorphism between algebraic groups (e.g. dividing out an elliptic curve $E = G$ by a finite subgroup, $H = E/N$). We see this need not be locally trivial in the Zariski topology (e.g. if G is irreducible and N is a finite group, but $N \neq 0$), but the covering can be trivialized (locally) by an étale map to a Zariski open of H . Objects in this new notion of ‘covering’ are maps with certain properties onto Zariski open subsets. We see that the search for a proof can give new insights and constructions of radically new concepts.

This opened the way for Grothendieck to define a new notion of topologies, and to construct the sought-for cohomology theory. Grothendieck on page 104 of [13] seemed to be the first who used the term ‘Weil cohomology’.

Grothendieck, together with Michael Artin, Giraud, Michel Raynaud, Illusie, Deligne and many others managed to find the earlier elusive ‘Weil cohomology’. They were able to pin down basic properties. Here we record just some of these properties: fix the prime number p and choose another prime number $\ell \neq p$. It turned out that the best choice for a ring or field of constants was $\mathbb{Z}_\ell$, the ring

of ℓ -adic integers respectively the field $\mathbb{Q}_\ell$ of ℓ -adic numbers.

- For every variety V of dimension d over a field of characteristic p and for every choice of ℓ there exists a cohomology theory $H^*(V, \mathbb{Z}_\ell)$, the ‘étale cohomology’. (As usual, obtained by derived functors in some topology, here in the ‘étale topology’ of H^0).
- For this cohomology properties like duality and more other vital ingredients were proved.

From these Grothendieck and his co-workers derived:

- Rationality of $Z_V(T)$ and hence analytic continuation of $\zeta_V(s) = Z_V(q^{-s})$.
- A Lefschetz type of fixed point formula for the Frobenius morphism.
- Functional equation.

See [14] for a first description of these results. Proofs were described in various volumes of SGA. For example, see [10, 27–28, 39], [17, Appendix C] and also see [38].

However the property pRH, the characteristic p analogue of the Riemann hypothesis, still escaped proofs:

- (pRH) The eigenvalues of Frob_V on $H^i(V, \mathbb{Z}_\ell)$ have absolute value $\sqrt{q^i}$. Here the coefficient ring is $\mathbb{Z}_\ell$, the ring of ℓ -adic integers, where ℓ is a prime number different from p .

How to proceed? We see once the general machinery of cohomology developed, most of the aspects of the Weil conjectures followed by ‘pure thought’. However the analogue (pRH) of the Riemann Hypothesis seemed out of reach of abstract theory.

It is wonderful to see how various mathematicians did continue in different ways.

Generalization. Grothendieck came with much more general conjectures; a survey of these conjectures can be found in: [16, 21–24]. These ‘standard conjectures’ on algebraic cycles describe, amongst others, relations between algebraic cycles and the Weil conjectures. Once these would be proved the (pRH) would simply follow. A fascinating idea. However most of this material seems completely inaccessible for the time being.

Inspiration from other fields. Deligne tried to prove the (pRH) directly (as many others had tried). Finally he was convinced he could prove the (pRH), Deligne wrote to Serre and remembers: “I wrote him a letter ... I think he got it just before he had to go to the hospital for an operation of a torn tendon. He told me later that he went in a euphoric state be-

cause he knew now that the proof was roughly done.” See [32, p. 19].

A wonderful description of the proof to appear later in [4] we find in [40]. We will not — alas! — describe the beautiful proof of Deligne here. It seems much better either to read the original paper by Deligne, or to go through the description of Serre [40], or the description by Katz in [20].

Deligne knew aspects and difficulties of this problem inside out (“I had all these tools at my disposal”). Instead of finishing of the general program of Grothendieck on cycles (still a complete mystery), Deligne followed a suggestion by Serre: “I think it was Serre who told me about an estimate due to Rankin”; see [29] (or came the suggestion from Langlands?, see [20, p. 287]). This idea did put Deligne on the right track to finish the proof. However, as Deligne says: “It would have been much nicer if the program had been realized”, see [32, p. 18] (i.e. the program by Grothendieck: the proof of the Weil conjectures via the standard conjectures).

For a description of the prehistory see [33] (4 papers), [8, 26, 46], and references to E. Artin, F.K. Schmidt and Hasse cited above. For a description of the Weil conjectures, see: [10, 26–27, 44] and [17, Appendix C]. Work by Tate, see [41] can be seen as pre-history of Grothendieck’s standard conjectures. For a complete and beautiful survey of the prehistory, and of Deligne’s proof see [20]. For a survey of Deligne’s proof, see [40].

Pierre Deligne

Maybe the essence of mathematics of Pierre Deligne is described in his words: “Proofs in geometry make sense at that age because surprising statements have not too difficult proofs.” These words are telling us about his interests in mathematics already at a very early stage [32, p. 16]. I would like to see this as a qualification for all of his mathematical work. Throughout the years Deligne has amazed us by his clear insight and his beautiful and clear description of structures and proofs in mathematics.

We hope this note will give enough credit to all mathematicians on whose shoulders the theory was built (Euler, Riemann, Emil Artin, Hasse, Weil, Serre, Grothendieck and many others) on the one hand, and on the other hand it will show the quantum leap, the deep insight of Deligne that was vital in this proof of the Weil conjectures (well, a ‘surprising statement’, however not an easy proof).



