Wat is wiskunde?
Op zoek naar zekerheid

Klaas Landsman

"Voor zover de conclusies van de wiskunde met de werkelijkheid te maken hebben zijn ze niet zeker, en voor zover ze zeker zijn verwijzen ze niet naar de werkelijkheid."
(Albert Einstein)

Hoorcollege: maandag 10:45-12:30, HG.00.068
Weken: 6, 8-13, 16-17, 19-20, 22-25
Werkcollege: Groepen 1, 2, 3: vrijdag 13:45-15:30 in:
HG.01.058 (Arjo Buijtenweg)
HG.03.632 (John van de Wetering)
HG.01.139 (Valijn Verbart
Groep 4: vrijdag 15:45-17:30 in HG.00.071 (weken 6, 10, 11) (Abel Planting)
vrijdag 13:45-15:30 in HG.02.028 (weken 7-9, 16-17, 20-25) (idem)
Tentamen: vrijdag 28 juni 12:30-15:30 HAL 2

Radboud Universiteit Nijmegen
Institute for Mathematics, Astrophysics, and Particle Physics
Heyendaalseweg 135, 6525 AJ Nijmegen

CONCEPT: 27 FEBRUARI 2017
landsman@math.ru.nl

1

Inleiding

Wat is wiskunde? In de eerste plaats kan op deze vraag een beschrijvend antwoord worden gegeven: wiskunde is dat wat zich 'wiskundigen' noemende mensen doen. Dat doen ze al zo'n 2500 jaar en zullen ze, zolang de mensheid bestaat, hopelijk ook blijven doen. Uit historisch onderzoek in vooral de afgelopen vijftig jaar is duidelijk geworden dat het begrip wiskunde in een periode van slechts 40 jaar is ontstaan in het Athene van de vierde eeuw v.Chr., en dan in het bijzonder in Plato's Academie.[1] Deze periode liep van ongeveer 387 v.Chr., het jaar waarin Plato zijn Academie stichtte, tot de dood van Plato op tachtigjarige leeftijd in 348 of 347.[2] In deze periode werd een praktische bezigheid die duizenden jaren eerder in de Egyptische en Babylonische beschavingen was ontwikkeld als hulpmiddel bij zaken als astronomie, landmeetkunde, handel en belastinginning omgezet in een nieuwe wetenschap met een eigen taal en methodiek. De wezenlijke kenmerken van de moderne wiskunde, namelijk haar axiomatisch-deductieve opbouw en het abstracte karakter van wiskundige objecten en structuren, dateren uit het genoemde tijdvak.[3] Euclides, Archimedes en Apollonios, van wie de werken pas in de derde eeuw v.Chr. verschenen, troffen dit raamwerk vrijwel voltooid aan en vulden het verder in.

Wiskunde heeft zo te zien iets te maken met getallen, figuren, axioma's, stellingen, en bewijzen. Bovendien maken andere vakken er gebruik van. Traditioneel was dat de sterrenkunde, vanaf de 17e eeuw ook de natuurkunde,[4] en in de 20e eeuw kwam daar de informatica bij.[5] Inmiddels is wiskunde het onzichtbare fundament van een belangrijk deel van onze technologische infrastructuur, bijvoorbeeld:

- Dienstregeling NS (grafentheorie en combinatorische optimalisatietheorie);
- TomTom (positiebepaling m.b.v. driehoeksberekeningen vanuit gps-data, en tevens kortste-pad algoritmen voor de routebepaling met soortgelijke technieken als bij de NS);
- Elektronisch betalingsverkeer (versleuteling m.b.v. rekenkunde en algebraïsche meetkunde);
- MP3/AAC muziekspelers (datacompressie m.b.v. Fourier-analyse);
- Mobiele telefonie (stochastische netwerktheorie en alle tot nu toe genoemde technieken);
- Google (page ranking methode gebruikt lineaire algebra);
- Bank-, verzekerings-, en pensioenwezen (statistiek, analyse, wiskundig modelleren);
- Algoritmische handelssystemen op de beurs (wiskunde geheim!);
- Containertransport in de Rotterdamse haven (optimalisatie, lineair programmeren).

---

1. Zie bijvoorbeeld F. Laserre, *The Birth of Mathematics in the Age of Plato* (Londen, 1964), D.H. Fowler, *The Mathematics of Plato's Academy* (Oxford, 1987), R. Netz, *The Shaping of Deduction in Greek Mathematics* (Cambridge, 1999) en, enigszins verouderd maar nog steeds heerlijk leesbaar, *Ontwakende Wetenschap* door B.L. van der Waerden (Groningen, 1950). Het is een wijdverbreid misverstand Pythagoras een belangrijke rol in de geschiedenis van de wiskunde toe te schrijven; zie W. Burkert, *Weisheit und Wissenschaft: Studien zu Pythagoras, Philolaos und Platon* (Nürnberg, 1962). Over de wiskundige activiteiten van Thales van Milete is te weinig bekend om hem in deze context een prominente plaats te geven.
2. Naast Plato's eigen vertrek uit het leven verlieten rond die tijd ook Eudoxos (naar verluidt de grootste wiskundige van zijn tijd) en Plato's belangrijkste leerling Aristoteles (in deze geschiedenis de rol spelend van de grondlegger van de logica) Athene.
3. Ofschoon concrete wiskundige resultaten van Plato zelf niet bekend zijn, speelde hij in deze ontwikkeling vermoedelijk een beslissende rol. Ten eerste hamerde hij in zijn Academie voortdurend op het belang van de wiskunde. Dit wordt sterk gesuggereerd door dialogen als *Meno, Staat, Theaitetos, Philebos* en *Timaios* en blijkt tevens direct uit latere getuigenissen, met name van Aristoteles. Het invoeren van wiskunde in het hoger onderwijs voor de Atheense elite, dat tot dan toe voornamelijk uit lichamelijke opvoeding, muzikale scholing en retorica had bestaan, was een belangrijke vernieuwing van Plato. Het wiskundeprogramma op de Academie duurde maar liefst tien jaar. Wie dat had doorstaan kon op zijn dertigste nog eens verder met een vijfjarige studie van de 'dialectiek' (i.e. filosofie naar Socratisch model), om pas dán in de (hoogste kringen van de) samenleving terug te keren.
4. Dé doorbraak die de huidige natuurkunde mogelijk heeft gemaakt was precies de combinatie van experiment en op wiskunde gebaseerde theorievorming, voor het eerst in primitieve vorm bij Galileo Galilei (1564–1642) en kort daarna zeer geavanceerd bij Isaac Newton (1642–1727). Zie bijvoorbeeld het klassieke werk van E.J. Dijksterhuis, *De Mechanisering van het Wereldbeeld* (Amsterdam, 1950), en meer recent Floris Cohen, *De Herschepping van de Wereld* (Bert Bakker, 2007) en Stephen Gaukroger, *The Emergence of a Scientific Culture: Science and the Shaping of Modernity 1210–1685* (Oxford University Press, 2006).
5. De uitvinder van de moderne computer, John von Neumann (1903–1957) was niet toevallig een wiskundige.

In de geldwereld is de rol van complexe producten het afgelopen decennium sterk toegenomen; het door zowel aanbieder als afnemer niet goed begrijpen van dergelijke producten behoort tot de onomstreden oorzaken van de kredietcrisis. Niet voor niets was het pensioenfonds APG drie jaar lang (2007–2009) hoofdsponsor van het Wiskundetoernooi! Een opvallende recente ontwikkeling is de groeiende betrokkenheid van de wiskunde ook bij de economische, juridische, sociale, en cognitiewetenschappen. Ook dit heeft uiteraard dan weer maatschappelijke consequenties: forensische statistiek is soms zelfs voorpaginanieuws (het Nederlands Forensisch Instituut was de sponsor van het Wiskundetoernooi van 2010). Meer in het algemeen blijkt wiskunde onontbeerlijk voor het begrip van complexe systemen in een maatschappij die zelf steeds ingewikkelder wordt. Zelfs ouderwets klinkende bedrijfstakken als plantenveredeling en fokkerij van dieren - die voor de BV Nederland van groot belang zijn - hebben om concurrerend te kunnen blijven tegenwoordig grote behoefte aan genetici met een wiskundige achtergrond. Er staat echter nog meer op het spel: in een dichtbevolkt land als Nederland is kennis van een wiskundig gebied als epidemiologie (zowel humaan als vetrinair) letterlijk van levensbelang!