Alexander Grothendieck

Photo: Archive of Winfried Scharlau



Pierre Deligne

Pierre Deligne was born in 1944 in Belgium. Already at a young age it was clear his insight and taste for deep mathematics could enable him to do extraordinary things. In the interview with Pierre Deligne in the Newsletter of the European Mathematical Society of September 2013 we obtain a clear picture of this modest and friendly person, see [32]. In the period Deligne was still in elementary school the father of a friend gave him Bourbaki mathematics to read. His ('excellent elementary school') teacher did put him in contact with Jacques Tits. In high school Deligne enjoys problems in geometry (see the citation above).

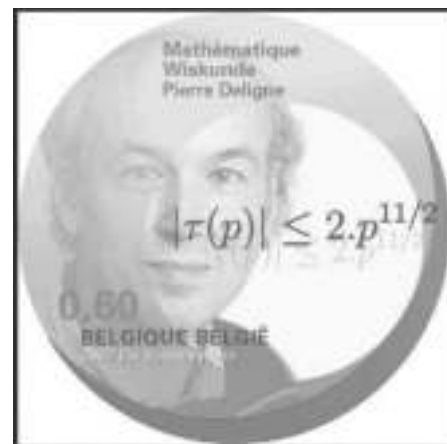
Deligne at age 16 joins a course by Jacques Tits, who comments: "A remarkable feature of Pierre Deligne's thinking is that, when confronted with a new problem or a new theory, he understands and, so to speak, makes his own its basic principles at a tremendous speed, and is immediately able to discuss the

problem or use the theory as a completely familiar object." See <http://www-history.mcs.st-and.ac.uk/Biographies/Deligne.html> I fully agree with this remarkable description. Indeed, you have the feeling: Pierre Deligne is "able to discuss the problem or use the theory as a completely familiar object".

With this ability he came under the influence of Serre (1926) and of Grothendieck (1928) (his official PhD-advisor) in his Paris years. Not only did he learn much from these two towering figures in algebraic geometry, but the respect and admiration was certainly reciprocal. In their correspondence Grothendieck complains to Serre that his 'anciens élèves' did not continue his work. Serre answers that this is not surprising: "You have the vision on a programme, and they do not have that (with the exception of Deligne, of course)", see [2, p. 244].

In his Paris period Deligne has an impressive production, not only in diversity of problems studied, but especially in depth of understanding. Grothendieck tries to prove the Weil conjectures, and Deligne witnessed, and collaborated at close range. In 1973 Deligne proves the last missing part, the Riemann hypothesis (pRH), in the program of the Weil conjectures. This is seen as his most prestigious achievement. For this he receives in 1978 the Fields medal. In 1984 Deligne moved to the Institute for Advanced Study in Princeton.

Let me mention here one of his theorems: The *Ramanujan-Petersson conjecture*. This is a statement about Fourier coefficients of an interesting modular form (no explanation given here). Ramanujan conjectured their absolute values should satisfy inequalities as printed on a Belgium stamp. In 1971 Deligne proved this would follow from pRH. Hence the proof (1974) of the aspect pRH of



Pierre Deligne on a Belgian postage stamp

the Weil conjectures implies the Ramanujan-Petersson conjecture holds true. E.g. see [25, 6.4.1].

Pierre Deligne

Some of his many awards:

Abel Prize (2013)
Wolf Prize (2008)
Balzan Prize (2004)
Crafoord Prize (1988)
Fields Medal (1978)

Timeline:

1944 Born
1962 Finishes High School
1966 Finishes University (Free University Brussels)
1968 PhD University of Paris-Sud (France)
1972 Doctorat d'État des Sciences Mathématiques
1968–1970, 1970–1984 IHES Bures sur Yvette (France)
≥ 1984 IAS Princeton (USA)

References

- 1 E. Artin, Quadratische Körper im Gebiet der höheren Kongruenzen, I and II, *Math. Zeitschr.* 19 (1924), 153–206, 207–246.
- 2 P. Colmez and J.-P. Serre, eds., *Correspondance Grothendieck–Serre*, Documents Mathématiques (Paris), No. 2, Soc. Math. France, Paris, 2001. Translated and edited as a bilingual version by the American Mathematical Society in 2003.
- 3 P. Deligne, Formes modulaires et représentations ℓ -adiques, Exp. 355 in *Sém. Bourbaki, 1968/69*, Lecture Notes in Mathematics, No. 179, Springer, Berlin, New York, 1971.
- 4 P. Deligne, La conjecture de Weil: I, *Publications Mathématiques de l'IHÉS* 43 (1974), 273–307.
- 5 P. Deligne, La conjecture de Weil: II, *Publications Mathématiques de l'IHÉS* 52 (1980), 137–252.
- 6 P. Deligne and D. Mumford, The irreducibility of the space of curves of given genus, *Publications Mathématiques de l'IHÉS* 36 (1969), 75–109.
- 7 P. Deligne and J.-P. Serre, Formes modulaires de poids 1, *Annales scientifiques de l'École Normale Supérieure, Sér. 4* 7 (1974), 507–530.
- 8 J. Dieudonné, On the history of the Weil conjectures, *The Mathematical Intelligencer* 10 (1975), 7–21. Reprinted in [10], pp. IX–XVIII.
- 9 B. Dwork, On the rationality of the zeta function of an algebraic variety, *American Journal of Mathematics* 82 (1960), 631–648.
- 10 E. Freitag and R. Kiehl, *Etale Cohomology and the Weil Conjecture*, with an historical introduction by J.A. Dieudonné, *Ergebnisse der Mathematik und ihrer Grenzgebiete* 3 Folge, No. 13, Springer, 1988.
- 11 C. Gauss, *Disquisitiones Arithmeticae*, Fleischher, Leipzig, 1801. Translation by A. Clarke: *Disquisitiones Arithmeticae*, Yale University Press, 1965.
- 12 C. Gauss, *Tagebuch 1796–1814*. Rediscovered (1897) and published (1903) by F. Klein; C. Gauss, *Mathematisches Tagebuch 1796–1814*, edited by K.-R. Biermann, *Ostwalds Klassiker der Exakten Wissenschaften*, No. 256 (5th ed.), Verlag Harri Deutsch, Frankfurt am Main, 2005.

- 13 A. Grothendieck, The cohomology theory of abstract algebraic varieties, *Proc. Internat. Congress Math. (Edinburgh, 1958)*, Cambridge Univ. Press, New York, 1960, pp. 103–118.
- 14 A. Grothendieck, Formule de Lefschetz et rationalité des fonctions L , Exp. 279 in *Sém. N. Bourbaki, 1964–1966*, pp. 41–55.
- 15 A. Grothendieck, Formule de Lefschetz et rationalité des fonctions L , in *Dix exposés sur la cohomologie des schémas*, Advanced Studies in Pure Mathematics, No. 3, North-Holland, Amsterdam; Masson et Cie, Éditeur, Paris, 1968; Exp. III, pp. 31–45.
- 16 A. Grothendieck, Standard conjectures on algebraic cycles, *Algebraic Geometry (Internat. Colloq., Tata Inst. Fund. Res., Bombay, 1968)*, Oxford University Press, 1969, pp. 193–199.
- 17 R. Hartshorne, *Algebraic Geometry*, Graduate Texts in Mathematics, No. 52, Springer, 1977.
- 18 H. Hasse, Abstrakte Begründung der komplexen Multiplikation und Riemannsche Vermutung in Funktionenkörpern, *Anh. Math. Sem. Hamburg* 10 (1934), 325–348.
- 19 H. Hasse, Theorie der höheren Differentiale in einem algebraischen Funktionenkörper mit vollkommenem Konstantenkörper bei beliebiger Charakteristik, I, II and III, *Journ. reine angew. Math. (Crelle)* 175 (1936), 55–62, 69–88 and 193–208.
- 20 N. Katz, An overview of Deligne's proof of the Riemann hypothesis for varieties over finite fields, in *Mathematical Developments Arising from Hilbert Problems* (Proc. Sympos. Pure Math., Vol. XXVIII, Northern Illinois Univ., De Kalb, Ill., 1974), Amer. Math. Soc., Providence, RI, 1976, pp. 275–305.
- 21 S. Kleiman, Algebraic cycles and the Weil conjectures, *Dix exposés sur la cohomologie des schémas*, Advanced Studies in Pure Mathematics, No. 3, North-Holland, Amsterdam, and Masson et Cie, Éditeur, Paris, 1968, pp. 359–386.
- 22 S. Kleiman, Motives, in *Algebraic Geometry*, F. Oort, ed., Proc. Fifth Nordic Summer School in Math., Oslo, 1970, pp. 53–82; Appendix I, Finiteness theorems for algebraic cycles, pp. 83–88.
- 23 S. Kleiman, Finiteness theorems for algebraic cycles, *Actes du Congrès International des Mathématiciens (Nice, 1970)*, No. 1, Gauthier-Villars, Paris, 1971, pp. 445–449.
- 24 S. Kleiman, The standard conjectures, *Motives* (Seattle, WA, 1991), Proceedings of Symposia in Pure Mathematics, No. 55, American Mathematical Society, 1994 pp. 3–20.
- 25 Yu. Manin and A. Panchishkin, *Introduction to Modern Number Theory: Fundamental Problems, Ideas and Theories*, Springer, 2007, 2nd ed.
- 26 B. Mazur, Eigenvalues of Frobenius acting on algebraic varieties over finite fields, *Algebraic Geometry* (Humboldt State Univ., Arcata, Calif., 1974), Proc. Sympos. Pure Math., No. 29, Amer. Math. Soc., Providence, RI, 1975, pp. 231–261.
- 27 J. Milne, *Etale cohomology*, Princeton Mathematical Series, No. 33, Princeton University Press, Princeton, NJ, 1980.
- 28 J. Milne, Lectures on etale cohomology, Notes for a course taught at the University of Michigan in 1989 and 1998. <http://www.jmilne.org/math/CourseNotes/lec.html>
- 29 R. Rankin, Contributions to the theory of Ramanujan's function $\tau(n)$ and similar arithmetical functions, *Math. Proc. Cambridge Philos. Soc.* 35 (1939), 357–372.
- 30 G. Rieger, Die Zahlentheorie bei C.F. Gauss, in *C.F. Gauss Gedenkband anlässlich des 100 Todestages am 23. Februar 1955*, Teubner, 1957, pp. 37–77.