De wiskunde is weliswaar uit haar toepassingen (in de oudheid) voortgekomen, maar toch ligt het allerminst voor de hand dat wiskunde überhaupt toepassingen heeft! Bij Plato was dat dan ook niet het geval. Één van Plato's belangrijkste ideeën was dat wiskundige objecten los zouden staan van de empirische werkelijkheid en dus een abstract karakter hebben.[6] Meer nog dan de bewijstheoretische aard van de wiskunde (die goed beschouwd slechts een geïdealiseerde versie van de retoriek is, een vaardigheid die in Athene van groot belang werd geacht) is het deze eigenschap van abstractie die wiskunde vleugels geeft en de ongelofelijke kracht ervan verklaart. Juist de abstractie maakt het namelijk mogelijk om hetzelfde wiskundige instrumentarium in schijnbaar totaal verschillende situaties in te zetten. Maar tegelijk is het deze abstractie van de wiskunde die het moeilijk uit te leggen maakt dat zij zo toepasbaar is! Een verwant probleem is dat van de (vermeende) *waarheid* van wiskundige uitspraken. In de werkelijkheid om ons heen lijkt niets waar, het is eigenlijk maar een rommeltje. Hoe kan deze werkelijkheid dan een exacte wiskundige beschrijving hebben? Hoe meer nadruk de waarheid van de wiskunde krijgt, hoe lastiger het is de toepasbaarheid ervan te begrijpen. Plato's leerling Aristoteles was het dan ook niet met zijn leermeester eens: waar Plato dacht dat de zintuigelijk toegankelijke wereld eigenlijk een schijnwereld is die een vertroebeld beeld geeft van een intellectueel toegankelijke perfecte wereld van wiskundige 'vormen', vond Aristoteles juist het omgekeerde: de wereld om ons heen is de echte wereld, en de wiskunde geeft daar een geïdealiseerd (en dus vertekend) beeld van.[7]

We zullen later uitvoerig terugkomen op de mogelijke waarheid van de wiskunde, maar voorlopig is het voldoende het *duale karakter* van de wiskunde te beseffen:

- zuiver én toegepast;
- creatie van de menselijke geest én beschrijving van de werkelijkheid;
- constructie én ontdekking;
- linkse hobby én motor van de economie;
- hoog verheven én laag bij de grond.

---

6. Plato's ontdekking van wiskundige abstractie is nauw verbonden met zijn vormenleer (oftewel ideeënleer, een minder gelukkige naam) en is daar in zekere zin ook de culminatie van, zowel in scherpte van de formulering als in de nadruk op juist de wiskundige vormen (ten koste van de ethische, waar bij Socrates de nadruk op lag) in zijn latere geschriften. Volgens deze leer zijn—ruw gezegd—zowel objecten uit de alledaagse waarneming als bepaalde ethische begrippen slechts onvolmaakte afspiegelingen van oorspronkelijke vormen die zich bevinden in een hoger domein dat als het ware achter de empirische werkelijkheid verborgen ligt. Dit domein is niet toegankelijk voor de waarneming, maar uitsluitend voor het denken. Veel wiskundigen verbinden Plato's cruciale idee van wiskundige abstractie nog steeds met diens twijfelachtige doctrine dat abstracte wiskundige objecten 'echt bestaan' in een 'hogere sfeer'. Deze combinatie is niet nodig en leidt tot aanzienlijke filosofische problemen. Plato's nauw gerelateerde inzicht dat achter de verschijnselen een fraaie wiskundige structuur schuilgaat was daarentegen een ontdekking van de eerste orde, zonder welke de latere exacte wetenschap onmogelijk of sterk vertraagd zou zijn geweest. In Plato's *Timaios* vinden we bijvoorbeeld de gedachte dat de kosmos op harmonieuze wijze is georganiseerd als een perfecte meetkundige structuur, namelijk een systeem van concentrische bollen. Ook de vijf platonische veelvlakken spelen in dit wereldbeeld een belangrijke rol als wiskundige vormen die achter de waargenomen diversiteit van materile objecten schuilgaat. Deze wiskundige perfectie is inderdaad abstract en niet zichtbaar: de verschijnselen maken eerder een rommelige dan een harmonieuze, laat staan een perfecte indruk. Hier speelde ook een rol dat hogere zaken als muziek en abstractie het domein van de gegoede burgers (zoals Plato zelf) waren, terwijl toepassingen en zo iets als werken voorbehouden waren aan slaven. De stricte scheiding tussen zuivere en toegepaste wiskunde (en meer in het algemeen tussen zuivere en toegepaste wetenschap), die veel wiskundigen (en wetenschappers) ook nu nog aanhouden, maar die in feite al lang achterhaald is, is daarmee een erfenis van de scheiding tussen burgers en slaven in Athene. Zie Donald E. Stokes, *Pasteur's Quadrant: Basic Science and Technological Innovation* (Brookings Institution Press, 1997).

7. Je vindt een soortgelijke discussie in een religieuze context: schiep God de mens naar zijn evenbeeld of schiep de mens God naar zijn evenbeeld? De zogenaamde 'Platonist' kent de wiskunde een soort goddelijke, absolute status toe, terwijl een 'Aristoteliaan' de wiskunde als een menselijke creatie ziet.

Het is de bedoeling van het college *Wat is wiskunde?* om deze duale aard van het vak te leren kennen en waarderen. Het eerste onderdeel *Op zoek naar zekerheid* lijkt vooral over het (zogenaamde) zuivere deel te gaan, maar daarin blijkt tevens de sleutel tot de dualiteit van de wiskunde te liggen. Ons huidige begrip van deze zaken is terug te voeren tot een diepgaande studie van de grondslagen van de wiskunde die rond 1900 plaatsvond.[8] Belangrijke bijdragen aan deze discussie werden geleverd door Richard Dedekind (1831–1916), Georg Cantor (1845–1918), Gottlob Frege (1848–1925), Giuseppe Peano (1858–1932), David Hilbert (1862–1943), Ernst Zermelo (1871–1953), Bertrand Russell (1872–1970), L.E.J. (Bertus) Brouwer (1881–1966), en in een later stadium ten slotte Kurt Gödel (1906–1978) en Alan Turing (1912–1954). Er zijn dus twee perioden geweest waarin intensief over de vraag *Wat is wiskunde?* is nagedacht:

1. de 4e eeuw v.Chr.;
2. een tijdvak rond 1900.[9]

Dat er door de oude Grieken goed over de wiskunde is nagedacht toen deze discipline ontstond ligt voor de hand, maar wat verklaart het ontstaan van de tweede belangrijke grondslagendiscussie in de tweede helft van de 19e eeuw? Deze discussie had een lange aanloop en had haar oorsprong in het werk van Newton in de 17e eeuw. Newton was de grootste wiskundige sinds de oudheid.[10] Vanuit modern perspectief ontwikkelde hij—in een unificatiestap die zijn weerga in de wetenschapsgeschiedenis niet kent—naast de al bestaande meetkunde en rekenkunde (en tot op zekere hoogte algebra) een derde tak van de wiskunde, namelijk de analyse, of preciezer gezegd de voorloper daarvan, de calculus.[11] Hiermee reduceerde hij alle methoden die sinds de oudheid waren ontwikkeld voor de berekening van lengtes, oppervlakten, inhouden, snelheden, versnellingen, minima en maxima, enzovoort, tot twee operaties, namelijk differentiatie en integratie,[12] die ook nog eens de inverse van elkaar zijn.

Niemand twijfelde aan de geldigheid van de stellingen van de meetkunde en de rekenkunde. Maar in de calculus gebeurden soms rare dingen. Wat betekende bijvoorbeeld de snelheid van een voorwerp op een bepaald tijdstip? In eerste instantie is snelheid een gemiddelde over een eindig tijdsinterval (zoveel kilometer per uur bijvoorbeeld), maar wat gebeurt er precies als dit tijdsinterval naar nul gaat, zoals in het werk van Newton? Dit stond in nauw verband met de status van 'infinitesimalen', de 'oneindig kleine' grootheden als dx die oorspronkelijk de basis van de calculus vormden, al schudde Newton ze (i.t.t. Leibniz) in zijn latere werk af ten gunste van meetkundig gedefinieerde limieten. Al waren er rekenregels voor, niemand begreep eigenlijk wat infinitesimalen of limieten waren. Naast limieten was Newton een fanatiek gebruiker van oneindige reeksen, waarmee hij bijvoorbeeld integralen uitrekende.[13] Dat