- 31 B. Riemann, Über die Anzahl der Primzahlen unter einer gegebenen Grösse, *Monatsberichte der Berliner Akademie*, November 1859, 6 pp; in *Monath. der Kön. Preuss. Akad. der Wissen. zu Berlin aus der Jahre 1859* (1860), 671–680; also in *Gesammelte math. Werke und wissenschaft. Nachlass* 2 (1892), 145–155. <http://www.claymath.org/millennium/Riemann.Hypothesis/1859.manuscript>, http://en.wikipedia.org/wiki/On_the_Number_of_Primes_Less_Than_a_Given_Magnitude
- 32 M. Raussen and C. Skau, Interview with Abel laureate Pierre Deligne, *Newsletter European Math. Soc.* 89 (2013), 15–23.
- 33 P. Roquette, The Riemann hypothesis in characteristic p , its origin and development. Part I: The formation of the zeta-functions of Artin and of F. K. Schmidt, in *Hamburger Beiträge zur Geschichte der Mathematik*, Mitt. Math. Ges. Hamburg, No. 21 (2002), 79–157; Part 2: The first steps by Davenport and Hasse, No. 22 (2004) 5–74; Part 3: The elliptic case, No. 25 (2006), 103–176; Part 4: Davenport–Hasse fields, No. 32 (2012) 145–210.
- 34 F. K. Schmidt, Analytische Zahlentheorie in Körpern der Charakteristik p , *Math. Zeitschr.* 33 (1931), 1–32 (Habilitationsschrift).
- 35 J-P. Serre, Sur la topologie des variétés algébriques en caractéristique p , *Symposium internacional de topología algebraica*, Mexico (1958), pp. 24–53.
- 36 J-P. Serre, Espaces fibrés algébriques, in *Anneaux de Chow et applications*, Sém. C. Chevaly E.N.S., No. 2 (1958), pp. 1-01–1-37; also in J-P. Serre, *Exposés de séminaires (1950–1999)*, 2nd ed., Docum. Math., No. 1, Soc. Math. France, 2008, pp. 107–140.
- 37 J-P. Serre, Rationalité des fonctions ζ des variétés algébriques, Exp. 198 in *Sém. Bourbaki, 1959/60*, No. 12.
- 38 J-P. Serre, Zeta and L functions, in *Arithmetical Algebraic Geometry* (Proc. Conf. Purdue Univ., 1963), Harper & Row, New York, 1965, pp. 82–92.
- 39 J-P. Serre, Facteurs locaux des fonctions zêta des variétés algébriques (définitions et conjectures), No. 19 in *Sém. Delange–Pisot–Poitou* 11 (1969/70).
- 40 J-P. Serre, Valeurs propres des endomorphismes de Frobenius, Exp. 446 in *Sém. Bourbaki, 1973/1974*.
- 41 J. Tate, Algebraic cycles and poles of zeta functions, in *Arithmetical Algebraic Geometry* (Proc. Conf. Purdue Univ., 1963), Harper & Row, New York, 1965, pp. 93–110.
- 42 A. Weil, Sur les fonctions algébriques à corps de constantes fini, *C.R. Acad. Sci. Paris* 210 (1940), 592–594.
- 43 A. Weil, On the Riemann hypothesis in function fields, *Proc. Nat. Acad. Sci. U.S.A.* 27 (1941), 345–347.
- 44 A. Weil, Numbers of solutions of equations in finite fields, *Bull. Amer. Math. Soc.* 55 (1949), 497–508.
- 45 A. Weil, Abstract versus classical algebraic geometry, in *Proceedings of the International Congress of Mathematicians, 1954, Amsterdam*, Vol. III, Noordhoff, Groningen, and North-Holland, Amsterdam, 1956, pp. 550–558.
- 46 A. Weil, Prehistory of the zeta-function, in *Sympos. Atle Selberg (1987): Number Theory, Trace Formulas and Discrete Groups*, A. Aubert, E. Bombieri and D. Goldfeld, eds., Acad. Press, 1989.
- 47 <http://www.claymath.org/millennium/Riemann.Hypothesis/riemann.pdf>
- 48 <http://www.claymath.org/millennium/Riemann.Hypothesis/riemann.pdf>

Ionica Smeets

wetenschapsjournalist, Leiden

i@ionica.nl

Voorpublicatie Het exacte verhaal – Wetenschapscommunicatie voor bèta's

Waarom zou je?

Ionica Smeets, bij de lezers van dit blad bekend van 'Het keerpunt', schrijft columns, geeft regelmatig voordrachten en werkt mee aan TV-programma's. In augustus was zij nog te zien als zomergast. In haar nieuwe boek *Het exacte verhaal* geeft zij een lesje wetenschapscommunicatie voor bèta's. Het boek wordt op donderdag 2 oktober 2014 officieel gepresenteerd in NEMO. Dit artikel is een voorpublicatie van het tweede hoofdstuk uit het boek: 'Waarom zou je? Over nut, inspiratie en plezier'.

Waarom zou je in hemelsnaam op vrijdagavond in de bibliotheek van Haaksbergen over je onderzoek vertellen? Waarom zou je je best doen om jouw prachtige vakgebied in één schamel A4'tje samen te vatten voor leken? En waarom zou je in een muf klaslokaal een groep onverschillige pubers toespreken? Kortom: waarom zou je aan wetenschapscommunicatie doen? Op die vraag zijn veel verschillende antwoorden mogelijk.

Maatschappelijk nut

Puur uit eigenbelang moeten wetenschappers zorgen dat hun werk door de maatschappij wordt gedragen, anders is het lastig om aan subsidies te komen. PvdA-politicus Diederik Samsom sprak eens een zaal natuurkundigen toe in de tijd dat de politiek net flink had bezuinigd op kunst. Natuurkundige Ivo van Vulpen zat in de zaal en lette goed op.

"Samsom is zelf natuurkundige. Als wij het als natuurkundigen van iemand in de politiek moeten hebben, is hij het. Maar hij waarschuwde ons dat het niet vanzelfsprekend is dat er geld naar fundamenteel onderzoek gaat. Daar moet je aan werken. Het is niet genoeg om jezelf belangrijk te vinden, je moet juist over natuurkunde praten op plaatsen waar mensen het eigenlijk niet

willen horen. Je moet naar plekken gaan waar je normaal niet komt. Samsom had natuurlijk gelijk. Als je mensen via een referendum vraagt waar subsidiegeld naartoe moet, gaan ze niet zomaar stemmen voor onderzoek naar het Higgs-deeltje. Je moet ze laten zien waarom je vak nuttig is."

Iedereen gebruikt elke dag dingen die er niet waren geweest zonder wetenschap, al staan de meeste mensen daar nooit bij stil. Sterker nog, ze hebben geen idee hoe hun navigatiesysteem eigenlijk werkt, of wat er achter de schermen gebeurt als ze op internet met een creditcard betalen. Door uit te leggen welke ideeën en principes achter deze alledaagse voorwerpen of handelingen zitten, help je mensen om het belang van exacte wetenschap in te zien.

De weg wijzen

Het is voor een buitenstaander helemaal niet zo makkelijk om iets over een bèta-onderwerp te leren. Als ik als wiskundige iets wil weten over geschiedenis, kunst, of zelfs economie, dan is dat relatief eenvoudig. Er is een hele stapel toegankelijke literatuur. Ik kan naar lezingen en avondcursussen. Maar als een alfa besluit dat hij meer wil weten over wiskunde, is dat een stuk ingewikkelder. Daarom vind ik

het een morele plicht om iedereen die interesse toont in mijn vakgebied zo goed mogelijk de weg te wijzen. Het is ook een natuurlijke impuls om dingen die je mooi vindt te delen met anderen. Soms lees ik een boek dat ik zo mooi vind, dat ik het aan al mijn vrienden cadeau wil geven. Of hoor ik een nummer dat ik zo goed vind, dat ik het draai iedere keer als er visite is. Hetzelfde geldt voor mooie ideeën uit de wiskunde: daar raak ik zo enthousiast over, dat ik sta te popelen om ze aan anderen te vertellen. Of zoals Lieven Scheire — van oorsprong natuurkundige, maar inmiddels vooral stand-up comedian en tv-presentator — zegt:

"Een grote Van Gogh-kenner praat graag over diens schilderijen, op diezelfde manier wil ik graag vertellen over fysica. Die drive is hetzelfde."

Helaas is het moeilijker om een enthousiast publiek te vinden voor een verhaal over relativiteitstheorie dan voor een spannende thriller. Maar als je aan popularisering doet, ontmoet je vanzelf de mensen die dezelfde dingen mooi vinden als jij.

Bioloog Freek Vonk presenteert tv-programma's, geeft lezingen en schrijft columns over zijn werk. Hij snapt niet waarom niet meer collega's doen wat hij doet.

"Alle wetenschappers praten graag over hun werk. Je doet wetenschap niet voor het geld, maar vanwege je passie, de fascinatie voor je vak. Dan is het toch waanzinnig gaaf om daarover te praten? Wetenschappers doen dat ook wel, alleen het liefst met hun collega's. Maar het is juist zo leuk om erover te vertellen aan een algemeen publiek."

Over die collega's gesproken: maak je niet te druk over wat zij ervan vinden. Er is nog steeds een groep wetenschappers die gelooft dat collega's die in de media optreden per definitie prutters zijn. Vonk moet lachen om dat soort reacties:

"Er zijn mensen die mij meer als een tele-visiebioloog zien, dan als een serieuze wetenschapper. Dan denk ik: leg onze wetenschappelijke cv's maar eens naast elkaar, dan kijken we wel hoe het zit. De criteria waarop een wetenschapper uiteindelijk moet worden afge-rekend, zijn publicaties, subsidies en prijzen. Wat iemand daarnaast doet, staat los van zijn kwaliteit als wetenschapper. Ronald Plasterk werd door sommige collega's minder serieus genomen als wetenschapper toen hij bij Buitenhof columns ging voorlezen. Terwijl hij publicaties in Nature en Science op zijn naam had en de Spinozapremie won. Waar hebben we het dan over?"

Beroepseer

Het algemene imago van bèta's laat ook nog wel iets te wensen over. Ivo van Vulpen werkte bij CERN, toen hij op een terras in Genève een bankier ontmoette.