8. Zie voor en korte inleiding M. Giaquinto, *The Search for Certainty* (Oxford, 2002), en voor een encyclopedisch overzicht I. Grattan-Guinness, *The Search for Mathematical Roots, 1870-1940: Logics, Set Theories and the Foundations of Mathematics from Cantor through Russell to Gödel* (Princeton University Press, 2000). Op de website van Desda staat een mooie film van de BBC over dit onderwerp, zie `www.desda.science.ru.nl/cgi-bin/script.pl?archief,nieuws`.
9. De precieze duur en eindpunten daarvan worden door verschillende auteurs verschillend genomen, van 50–90 jaar.
10. Newtons wiskundige werk is met zeer uitvoerig commentaar te vinden in D.T. Whiteside, *The Mathematical Papers of Isaac Newton*, Vols. I-VIII (Cambridge University Press, 1967 - 1981). Deze editie, die lange tijd zo al verkrijgbaar dan toch onbetaalbaar was voor particulieren, is begin 2008 door CUP uitgebracht in paperback en kost nu nog slechts £400. Behalve de grootste wiskundige van zijn tijd was Newton tevens de belangrijkste fysicus van alle tijden, zowel als theoreticus als experimentator. Zie respectievelijk I. Newton, *The Principia: Mathematical Principles of Natural Philosophy*, A new translation by I.B. Cohen and A. Whitman, Preceded by *A Guide to Newton's Principia* by I.B. Cohen (University of California Press, Berkeley, 1999), oorspronkelijk uit 1687, en I. Newton, *Opticks* (Dover, 1952), oorspronkelijk uit 1704. De beste biografie van Newton is *Never at Rest* door R.S. Westfall (Cambridge University Press, 1980), waaruit het volgende citaat: "The end result of my study of Newton has served to convince me that with him there is no measure. He has become for me wholly other, one of the tiny handful of supreme geniuses who have shaped the categories of the human intellect, a man not finally reducible to the criteria by which we comprehend our fellow beings." Een goede korte en fraai geïllustreerde Nederlandstalige biografie is N. Guicciardini, *Newton: Alchemist, Filosoof en Natuurwetenschapper* (Natuur en Techniek, Veen Magazines, Amsterdam, 2002). ook aan te bevelen is *Isaac Newton en het Ware Weten* door F. Cohen (Bert Bakker, 2010). Ten slotte is K. Landsman, *Requiem voor Newton* (Contact, 2005) een smeuïg boek over de plaats van Newton in de wetenschapsgeschiedenis (helaas nog slechts antiquarisch of in de bibliotheek verkrijgbaar).
11. Uiteraard kwam deze niet uit de lucht vallen, zie bijv. R. Calinger, *A Contextual History of Mathematics* (Prentice-Hall, 1999). Sommige onderdelen van de calculus werden na Newton ook ontwikkeld door Gottfried Wilhelm Leibniz (1646–1716), die soms als mede-grondlegger van de differentiaal- en integraalrekening wordt beschouwd. Leibniz had tijdens een bezoek aan Londen echter inzage had gehad in het eerdere werk van Newton, dat pas na de dood van de laatste werd gepubliceerd, maar onder vakgenoten in Engeland al wel bekend was. In de 18e eeuw ontstond tussen Newton en Leibniz een gevecht over de prioriteit van de ontdekking van de caclulus, dat na hun dood door hun volgelingen werd voortgezet. Dit had tot gevolg dat de wiskunde zich in Engeland grotendeels onafhankelijk ontwikkelde t.o.v. het continentale Europa. De wet van de remmende voorsprong leidde uiteindelijk tot een achterstand van Engeland, temeer daar de notatie van Leibniz handiger was en zijn eerste generatie leerlingen (met name de Bernoulli familie) getalenteerder was dan de club rond Newton. Ook Leonard Euler (1707-1783), de belangrijkste wiskundige van de 18e eeuw, kwam indirect voort uit de school van Leibniz.
12. Newton schreef optimistisch: "could this ever be done all problems whatever might be resolved."
13. We zouden nu zeggen dat hij de te integreren functie in een Taylor-reeks expandeerde en deze termsgewijs integreerde om

leidde echter tot verwarring. Men kende de meetkundige reeks $1 + x + x^2 + x^3 + \cdots$ en zag in dat dit voor kleine x een steeds betere benadering van $1/(1-x)$ vormde. Voor $x = -1$ echter is de reeks $1-1+1-1+\cdots$, waarover de meningen verschilden. De een groepeerde de termen als $(1-1)+(1-1)+\cdots$ en beweerde dat er daarom 0 uit kwam. De ander schreef de reeks als $1-(1-1)-(1-1)+\cdots$ en kreeg dus 1 als resultaat. Een derde noemde de reeks S en bewees dat $1 - S = S$, wat $S = \frac{1}{2}$ geeft, toch?

Kortom, de betrouwbaarheid van de wiskunde leek verdwenen, terwijl dat juist haar bepalende eigenschap zou moeten zijn! Daar stonden dan wel de enorme successen van Newton en zijn opvolgers tegenover. Zijn belangrijkste opvolger was Euler, die de wiskunde (en mathematische fysica) van 18e eeuw domineerde. Euler zag wel in dat er problemen waren met de calculus, en kwam daar gedeeltelijk aan tegemoet door de krommen van Newton (die in feite werkte met grafieken van functies, die hij zag als trajecten van deeltjes) te vervangen door het begrip 'functie' (zoals gebruikt op het vwo).[14] Dat deed hij in eerste instantie (in *Introductio in Analysin Infinitorum* uit 1748) door middel van een formule, meestal een (eindige of oneindige) machtreeks, zoals bij de exponentiële functie, of door een voorschrift, zoals bij de logaritme, die hij introduceerde als de inverse van de exponentiële functie (Euler suggereerde dat iedere functie als een machtreeks kan worden geschreven). Later (in *Institutiones Caculi Differentialis* uit 1755) werkte hij met functies als grootheden die van een andere grootheid afhangen.

Maar hiermee werden de moeilijkheden met de wiskunde eigenlijk alleen nog maar erger, want alle problemen met convergentie en limieten kwamen zo met dubbele kracht terug en leidden tevens tot nieuwe vragen: is iedere functie zoals oorspronkelijk gedefinieerd door Euler (dus door een formule of voorschrift) inderdaad te schrijven als machtreeks? Is een machtreeks altijd continu?[15] Differentieerbaar? 'Glad'? Is een continue functie overal differentieerbaar behalve in eindig veel punten (denk aan een zaagtand)? Enzovoort. Bovendien voerden Euler en zijn tijdgenoten partiële differentiaalvergelijkingen in, zoals die voor de trillende snaar $\partial^2 u/\partial t^2 = c^2 \partial^2 u/\partial x^2$ voor $u = u(x,t)$, waarbij allerlei nieuwe vragen en onduidelijkheden ontstonden, zoals over het bestaan en de uniciteit van de oplossing (bij gegeven randvoorwaarden) en over de mogelijkheid om willekeurige oplossingen te schrijven als machtreeksen in $\sin$ en $\cos$.[16] Men wist zich met dergelijke kwesties gewoon geen raad. Intussen bleek de analyse wel het krachtigste middel ooit om de wereld te beschrijven, en verdrong zij gaandeweg de traditionele disciplines van de wiskunde, zoals de meetkunde. Kortom, men ging onverdroten door maar maakte zich tegelijk zorgen. Deze werden versterkt doordat na de Franse Revolutie de gewoonte ontstond om analyse op universiteiten te onderwijzen,[17] zodat een stevige grondslag noodzakelijk was van het soort die de studenten uit de meetkunde gewend waren.[18]

---

vervolgens de som te nemen, dus $\int_0^x dy\, f(y) = \int_0^x dy\, \sum_k c_k y^k = \sum_k c_k \frac{1}{k+1} x^{k+1}$.

14. "The modern reader is likely to miss the import of this [first] chapter, 'On Functions in General,' for its main idea has been so totally incorporated into mathematics that we think nothing of it. This chapter is about functions. It is not about curves. This change of viewpoint represents a benchmark in the history of the calculus. Newton and Leibniz studied curves. The title of the first calculus book, *Analyse des infiniment petits, pour l'intelligence des lignes courbes* (L'Hôpital 1696), reflects this early point of view. Agnesi's book, published the same year as the *Introductio*, also studies curves." Geciteerd uit *A Readers Guide to Eulers Introductio* door V. Frederick Rickey, `www.math.usma.edu/people/Rickey/hm/Euler-Introductio.pdf`.

15. Het huidige begrip van continuïteit stamt uit de 19e eeuw en bestond in de tijd van Euler dus nog niet. Voor Euler was een functie continu als deze functie over haar hele domein door hetzelfde 'voorschrift' wordt gegeven. Veel van zijn tijdgenoten dachten bij continuïteit eerder aan de grafiek van de functie, die bij Euler een ondergeschikte rol speelde. Deze twee begrippen zijn niet hetzelfde. De functie $f : [-1,1] \to \mathbb{R}$ gegeven door $f(x) = x$ voor $x \geq 0$ en $f(x) = -x$ voor $x < 0$, oftewel $f(x) = |x|$, was voor Euler discontinu, terwijl de grafiek wel degelijke continu is. Ook naar de moderne definitie is deze functie continu. De stapfunctie daarentegen (i.e. $\theta(x) = 1$ voor $x \geq 0$ en $\theta(x) = 0$ voor $x < 0$) was voor iedereen discontinu.