"We raakten aan de praat over ons werk. Hij vertelde dat hij zijn beslissingen nam op basis van modellen. Ik vroeg wie die modellen dan maakte. Zijn antwoord was: 'Mensen zoals jij, daar beneden in het gebouw.' Dat was zo denigrerend. Hij nam de mensen die de echte beslissingen bepaalden helemaal niet serieus. Het klonk alsof wij een inferieur soort mensen waren."

We mogen als bèta's weleens iets doen aan onze beroepseer. Bij andere vakgebieden lijken ze daar een stuk beter in, terwijl wij ook veel hebben om trots op te zijn. Als ik een inspirerende lezing over sterrenkunde zie, krijg ik altijd even spijt dat ik geen sterrenkunde heb gestudeerd (en bij andere vakgebieden gaat het precies zo). Maar tegelijkertijd ben ik trots om een bèta te zijn en toch nog een beetje bij de wetenschap te horen. Of zoals Ivo van Vulpen het verwoordt:

"Een keer, bij een lezing van Robbert Dijkgraaf, was ik helemaal trots dat ik ook een wetenschapper was. Zoals hij onderzoek presenteerde, dat was zo gaaf. Voor Nederland, voor de wereld, voor iedereen. En daar hoorde ik bij."

Dat gevoel moeten wij onszelf maar eens wat vaker bezorgen.

Meer inzicht

Als je wetenschap aan een algemeen publiek uitlegt, gaat het om de grote ideeën

en niet om de details. Zoals een beroemde wetenschapper ooit zei: "Een theorie is pas compleet als je hem zo helder hebt dat je hem aan de eerste de beste voorbijganger kunt uitleggen." Dit citaat, of varianten hierop met oma's of juist met zesjarigen, wordt vaak toegeschreven aan Albert Einstein of Richard Feynman. Het komt echter uit een toespraak van David Hilbert uit 1900 over de grote nog onopgeloste problemen in de wiskunde (zie www.mathematik.uni-bielefeld.de/~kersten/hilbert/rede.html). Ivo van Vulpen legt uit waarom deze uitspraak nog steeds waar is — of misschien wel meer dan ooit, nu wetenschap steeds specialistischer wordt:

"Als je echt diep in je werk zit, gaat het om technische details. Je praat nog maar weinig over concepten. Soms heb je daardoor niet eens door wat je niet begrijpt. Als student was ik heel goed in integralen oplossen. Op een gegeven moment zat ik naast een nieuwe jongen. We moesten een som doen en ik ging heel druk aan de slag om de oplossing te vinden. De jongen naast me dacht even na en zei dat het antwoord volgens hem een bepaalde afstand keer de gemiddelde snelheid van alle deeltjes moest zijn. Daarna schreef hij het goede antwoord in een keer op. Ik besepte toen in een klap dat ik wel een oplossing had, maar niet begreep waarom dat het antwoord was. Het gevaar is dat je niet loskomt van de formules. Pas als je met anderen deelt wat je aan het doen bent, merk je wat je eigenlijk niet begrijpt."

Een nieuwe generatie

Een andere reden om aan wetenschapscommunicatie te doen, is om een nieuwe generatie te inspireren. Als ik wetenschappers interview, vraag ik weleens of ze als kind al bezig waren met wetenschap. Vaak kunnen ze een persoon of gebeurtenis noemen die hun liefde voor het vak heeft aangewakkerd. Dat kan een leraar zijn, of een oom, maar ook een lezing of een boek.

De Britse wiskundige Marcus du Sautoy zag als kind bijvoorbeeld de *Royal Institution Christmas Lectures* van Christopher Zeeman en besepte dat hij ook wiskundige wilde worden. Freek Vonk mocht als puber een keer een tijgerpython aanraken en was verkocht. Natuurkundige Robbert Dijkgraaf zat op een basisschool die de leerlingen een onderzoekende houding wilde meegeven en hij bouwde als jonge jongen een telescoop om tot een microscoop. Zelf las ik Simon Singh's *Fermat's Last Theorem* en besloot dat wiskundigen de coolste mensen op aarde waren.

Door kinderen enthousiast te maken, garandeer je dat er na jou een nieuwe generatie onderzoekers doorgaat met jouw belangrijke werk.

Het is zo leuk

De laatste maar belangrijkste reden om aan popularisering te doen, is omdat het ontzettend leuk is (zoals iedereen beaamt die ik voor dit boek interviewde). Ivo van Vulpen vat te het zo samen:

"Soms zit je vast in je onderzoek en zorgt dat voor allemaal gedoe. Maar als je dan een lezing geeft in een Science Café en er komen na afloop een paar mensen enthousiast naar je toe, kun je er weer een week tegen."

En Lieven Scheire concludeert ook dat het plezier uiteindelijk het belangrijkste is:

"De bedrijven waar ik kom, zeggen allemaal hetzelfde: geef ons meer onderzoekers, ingenieurs, natuurkundigen, chemici en informatici. Toch is dat niet de reden dat ik mijn werk doe. Stel dat ik in een land woonde met een grote oorlogsdreiging en er meer soldaten nodig waren. Dan zou ik toch niet uit een maatschappelijk bewustzijn het leger gaan promoten. De hoofdrede is toch dat je graag praat over waar je enthousiast over bent."



Ionica Smeets, *Het exacte verhaal*, Uitgeverij Nieuwezijds, ISBN 9789057123931, prijs € 19,95. De officiële boekpresentatie vindt plaats op 2 oktober 2014 in NEMO, zie ook: www.nieuwezijds.nl.

Problemen

Problem Section

This Problem Section is open to everyone; everybody is encouraged to send in solutions and propose problems. Group contributions are welcome.

For each problem, the most elegant correct solution will be rewarded with a book token worth €20. At times there will be a Star Problem, to which the proposer does not know any solution. For the first correct solution sent in within one year there is a prize of €100.

When proposing a problem, please either include a complete solution or indicate that it is intended as a Star Problem. Electronic submissions of problems and solutions are preferred (problems@nieuwarchief.nl).

The deadline for solutions to the problems in this edition is 1 December 2014.

All three problems ask for a construction with origami in a limited number of moves.

More precisely, given a collection of points and lines (or *folds*) in the plane, a *move* (cf. the Huzita–Justin–Hatori axioms) consists of adding to the collection one of the following:

- a fold aligning two distinct points;
- a fold aligning two distinct lines;
- if it exists, a fold having two properties of the following types (except for type 3, one may have two distinct alignments of the same type):
 1. the fold aligns a point with a line;
 2. the fold passes through a point;
 3. the fold is perpendicular to a line;
- a sufficiently general fold having at most one property of types 1, 2 and 3.

For example, given points P_1 and P_2 and lines l_1 and l_2 , examples of moves are adding a fold that aligns P_1 with l_1 and P_2 with l_2 (having two properties of type 1), and adding a fold perpendicular to l_2 aligning P_1 with l_1 (having a property of type 1 and one of type 3). (These two example moves correspond to axioms 6 and 7 from the Huzita–Justin–Hatori axioms.) At any time one is allowed to freely add any intersection point among the lines.

For example, one can construct a square (including its sides) in five moves as follows. First, make any fold l . Then make any two distinct folds l_A and l_B perpendicular to l . Let A and B be the intersections of l with l_A and l_B , respectively. Next, make a fold d aligning l and l_A , and denote its intersection with l_B by C . Finally, make the fold m perpendicular to l_A passing through C , and denote its intersection with l_A by D . Then $ABCD$ (together with the lines l , l_A , l_B , m) is a square.

Problem A

Given three points A , B , and C , and a line l passing through C , construct in at most six moves a point D on the line l such that $|CD| = |AB|$.

Problem B

Construct a golden rectangle (including its sides) in at most eight moves.

Problem C

Given two points A and B , construct in at most four moves the point C on the segment AB such that $|AC| = \frac{1}{3}|AB|$.

Erratum to solution 2013-4/B. The map $h: A \otimes_{\mathbb{Z}} B \rightarrow C$ is not necessarily a *ring* homomorphism; it is just a $\mathbb{Z}$ -module homomorphism. Nevertheless, the natural maps $i: A \rightarrow A \otimes_{\mathbb{Z}} B$ and $j: B \rightarrow A \otimes_{\mathbb{Z}} B$ are ring homomorphism, so the proof is unaffected.

Redactie:

Johan Bosman

Gabriele Dalla Torre

Christophe Debry

Jinbi Jin

Marco Streng

Wouter Zomervrucht

Problemenrubriek NAW

Mathematisch Instituut

Universiteit Leiden

Postbus 9512

2300 RA Leiden

problems@nieuwarchief.nl

www.nieuwarchief.nl/problems

Edition 2014-1 We received solutions from Rik Bos (Bunschoten), Charles Delorme, Pieter de Groen (Brussels, Belgium), Alex Heinis (Amsterdam), Nicky Hekster (Amstelveen), Alexandervan Hoorn (Abcoude), Huub van Kempen (The Hague), Thijmen Krebs (Nootdorp), Hendrik Reuvers (Maastricht), Traian Viteam (Cape Town, South Africa), Robert van der Waall (Huizen) and Sander Zweegers (Cologne, Germany).

Problem 2014-1/A (proposed by Hendrik Lenstra)

Let G be a group, and let $a, b \in G$ be two elements satisfying $\{gag^{-1} : g \in G\} = \{a, b\}$. Prove that for all $c \in G$ one has $abc = cba$.

Solution We received solutions from Rik Bos, Pieter de Groen, Alex Heinis, Nicky Hekster, Alexander van Hoorn, Thijmen Krebs, Traian Viteam, Robert van der Waall and Sander Zwegers. All their solutions were along the same lines. The book token goes to Nicky Hekster.

The case $a = b$ is easy, so we assume $a \neq b$. We have $bab^{-1} \in \{a, b\}$ and $bab^{-1} = b$ would contradict $a \neq b$, hence we have $ba = ab$.

Note that $\{a, b\}$ is an orbit under the conjugation action, hence conjugation by c acts either by swapping a and b or by fixing both a and b .

In the latter case, the element c commutes with both a and b , which also commute with each other, hence $abc = cba$.

In the former case, we have $abc = a(cac^{-1})c = aca = c(c^{-1}ac)a = cba$.

Problem 2014-1/B (due to Albrecht Pfister [1])

Let K be a field, and consider for all positive integers n the subset S_n of $x \in K^*$ that can be written as the sum of n squares in K . Show that the subgroup of K^* generated by S_n is equal to $S_{t(n)}$. Here, for a positive integer n , we denote by $t(n)$ the smallest power of two that is greater than or equal to n .