16. De vergelijking voor de trillende snaar heeft als algemene oplossing $u(x,t) = f(x+ct) + g(x-ct)$, waar f en g 'willekeurige' functies zijn. Uit niets volgt dat f en g machtreeksen zijn, zoals in eerste instantie gedacht door Euler. Als de eindpunten van de snaar vastzitten, geldt $u(0,t) = u(L,t) = 0$ voor alle t, waarbij L de lengte van de snaar is. Hieruit volgt dat $g(y) = -f(-y)$, en dat $f(y + 2L) = f(y)$, m.a.w., f is periodiek met periode $2L$. Als wiskundige zeg je nu dat iedere functie van de vorm $f(y) = A_n \sin(n\pi y/L) + B_n \cos(n\pi y/L)$ een oplossing geeft, voor willekeurige constanten A_n en B_n, $n = 0, 1, 2, 3, \ldots$. Als fysicus verwacht je dat iedere beginconfiguratie $u(x,0) \equiv u_0(x)$ op tijdstip $t = 0$ na loslaten van de snaar een unieke beweging geeft. Als mathematisch fysicus—en dat was vrijwel iedere wiskundige in de 17e en 18e eeuw—concludeer je dan dat je een 'willekeurige' functie u_0 op het interval $[0, L]$ die voldoet aan $u_0(0) = u_0(L) = 0$ kennelijk kunt schrijven als $u_0(x) = 2\sum_{n=1}^{\infty} A_n \sin(n\pi y/L)$. Deze stap was het begin van wat later Fourier-analyse zou heten; het is duidelijk dat deze redenering talloze vragen over de analyse oproept, zoals de convergentie van de reeks en de eventuele continuïteit van de som (als deze bestaat).

17. Tot aan de Franse Revolutie waren vooraanstaande wiskundigen i.h.a. verbonden aan koninklijke academies of hoven (m.u.v. Newton, die aan de Universiteit van Cambridge werkte). Zij gaven daar hoogstens onderwijs aan een kleine elite. Op de universiteiten onderwezen destijds tweederangs figuren totaal verouderde kennis (met uitzondering van filosofie en geneeskunde).

18. Op de middelbare scholen werd destijds als wiskunde uitsluitend Euclidische meetkunde onderwezen, meestal uit de *Elementen* van Euclides zelf. In Nederland bestond het wiskundeonderwijs tot 1960 uit Euclidische meetkunde, rekenen,goniometrie, trigonometrie, en enige algebra. De analyse wordt dus pas sinds 1961 op scholen onderwezen, bijna drie eeuwen na haar ontstaan.

Zoals je in het college Analyse leert werden de problemen met dit vak opgelost door een goede grondslag.[19] Deze kwam voort uit het werk van Augustin-Louis Cauchy (1789–1857), Peter Lejeune Dirichlet (1805–1859), Karl Weierstrass (1815–1897), Eduard Heine (1821–1881), Bernhard Riemann (1826–1866), de al genoemde Cantor, Dedekind, Hilbert, von Neumann, en anderen. Zo gaan onze definities van convergentie en continuïteit terug tot Cauchy (waarna ze door Weierstrass werden geperfectioneerd), gaf Dirichlet de moderne definitie van een functie (als een toekenning van een element van een bepaalde verzameling aan een willekeurige element van een andere gegeven verzameling), definieerde Riemann de naar hem genoemde integraal, construeerden Cantor, Heine, en Dedekind op verschillende wijze de reële getallen (de eerste twee als limieten van Cauchy-rijen, de laatste als de naar hem genoemde sneden),[20] en gaf Hilbert de moderne abstracte definitie van $\mathbb{R}$ (als een volledig geordend en compleet lichaam), waar de constructies van Dedekind en Cantor–Heine voorbeelden van waren. Eind 19e eeuw gold dan ook niet meer de meetkunde maar de analyse als het summum van wiskundige gestrengheid. Vrijwel alle colleges Analyse in de wereld verlopen sindsdien op dezelfde manier: definitie van $\mathbb{R}$, limieten, convergentie, continuïteit, differentiatie, integratie, ... Er gebeuren nog steeds vreemde dingen, zoals het bestaan van een continue functie die nergens differentieerbaar is, of een functie die niet integreerbaar is, maar, hoe contraintuïtief ook, kan dat blijkbaar allemaal volgens de definities.

Dit had tot gevolg dat de analyse net als de Euclidische meetkunde op axiomatische grondslag werd gevest. Daardoor werd de analyse een formele aangelegenheid, waarbij aanschouwelijkheid, intuïtie en toepassingen steeds minder belangrijk werden. Een soortgelijke trend speelde zich in andere gebieden van de wiskunde af. Zelfs de Euclidische meetkunde bleek niet perfect. Sommige definities (bijvoorbeeld van een punt) waren onduidelijk en bepaalde bewijzen waren niet strict deductief vanuit de axioma's (maar gebruikten intuïtie of waren zelfs ronduit onvolledig). Dit leidde tot een nieuwe axiomatisering van de meetkunde door Hilbert (*Grundlagen der Geometrie*, 1899), waarin aanschouwelijkheid geen enkele rol meer speelt. Nog belangrijker dan Hilberts verbeterde axioma's en bewijzen was daarbij zijn eis dat begrippen als 'punt, lijn, en vlak' slechts een notatie zijn en net zo goed vervangen kunnen worden door 'liefde, wet, en schoorsteenveger', zolang ze maar worden gebruikt zoals de axioma's voorschrijven.[21] Ook de meetkunde werd dus geformaliseerd. Ten slotte ontstonden nieuwe, realiteitsvreemde gebieden als algebraïsche rekenkunde, projectieve meetkunde, lineaire algebra, algebraïsche logica, en differentiaalmeetkunde (met name in willekeurige dimensies), waarvan de mogelijke toepassingen in ieder geval op dat moment ver te zoeken waren.[22]

---

19. Voor een bondig overzicht daarvan zie bijvoorbeeld Victor J. Katz, *A History of Mathematics: An Introduction* (Addison Wesley Longman, 1998). Uitvoeriger is H.N. Jahnke (Ed.), *A History of Analysis* (American Mathematical Society, 2003).

20. De constructie van Heine en Cantor wordt behandeld in het college *Getallen*, maar voor de zekerheid: een rij (a_n) in $\mathbb{Q}$ heet een *Cauchy-rij* als er bij iedere $\varepsilon > 0$ (met $\varepsilon \in \mathbb{Q}$) een $N \in \mathbb{N}$ is zodat voor alle $m, n > N$ geldt $|a_m - a_n| < \varepsilon$. Twee Cauchy-rijen (a_n) en (b_n) heten *equivalent* als $\lim_{n\to\infty} |a_n - b_n| = 0$, met andere woorden, er is bij iedere $\varepsilon > 0$ een $N \in \mathbb{N}$ is zodat $|a_n - b_n| < \varepsilon$ voor alle $n > N$. Een reëel getal is ten slotte een equivalentieklasse van Cauchy-rijen in $\mathbb{Q}$. De door Simon Stevin (1548–1620) in 1585 ingevoerde decimaalexpansie van een reëel getal kan worden gezien als een Cauchy-rij: bijvoorbeeld π is (de equivalentieklasse van) de Cauchy-rij $3, 3.1, 3.14, 3.141, \ldots$. Soortgelijke constructies verschenen tussen 1870 en 1880 tevens van Méray, Weierstrass, en Thomae. Een meer symmetrische maar equivalente definitie volgens ditzelfde idee werd later gegeven door Brouwer, als volgt.
We noemen een rij $([a_n, b_n])$ van gesloten intervallen in $\mathbb{Q}$ een *Brouwer-rij* als $[a_{n+1}, b_{n+1}] \subset [a_n, b_n]$ en $\lim_{n\to\infty} |a_n - b_n| = 0$. We verklaren twee Brouwer-rijen $([a_n, b_n])$ en $([a'_n, b'_n])$ equivalent als $\lim_{n\to\infty} |a_n - a'_n| = 0$ of $\lim_{n\to\infty} |b_n - b'_n| = 0$ (deze condities zijn equivalent voor Brouwer-rijen). Een reëel getal is dan een equivalentieklasse van Brouwer-rijen. Het idee is dat $[a_n, b_n]$ voor toenemende n steeds betere informatie verschaft over het gezochte reële getal. Zo kan π worden voorgesteld door de Brouwer-rij $[3, 4], [3.1, 3.2], [3.14, 3.15], [3.141, 3.142], \ldots$.
Een *Dedekind-snede* is een paar (L, U) met $L \subset \mathbb{Q}$, $U \subset \mathbb{Q}$, $L \cup U = \mathbb{Q}$, $L \cap U = \emptyset$, en $l < u$ voor alle $l \in L$ en $u \in U$. Als L een bovengrens b (in $\mathbb{Q}$) heeft, of U een ondergrens o, dan staat (L, U) voor het getal b resp. o in $\mathbb{Q}$, nu gezien als deelverzameling van de de verzameling $\mathbb{R}$ van alle Dedekind-sneden. Als dit echter niet het geval is, is de snede (L, U) een irrationeel getal in $\mathbb{R}$. We kunnen π bijvoorbeeld identificeren met de snede (L, U) waarbij L bestaat uit alle $q \in \mathbb{Q}$ zodat $q < a_n$ voor zekere n, terwijl U bestaat uit alle $r \in \mathbb{Q}$ zodat $r > b_n$ voor een bepaalde, met $(a_n) = 3, 3.1, 3.14, 3.141, \ldots$ en $(b_n) = 4, 3.2, 3.15, 1.142, \ldots$.