Solution We received solutions by Rik Bos, Alex Heinis, Thijmen Krebs and Robert van der Waall. They all used or referred to Pfister's lemma. The book token goes to Thijmen Krebs.

For any $n \geq 1$ the set S_n contains 1, and if $x_1^2 + \dots + x_n^2$ is non-zero, then

$$(x_1^2 + \dots + x_n^2)^{-1} = \left(\frac{x_1}{x_1^2 + \dots + x_n^2} \right)^2 + \dots + \left(\frac{x_n}{x_1^2 + \dots + x_n^2} \right)^2.$$

Pfister's lemma. Let $n = 2^m$. For all $x \in S_n$ there exists an $n \times n$ -matrix X such that $XX^T = X^T X = xI_n$.

Proof. By induction on m . It is obvious for $m = 1$, so suppose the lemma is true for some $m \geq 1$. Any $x \in S_{2n}$ either lies in S_n , or is of the form $y + z$ with $y, z \in S_n$. In the first case, there is nothing to prove. In the second case, let Y, Z be matrices with $YY^T = Y^T Y = yI_n$ and $ZZ^T = Z^T Z = zI_n$. They exist by assumption. Let X be the block matrix

$$X = \begin{pmatrix} Y & Z \\ -(Y^{-1}ZY)^T & Y^T \end{pmatrix}.$$

Then $XX^T = X^T X = xI_n$ as desired. □

Let n be a power of 2. Take $x, y \in S_n$, and let X, Y be corresponding matrices. Then $Z = XY^T$ satisfies $ZZ^T = xyI_n$. If $z_1, \dots, z_n$ is the first row of Z , this implies $xy = z_1^2 + \dots + z_n^2$, hence S_n is closed under multiplication. It follows that S_n is a group.

It now suffices to show that for any $n \geq 1$ we have $S_{t(n)} \subseteq \langle S_n \rangle$. Write $t(n) = 2r$. Any $x \in S_{t(n)}$ is either in $S_r \subseteq \langle S_n \rangle$, or can be written as $y + z$ with $y, z \in S_r$. Then $x = y(1 + z/y)$ is the product of $y \in S_r$ and $1 + z/y \in S_{r+1}$, using that z/y lies in S_r since S_r is a group. It follows that x is in $\langle S_n \rangle$.

Problem 2014-1/C (folklore)

Given five pairwise distinct points A, B, C, D, E in the plane, no three of which are collinear, and given a line l in the plane not passing through any of the five points. Assume that l intersects the conic section c passing through A, B, C, D, E . Construct the intersection points of l and c .

Oplossingen

Solutions

Solution We received solutions from Charles Delorme (17 moves), Huub van Kempen (19 moves), and Hendrik Reuvers (20 moves). The book token goes to Charles Delorme. This solution below is based on that of Charles Delorme, Hendrik Reuvers and [2].

Rename the 5 points to A_1, A_2, A_3, X_1, X_2 . The construction is then as follows.

– For all $i \in \{1, 2, 3\}$ and $j \in \{1, 2\}$, draw the line $A_i X_j$. (6 moves)

Let B_{ij} be the intersection of $A_i X_j$ with l , for $i \in \{1, 2, 3\}$ and $j \in \{1, 2\}$. Note that the desired intersection points c with l then are the fixed points of the projectivity on l sending B_{i1} to B_{i2} for $i \in \{1, 2, 3\}$. The idea is now to project these points to a circle, and then use Steiner's double element construction (see e.g. [2]).

– Draw the circle Γ with centre X_2 passing through X_1 . (1 move)

– For all $i \in \{1, 2, 3\}$, draw the line $B_{i2} X_1$. (3 moves)

Let C_{ij} be the intersection of $B_{ij} X_1$ with Γ , for $i \in \{1, 2, 3\}$ and $j \in \{1, 2\}$. Note here that, for $i \in \{1, 2, 3\}$, $B_{i1} X_1 = A_i X_1$, a line that we have already drawn. We will now perform Steiner's double element construction.

– Draw the lines $C_{11} C_{32}, C_{12} C_{31}, C_{21} C_{32}, C_{22} C_{31}$. (4 moves)

Let $P_1 = C_{21} C_{32} \cap C_{22} C_{31}$ and $P_2 = C_{11} C_{32} \cap C_{12} C_{31}$.

– Draw $P_1 P_2$. (1 move)

Let Q_1 and Q_2 denote the two intersections of $P_1 P_2$ with Γ .

– Draw $Q_1 X_1$ and $Q_2 X_1$. (2 moves)

Let R_i ($i \in \{1, 2\}$) denote the intersection of $Q_i X_1$ with l . We have now used 17 moves. Moreover, by Steiner's double element construction, Q_1 and Q_2 were the fixed points of the projectivity such that $C_{i1} \mapsto C_{i2}$ for all $i \in \{1, 2, 3\}$, hence R_1 and R_2 are the intersection points of c with l , as desired.

References

1. Albrecht Pfister, Zur Darstellung von -1 als Summe von Quadraten in einem Körper, *J. London Math. Soc.* 40 (1965), 159–165.
2. H. Dörrie, *100 Great Problems of Elementary Mathematics, their History and Solution* (translation of *Triumph der Mathematik*, 1932), reworked in 2010 by M. Woltermann.