21. Zo schreef Hilbert op 29-12-1899 aan Frege: *"Ich will nichts als bekannt voraussetzen (...) Wenn ich unter meinen Punkten irgendwelche Systeme von Dingen, z.B. das System: Liebe, Gesetz, Schornsteinfeger ..., denke und dann meine sämtlichen Axiome als Beziehungen zwischen diesen Dingen annehme, so gelten meine Sätze, z.B. der Pythagoras, auch von diesen Dingen."* Dit was een reactie op een eerdere brief van Frege, waarin deze ten onrechte opmerkt dat Hilbert begrippen als punt en lijn bekend veronderstelt, zodat hij het (in tegenstelling tot Euclides) niet nodig vond om ze expliciet te definiëren. Hilbert zegt daarover zelfs: *"Hier liegt wohl der Cardinalpunkt des Misverständnisses."* Voor de Nederlandse lezer: het kardinale misverstand bij Frege (overigens niet de minste), dat helaas nog steeds leeft bij de medewerkers van het Freudenthal-Instituut in Utrecht die in de jaren '80 het zgn. 'realistische' wiskundeonderwijs in Nederland hebben ingevoerd (later 'contextrijk' geheten), is dat wiskunde noodzakelijkerwijs aan de werkelijkheid gerelateerd moet worden en dat alle symbolen en constructies dus ook echt bestaan. Het tegendeel is waar: op het niveau waarop de wiskunde zekere resultaten geeft betekenen de symbolen juist helemaal niets, zoals Hilbert (maar voor hem al George Boole en Federigo Enriques) zeer scherp inzag.

22. Later kwamen er volkomen onverwachte toepassingen van bijvoorbeeld de differentiaalmeetkunde in de Algemene Relativiteitstheorie van Einstein (1915) en de van de lineaire algebra in oneindige dimensie (i.e. functionaalanalyse) in de kwantumme-

In de 19e eeuw vond aldus een ontwikkeling plaats die het aangezicht van de wiskunde voor altijd zou veranderen. Van Aristoteles en Euclides tot en met Newton en Euler ging de wiskunde, ondanks haar abstractie, over de werkelijkheid en was zij 'waar'. De Euclidische meetkunde beschreef de ruimte om ons heen, getallen kom je overal tegen, en de analyse beschreef de natuur(kunde) of was tenminste concreet. Nu, in de 21e eeuw (en gedurende het grootste deel van de 20e eeuw) zou niemand het in zijn hoofd halen om in het bos naar een 10-dimensionale vector-ruimte of een C*-algebra te zoeken. De wiskunde is *autonoom* geworden, en deze stap naar zelfstandigheid werd gezet in de 19e eeuw.[23]

De conclusie is dat wiskunde twee verschillende kanten heeft, die samen het vak vormen. De ene kant heet *syntax*: dit is een puur symbolische kant, die met een spel als schaken te vergelijken is. Wiskundige uitspraken zijn dan bepaalde welgedefinieerde combinaties van symbolen; we zullen later precies zijn hoe dat werkt. Een voorbeeld is $2+2=5$ (terwijl $2+2=$ geen uitspraak is). Deze symbolen betekenen in eerste instantie niets, hoewel het handig kan zijn als je er een bepaalde voorstelling bij hebt (zoals bij het symbool P voor punt, L voor lijn, en V voor vlak in de Euclidische meetkunde). Dan zijn er definities en axioma's die de symbolen aan elkaar relateren (er is geen stricte scheiding tussen definities en axioma's). Stellingen zijn uitspraken die je volgens bepaalde logische regels (die zelf eigenlijk ook weer keuzes zijn: er bestaan verschillende logische systemen om wiskunde te doen) uit de axioma's en definities af kunt leiden, zoals $2+2=4$. Zulke stellingen zeggen (nog) niets over de werkelijkheid.

Het schaakspel geeft hier een nuttige analogie. Bord en stukken staan dan voor wiskundige symbolen, definities voor de loop der stukken, axioma's voor de beginstand, en algemene logische regels voor de spelregels. Een wiskundige uitspraak is analoog aan een stand, in de zin van een willekeurige configuratie van de schaakstukken op het bord. Een wiskundige stelling is een uitspraak die kan worden bewezen; zo is een schaakstelling een stand die volgens de regels uit de beginstand kan ontstaan.

De tweede kant van de wiskunde heet *semantiek*: hierbij wordt de syntax op de een of andere manier geïnterpreteerd.[24] Je kunt de symbolen P, L, en V uit de abstracte Euclidische meetkunde bijvoorbeeld interpreteren als punten, lijnen en vlakken in de natuurlijke zin. Hierbij ga je er vanuit dat deze laatste ook echt bestaan. Zo'n interpretatie is zinvol als de 'echte' punten, lijnen en vlakken aan precies dezelfde axioma's voldoen als de abstracte. Vaak is dat maar bij benadering het geval. De stellingen op syntactisch niveau erven de interpretatie van de symbolen en zeggen dan iets over de werkelijkheid. Maar wat ze zeggen is meestal slechts een benadering, omdat de interpretatie zelf al slechts een benadering was. Dit is precies wat Albert Einstein uitdrukt met de woorden die ook op de kaft van deze syllabus staan:

> "Voor zover de conclusies van de wiskunde met de werkelijkheid te maken hebben zijn ze niet zeker, en voor zover ze zeker zijn verwijzen ze niet naar de werkelijkheid."

---

chanica (1930). Zulke toepassingen zouden onmogelijk zijn zonder het abstracte karakter van de moderne wiskunde.

23. Zie J. Gray, *Plato's Ghost: The modernist Transformation of Mathematics* (Princeton University Press, 2008).

24. Logici bedoelen met semantiek meestal de interpretatie van een of andere syntactische theorie in de verzamelingenleer; we gebruiken de term hier veel breder.

2

Paradox van Russell en Stelling van Cantor

Toch bleef er iets knagen. De hele grondslag van de analyse berust op de oneindige verzameling $\mathbb{R}$ van reële getallen. Maar wat is een verzameling eigenlijk en wat betekent het dat deze oneindig is? Waarom is oneindig veel informatie nodig om zo iets futiels als een punt op een lijn te identificeren? Hoe weten we dat redeneringen met oneindige hoeveelheden elementen van een oneindige verzameling (nl. $\mathbb{Q}$) niet tot een tegenspraak leiden? Dergelijke vragen werden met name opgepakt door Cantor en Frege.

Het werk van Frege was aan de ene kant zeer precies; zijn poging een perfecte logische taal voor de wiskunde te ontwikkelen vormt de basis voor de moderne logica.[1] We zullen daar later op ingaan en ook een paar voorbeelden van deze logische taal geven. Aan de andere kant ging hij (achteraf bezien) roekeloos om met het begrip verzameling, door aan te nemen dat ieder predikaat een verzameling definieert. Met andere woorden: iedere eigenschap E bepaalt volgens Frege de verzameling $\{x \mid E(x)\}$ van alle dingen x die aan die eigenschap voldoen.[2]

Helaas voor hem ontdekte de filosoof Bertrand Russell (1872–1970) in 1901 de naar hem genoemde paradox, die al in het college *Getallen* behandeld is: neem x een verzameling en $R(x)$ de eigenschap dat x geen element van zichzelf is, oftewel $x \notin x$. Volgens Frege bestaat dan de verzameling

$$\mathsf{R} = \{x \mid R(x)\} = \{x \mid x \notin x\} \tag{2.1}$$

van alle verzamelingen heeft die geen element van zichzelf zijn. Maar dat is onmogelijk, zoals blijkt wanneer we de vraag stellen: is R een element van zichzelf?

- Zo ja, dan is R per definitie geen element van zichzelf, zodat het antwoord juist "nee" is.
- Zo nee, dan is R per definitie wél een element van zichzelf, zodat het antwoord "ja" is.

Het antwoord op de vraag is dus tegelijk "ja" en "nee": het bestaan van R leidt tot een tegenspraak! Tegenspraken (of 'contradicties') zijn niet toegestaan in de wiskunde, zodat R niet kan bestaan. Dit argument is dus een bewijs uit het ongerijmde van de stelling dat de verzameling R niet bestaat.

---

1. Frege had als doel om tenminste de rekenkunde tot de logica te reduceren. Russell probeerde later zelfs de hele wiskunde uit de logica af te leiden. Zelfs het meer bescheiden doel van Frege werd niet bereikt, niet alleen vanwege de problemen met zijn verzamelingenleer (die Russell wist te omzeilen), maar omdat beiden er vanuit gingen dat logische axioma's vanzelfsprekend waren, in de zin dat iedereen die kon denken onmiddellijk zag dat ze 'waar' waren. Inderdaad had dat millennia lang gegolden voor de axioma's van de Euclidische meetkunde, en ook de axioma's van Peano voor de rekenkunde zagen er wat dat bereft goed uit. Uit de correspondentie tussen Frege en Hilbert blijkt zonneklaar dat de eerste de conceptuele vernieuwingen van de laatste niet begreep. Frege dacht dat Hilbert de primitieve termen in zijn axioma's (zoals punt, lijn, en vlak) niet nader specificeerde omdat de lezer er al vertrouwd mee was, terwijl Hilbert ze juist bewust als betekenisloos beschouwde. Uit de eerder genoemde brief van Hilbert aan Frege: "Sie sagen weiter: 'Ganz anders sind wohl die Erklärungen in Par. 1, wo die Bedeutungen Punkt, Gerade, … nicht angegeben, sondern als bekannt vorausgesetzt werden'. Hier liegt wohl der Cardinalpunkt des Misverständnisses. Ich will nichts als bekannt voraussetzen." Het inductieaxioma van Peano is echter met de beste wil van de wereld niet als vanzelfsprekend te beschouwen, en voor de veel ingewikkeldere axioma's van Russell en Whitehead in *Principia Mathematica* (Cambridge University Press, 1910–1913) geldt dat al helemaal. Zoals we later zullen zien wordt de grondslag van de huidige wiskunde gegeven door de verzamelingenleer, die gebaseerd is op een axiomasysteem dat weliswaar in een logische notatie à la Frege is opgeschreven, maar opnieuw allerminst vanzelfsprekend is.
2. Dit was een technische versie van het intuïtieve verzamelingsbegrip van Cantor en Dedekind, zodat Frege niet alleen stond in zijn verzamelingstheoretische naïviteit. Volgens de eerste was een verzameling "een geheel van bepaalde onderscheidbare objecten die wij in onze gedachten kunnen hebben", en volgens de tweede was een verzameling S "bepaald als object van onze gedachten als van ieder ding bepaald is of het een element van S is of niet." Het feit dat dit soort verbale definities tot tegenspraak leidt (zoals blijkt uit de paradox van Russell) geeft aan dat het ook in de verzamelingenleer het beste is om de primitieve begrippen (en dat zijn in dat geval slecht 'verzameling' en 'element van') niet nader te omschrijven, maar zo te gebruiken als de axioma's voorschrijven. Wat dit betreft is er dus geen verschil in mentaliteit tussen de Euclidische meetkunde in de aanpak van Hilbert en de wiskunde als geheel zoals geformaliseerd met verzamelingen.

Deze paradox lijkt eerder vermakelijk dan belangrijk, maar de impact ervan was enorm, in ieder geval op de kleine groep wiskundigen die zich met de grondslagen van hun vak bezighielden. De reden was dat Frege als enige een totale onderbouwing van de wiskunde leek te hebben, waarin de bovengenoemde constructie van verzamelingen door middel van predikaten een centrale rol speelde. Deze onderbouwing viel door de paradox van Russell in duigen.[3]

Al eerder had Cantor bewezen dat er meer reële dan natuurlijke getallen zijn, in de zin dat er geen bijectie $f : \mathbb{N} \to \mathbb{R}$ bestaat (en wel een injectie). Éen van zijn bewijzen was het *diagonaalargument*, waarmee hij in 1891 bewees dat voor iedere verzameling V geldt:

Stelling 2.1 *De machtsverzameling $P(V)$ van V (i.e. de verzameling van alle deelverzamelingen van V) is groter dan V, in de zin dat er geen bijectie $f : V \to P(V)$ bestaat (en wel een injectie).*

Het bewijs gaat als volgt (vgl. bijv. het boek *Getallen* van Frans Keune, Stelling 14.70, waarvan we het bewijs hier vrijwel letterlijk overnemen). Het is duidelijk dat er een injectie $V \to P(V)$ bestaat, nl. $x \mapsto \{x\}$. De stelling van Cantor zegt dat er geen functie $f : V \to P(V)$ bestaat die zowel injectief als surjectief is (en daarmee bijectief, i.e. inverteerbaar). Sterker nog, er bestaat überhaupt geen surjectie $f : V \to P(V)$, of deze nu inverteerbaar is of niet. We bewijzen dit uit het ongerijmde.

Stel eerst dat $f : V \to P(V)$ een willekeurige afbeelding is. Neem de volgende deelverzameling van V:

$$U = \{x \in V \mid x \notin f(x)\}. \tag{2.2}$$

Als f nu surjectief is (dit is de aanname die in dit bewijs uit het ongerijmde weerlegd gaat worden), dan ligt iedere $W \in P(V)$ in het beeld van f. Dit geldt dus in het bijzonder voor $W = U$: als f surjectief is, moet er per definitie (van surjectiviteit) een $y \in V$ bestaan zodat $f(y) = U$. Vraag: geldt $y \in U$?

- Zo ja, dan geldt per definitie van U dat $y \notin f(y)$. Maar $f(y) = U$, dus $y \notin U$. Tegenspraak.
- Zo nee, dan geldt per definitie van U juist dat $y \in f(y) = U$. Tegenspraak.

De enige uitweg is dat f niet surjectief kan zijn. Q.E.D.

Let op: hier maken we nog gebruik van de zogenaamde *naïeve verzamelingenleer*, zoals die in vrijwel alle wiskundevakken wordt gebruikt. Hierbij wordt nog steeds op een tamelijk intuïtieve manier met verzamelingen gewerkt, maar dan wel zodanig dat de ergste rampen (zoals de paradox van Russell) worden vermeden. Later zullen we de *axiomatische verzamelingenleer* behandelen, waarin precies wordt voorgeschreven wat je wel en niet mag doen met verzamelingen. Goede wiskundigen die met verzamelingenleer werken zorgen er stilzwijgend voor dat hun (op het eerste ook wellicht naïeve) constructies met verzamelingen ook volgens de axioma's zijn toegestaan. Zo is (2.2) correct omdat U door middel van een predikaat wordt gedefinieerd *als deelverzameling van een al bestaande verzameling* V.

Hoe dan ook volgt uit Stelling 2.1 dat er geen grootste verzameling S kan bestaan (immers, $P(S)$ zou groter zijn dan S: tegenspraak), en daarom kan ook de verzameling van alle verzamelingen niet bestaan. Die zou namelijk moeten samenvallen met S: in de verzamenlingenleer zijn er immers alleen maar verzamelingen (zoals we later in detail zullen zien). Elementen van verzamelingen zijn zelf dus ook verzamelingen. De grootste verzameling zou daarom de verzameling van alle verzamelingen zijn.

De conclusie dat deze laatste niet bestaat verbindt de paradox van Russell met de stelling van Cantor. Als S zou bestaan, kunnen we (2.1) nauwkeuriger schrijven als $\mathsf{R} = \{x \in S \mid x \notin x\}$. Uit de later te behandelen axioma's van de verzamelingenleer blijkt dat de eigenschap $E(x)$ gegeven door $x \notin x$ op zich goed gedefinieerd is, en tevens dat voor iedere verzameling V en iedere goed gedefinieerde eigenschap E de verzameling $\{x \in V | E(x)\}$ bestaat. Nemen we nu $V = S$ and $E(x) = (x \notin x)$, dan zou de verzameling R dus moeten bestaan. Maar dat is volgens Russell onmogelijk. Het enige dat in het argument dat tot R leidt fout kan zijn, is het bestaan van S. Het niet bestaan van een grootste verzameling is dus equivalent met het niet bestaan van de verzameling van alle verzamelingen én met het niet bestaan van de verzameling van alle verzamelingen heeft die geen element van zichzelf zijn.

3. Een leuk stripboek over deze episode, met (twijfelachtig) biografisch materiaal over de hoofdrolspelers, is *Logicomix* door A. Doxiadis e.a. (Vliegende Hollander, 2009).

Opgaven

1. Neem $V = \mathbb{N}$ in Stelling 2.1 en noteer $S_n = f(n)$; de rij $S_1, S_2, S_3, \ldots$ is dan een (tot mislukken gedoemde) poging de deelverzamelingen van $\mathbb{N}$ op te sommen. Bewijs (als speciaal geval van de stelling) dat de verzameling in (2.2), dus $U = \{n \in \mathbb{N} \mid n \notin S_n\}$, niet in deze opsomming voor kan komen (zodat deze opsomming niet volledig is). *Niet inleveren!*
2. Laat zien dat de verzameling van alle functies $f : \mathbb{N} \to \mathbb{N}$ overaftelbaar is (met andere woorden, dat er geen opsomming $f_1, f_2, f_3, \ldots$ van dergelijke functies bestaat).
3. We zeggen dat een functie $f : \mathbb{N} \to \mathbb{N}$ sneller groeit dan $g : \mathbb{N} \to \mathbb{N}$ als $\lim_{n\to\infty} f(n)/g(n) = \infty$. Bewijs dat er geen opsomming $f_1, f_2, f_3, \ldots$ van functies van $\mathbb{N}$ naar $\mathbb{N}$ bestaat met de volgende eigenschap: voor iedere $g : \mathbb{N} \to \mathbb{N}$ is er een $m \in \mathbb{N}$ zodat f_m sneller groeit dan g.
4. Laat zien dat een verzameling die *elk* van zijn deelverzamelingen tevens als element bevat, niet kan bestaan (dit is de *Paradox van Zermelo*). N.B. Het is wel degelijk mogelijk dat een verzameling een bepaalde deelverzameling ook als element bevat: $V = \{1, 2, 3, \{1, 2\}\}$ heeft bijvoorbeeld als *deelverzameling* $\{1, 2\}$ (dit zijn de 1 en 2 vooraan), maar ook als *element*.

3

Propositielogica

Eerste een korte samenvatting van het voorafgaande.

1. De meetkunde van Euclides gold meer dan tweeduizend jaar lang als "zeker" en "waar".
2. De Calulus van Newton, die de wiskunde vanaf de 17e eeuw begon te domineren, had daarentegen geen duidelijke (axiomatische) grondslag. De resultaten waren enerzijds op indrukwekkende wijze toepasbaar op de fysische werkelijkheid, maar de afleidingen waren wankel en hun "zekerheid" stond daarom ter discussie.
3. Als reactie ontstond de Analyse als grondslag voor de Calculus, maar de eerste had zelf weer een grondslag nodig in de vorm van de reële getallen.
4. En de reële getallen berustten op hun beurt weer op het begrip verzameling.

Uiteindelijk bleek een axiomatische opzet van de verzamelingenleer nodig, waarbij met name Hilbert het (moderne) standpunt verdedigde dat de symbolen in de axioma's op zich geen betekenis hebben. Iemand die dit echter al een halve eeuw voor Hilbert had begrepen was de Engelse wiskundige George Boole (1815–1864),[1] een van de grondleggers van de moderne logica (en met name van de propositielogica in dit hoofdstuk). Hij schreef in het voorwoord van zijn boek *Mathematical Analysis of Logic*:

> "They who are acquainted with the present state of the theory of Symbolic Algebra, are aware of the validity of the processes of analysis does not depend upon the interpretation of the symbols which are employed, but solely upon the laws of their combination."

Boole zag ook in, net als Leibniz 175 jaar eerder, dat de eerste stap in de axiomatische opbouw van welk gebied van de wiskunde ook de ontwikkeling van een geschikte *logische taal* is. Dat is op vele manieren geprobeerd, en we volgen in dit college de *mainstream*: eerste-orde logica (vnl. ontwikkeld door Frege, en later door Hilbert gekozen als de basis van de wiskunde). Die zou in principe direct in volle glorie ingevoerd kunnen worden, zoals in het volgende hoofdstuk, maar uit didactische overwegingen bespreken we in dit hoofdstuk eerst een op zichzelf staand fragment daarvan, de *propositielogica*. Net als bij alle andere vormen van logica is het bij de propositielogica de bedoeling om aan te geven wat:

- de notatie is (i.e. welke symbolen in de taal voorkomen);
- de regels zijn om welgedefiniëerde uitdrukkingen oftewel *formules* samen te stellen;
- de regels zijn om uit formules *uitspraken* te definiëren (in de propositielogica ook *proposities* genoemd): dit zijn speciale formules die (on)waar en/of (on)bewijsbaar kunnen zijn;
- de axioma's zijn (die als uitgangsspunten van bewijzen dienen);
- de deductieregels zijn (die formuleren hoe een correct bewijs verloopt);
- de regels zijn die bepalen of een bepaalde uitspraak (on)waar is.

De eerste vier punten heten de *syntax* en het laatste heet de *semantiek* van de axiomatisering.[2] We maken hier dus al een principieel verschil tussen *bewijsbaarheid* en *waarheid*. Het eerste is een puur syntactisch begrip, te vergelijken met het correct volgen van de regels van het schaakspel om zo een partij te spelen. Het tweede heeft te maken met de interpretatie van het formalisme in de werkelijkheid.

---

1. Een leuk boek over Boole, en tevens over Shannon, is Paul Nahin, *The Logician and the Engineer: How George Boole and Claude Shannon Created the Information Age* (Princeton University Press, 2013).
2. Deze termen kom je ook tegen in de linguïstiek. Er is dan ook een zekere overlap tussen taalkunde en logica, met het verschil dat natuurlijke talen gezien als logisch systeem inconsistent zijn. Dat blijkt uit paradoxen als "ik lieg", "mijn neus groeit" (gezegd door Pinokkio, voor wie geldt dat zijn neus groet als hij liegt), en "de kapper van Urk (die in Urk woont) scheert alle inwoners van Urk die zichzelf niet scheren". In alle gevallen is de uitspraak tegelijk waar en onwaar.

Bij een eerste kennismaking met de propositielogica is het handig om af te wijken van de bovenstaande volgorde (waarin de semantiek na de syntax komt) en na de eerste twee punten direct over te gaan op het laatste, en pas daarna terug te komen op de axioma's en de deductieregels. De reden is dat de axioma's op het eerste gezicht nogal vreemd overkomen, terwijl de zgn. waarheidstabellen heel natuurlijk zijn.

- De *notatie* van de propositielogica bestaat uit twee groepen symbolen:
  1. De *zuiver logische symbolen* zijn
     $\neg \ \wedge \ \vee \ \rightarrow$
     Dit zijn de bekende afkortingen voor resp. *niet, en, of, impliceert*. Maar let op! De hier gegeven betekenis van de zuiver logische symbolen is in principe niet nodig, omdat deze *betekenis* volgt uit de later op te stellen axioma's voor het *gebruik* van de symbolen.[3]
  2. Voor het gemak gebruiken we ook haakjes $(\ ,\ )$, maar we laten de regels daarvoor weg, want eigenlijk zijn ze overbodig als we afspreken dat $\neg$ sterker bindt dan $\vee$ and $\wedge$, die op hun beurt weer sterker binden dan $\rightarrow$: bijvoorbeeld $\neg\alpha \vee \delta \rightarrow \beta \wedge \gamma$ staat voor $((\neg\alpha) \vee \delta) \rightarrow (\beta \wedge \gamma)$.
  3. De *niet-logische sysmbolen* zijn $p_1, p_2, \ldots$ (aftelbaar veel, ook te schrijven als $p, p', \ldots$ of $p, q, \ldots$). Deze symbolen staan voor zogenaamde *atomaire proposities*, die het eenvoudigste voorbeeld zijn van uitspraken (zie volgende punt). Syntactisch zijn dit slechts symbolen, maar semantisch kun je ze binnen of buiten de wiskunde interpreteren, zoals resp. "$7 + 5 = 12$" of "het regent". Ze kunnen echter niet zelf weer variabelen bevatten.
- In de propositielogica is er geen verschil tussen formules en uitspraken; deze soorten uitdrukkingen vallen pas in de predikaatlogica uiteen. De *uitspraken* van de propositielogica, genaamd $\alpha, \beta, \ldots$, zijn alle uitdrukkingen in de bovenstaande symbolen die als volgt tot stand komen:

  i) ieder niet-logisch symbool $p_1, p_2, \ldots$ is een uitspraak;

  ii) Als α en β uitspraken zijn, dan zijn $\alpha \wedge \beta$, $\alpha \vee \beta$, $\neg\alpha$, en $\alpha \rightarrow \beta$ dat ook.[4]

  Dit is een *iteratief* voorschrift: als je regel **ii)** toepast op regel **i)** kom je bijvoorbeeld op $\alpha \equiv p_1 \vee p_2$ en $\beta \equiv \neg p_3$, en daaruit mag je vervolgens m.b.v. regel **ii)** $\alpha \rightarrow \beta$, oftewel $p_1 \vee p_2 \rightarrow \neg p_3$ maken, enzovoort. Let op: we gebruiken het symbool $\equiv$ hier informeel om een uitspraak een naam te geven. De notatie $\alpha \equiv p_1 \vee p_2$ betekent dus: de uitdrukking $p_1 \vee p_2$ heet α, of wordt afgekort als α.

We onderbreken nu de opbouw van de syntax en gaan verder met de *semantiek* van de propositielogica. Deze wordt gegeven door het toekennen van een oordeel 'waar' of 'onwaar' aan uitspraken α. We noteren $\alpha = 1$ als α waar is en $\alpha = 0$ als α onwaar is. Dit oordeel is in het algemeen niet absoluut: of α waar is hangt i.h.a. af van de (on)waarheid van de atomaire proposities p_i die α bevat. Stel, voor het meest triviale geval, dat $\alpha \equiv p_1$. Dan is α uiteraard waar desda p_1 waar is. Ingewikkeldere gevallen worden bepaald door de alledaagse betekenis van de symbolen $\neg, \wedge, \vee, \rightarrow$, via de *waarheidstabellen*:

α	$\neg\alpha$
0	1
1	0

α	β	$\alpha \wedge \beta$
0	0	0
0	1	0
1	0	0
1	1	1

α	β	$\alpha \vee \beta$
0	0	0
0	1	1
1	0	1
1	1	1

α	β	$\alpha \rightarrow \beta$
0	0	1
0	1	1
1	0	0
1	1	1

De eerste moet als volgt worden gelezen: als α onwaar is, dan is $\neg\alpha$ waar, en als α waar is, dan is $\neg\alpha$ juist onwaar, enzovoort. Het enige niet echt alledaagse gebruik van de logische symbolen is dat als α en β beide onwaar zijn, de implicatie $\alpha \rightarrow \beta$ dan waar is. Deze rare afspraak heeft echter grote voordelen.

Uit deze tabellen volgt de (on)waarheid van iedere uitspraak γ als functie van de (on)waarheid van alle atomaire proposities p_i die γ bevat; deze functie is in feite de waarheidstabel van γ zelf, zoals bijv.

p_1	p_2	γ
0	0	0
0	1	0
1	0	1
1	1	0

$\gamma \equiv p_1 \wedge (\neg p_2)$.

3. Dit is helemaal in de geest van de beroemde filosoof Ludwig Wittgenstein (1889–1951): *meaning is use*.
4. Dit geeft een tweede gebruik van haakjes: als bijv. $\alpha \equiv p_1 \rightarrow p_2$ en $\beta \equiv p_1 \wedge p_3$, dan staat $(p_1 \rightarrow p_2) \rightarrow (p_1 \wedge p_3)$ voor $\alpha \rightarrow \beta$.

Om het gebruik van deze tabellen uit te leggen behandelen we eerst het bovenstaande voorbeeld, en daarna een iets ingewikkelder voorbeeld. Als je deze voorbeelden goed begrijpt, en tevens doorhebt hoe je volgens de bovengenoemde regels op inductieve wijze uitspraken maakt, zul je inzien dat op een dergelijke wijze iedere uitspraak uit de propositielogica van een waarheidstabel kan worden voorzien (we laten het formele bewijs daarvan weg, dat gebruik maakt van inductie).

Het uitgangspunt is dat de vier tabellen gelden voor *alle* uitspraken α en β uit de propositielogica. Om bijvoorbeeld te zien of $\gamma \equiv p_1 \wedge (\neg p_2)$ (on)waar is voor $p_1 = p_2 = 0$ kijken we eerst in de tabel voor $\neg$ met $\alpha \equiv p_2$ en zien daar op de eerste rij dat $\neg p_2 = 1$ als $p_2 = 0$. Vervolgens kijken we in de tabel voor $\wedge$ met $\alpha \equiv p_1$ en $\beta \equiv \neg p_2$. We hebben net gezien dat $p_1 = p_2 = 0$ correspondeert met $p_1 = 0$ en $\neg p_2 = 1$. We kijken dus in de tweede rij, waar links $0\ 1$ staat en vinden onder $\alpha \wedge \beta$ de uitkomst 0. Voor $p_1 = p_2 = 0$ geldt dus $\gamma = 0$. Enzovoort.

Nu geven we een voorbeeld waarin slechts de implicatie $\rightarrow$ voorkomt. We willen weten of de uitspraak

$$(p_1 \rightarrow (p_2 \rightarrow p_3)) \rightarrow ((p_1 \rightarrow p_2) \rightarrow (p_1 \rightarrow p_3))$$

waar is, gegeven $p_1 = 1$, $p_2 = 0$, en $p_3 = 1$ (ga eerst na dat deze uitspraak volgens de twee regels **i)** en **ii)** boven kan worden gemaakt!). Met bijv. "tweede rij" in een tabel boven bedoelen we de tweede rij met nullen en enen. De rechtertabel is die voor $\rightarrow$.

Stap 1: Rechtertabel met $\alpha \equiv p_2 = 0$ en $\beta \equiv p_3 = 1$: uit de tweede rij volgt $(p_2 \rightarrow p_3) = 1$.
Stap 2: Rechtertabel met $\alpha \equiv p_1 = 1$ en $\beta \equiv (p_2 \rightarrow p_3) = 1$; vierde rij geeft $(p_1 \rightarrow (p_2 \rightarrow p_3)) = 1$.
Stap 3: Analoog $(p_1 \rightarrow p_2) = 0$ (derde rij) en $(p_1 \rightarrow p_3) = 1$.
Stap 4: En daaruit $((p_1 \rightarrow p_2) \rightarrow (p_1 \rightarrow p_3)) = 1$ (tweede rij).
Stap 5: Ten slotte geeft de vierde rij met $\alpha \equiv (p_1 \rightarrow (p_2 \rightarrow p_3)) = 1$ en $\beta \equiv ((p_1 \rightarrow p_2) \rightarrow (p_1 \rightarrow p_3)) = 1$ het antwoord: $(p_1 \rightarrow (p_2 \rightarrow p_3)) \rightarrow ((p_1 \rightarrow p_2) \rightarrow (p_1 \rightarrow p_3)) = 1$, oftwel de uitspraak is waar!

Hier is iets bijzonders aan de hand, dat allerminst voor iedere uitspraak geldt: de bovenstaande uitspraak is *altijd* (i.e., voor alle waarden 0 of 1 van p_1, p_2, p_3) waar (opgave)!

Definitie 3.1 *Een uitspraak φ die voor alle mogelijke waarheidstoekenningen (0 of 1) aan de atomaire proposities $p_1, p_2, \ldots$ die er in voorkomen waar is, heet een* tautologie*, notatie: $\models \varphi$.*

Zo is $\alpha \rightarrow \alpha$ een tautologie, hoe α ook is opgebouwd uit de $p_1, p_2, \ldots$. Dit volgt uit de waarheidstabel voor $\alpha \rightarrow \beta$ door α te substitueren voor β. Dan zijn de enige mogelijkheden $\alpha = 0$ (eerste rij) en $\alpha = 1$ (laatste rij), in beide gevallen met $(\alpha \rightarrow \alpha) = 1$. Als we een nieuw logisch symbool $\leftrightarrow$ invoeren d.m.v.

$\alpha \leftrightarrow \beta$ is een afkorting voor $(\alpha \rightarrow \beta) \wedge (\beta \rightarrow \alpha)$,

dan volgt (opgave):

Stelling 3.1 *De uitspraak $\alpha \leftrightarrow \beta$ is een tautologie desda het volgende geldt: voor iedere gegeven waarde van de atomaire proposities in α en β zijn α en β ofwel tegelijk waar, ofwel tegelijk onwaar (als α en β dezelfde atomaire proposities bevatten is dit het geval desda α en β dezelfde waarheidstabel hebben).*

We gaan nu terug naar de syntax van de propositielogica: wat zijn de axioma's en deductieregels? Bij deze vraag moeten we even stilstaan bij de bedoeling van de theorie. Zoals gebruikelijk noemen we een bewezen uitspraak φ een *stelling*, notatie: $\vdash \varphi$. Een bewijs van een stelling bestaat uit eindig aantal stappen, waarin telkens de deductieregels op de vorige stap(pen) worden toegepast. De eerste stap bestaat officieel uit het opschrijven van de axioma's die in het bewijs worden gebruikt. Welke uitspraken stellingen zijn is dus een puur syntactische kwestie, die niet afhangt van hun interpretatie. Juist daaraan ontleent de wiskunde volgens Hilbert haar zekerheid: de interpretatie en eventuele waarheid van uitspraken (regent het?) hangt af van de waan van de dag, maar de bewijsbaarheid niet. Daarom mag de eventuele bewijsbaarheid van een uitspraak niet afhangen van de (on)waarheid van de atomaire proposities die erin voorkomen. Tegelijk wil niemand dat stellingen die onder een bepaalde waarheidstoekenning aan de p_i onwaar zijn, bewezen kunnen worden: het kunnen bewijzen van onware stellingen zou rampzalig zijn voor de reputatie van de wiskunde! Een stelling moet dus altijd waar zijn, oftewel:

Een bewijsbare uitspraak in de propositielogica moet een tautologie zijn.

De kunst is nu om de axioma's en deductieregels zo te kiezen dat zo veel mogelijk tautologieën bewezen kunnen worden. Dit doel kan in de klassieke propositielogica op optimale wijze worden bereikt: bij de juiste keuze kunnen zelfs *alle* tautologieën worden bewezen (zie Stelling 3.3 verderop). Je kunt enigszins heen en weer schuiven tussen axioma's en deductieregels, maar wij kiezen kort en krachtig:

- De enige deductieregel is de *modus ponens*: voor alle uitspraken α en β geldt dat als α en $\alpha \to \beta$ bewezen zijn, dan β bewezen is. Kort: uit $\alpha \to \beta$ en α volgt β. Nog korter: $\alpha \to \beta, \alpha \vdash \beta$.
- De *axioma's* kunnen op vele manieren worden gegeven. Allereerst stellen we vast (opgave) dat

$$\alpha \wedge \beta \quad \leftrightarrow \quad \neg(\alpha \to \neg\beta) \tag{3.1}$$
$$\alpha \vee \beta \quad \leftrightarrow \quad \neg\alpha \to \beta \tag{3.2}$$

  tautologieën zijn, zodat het gebruik van de symbolen $\vee$ en $\wedge$ in principe overbodig is: als je wilt kun je $\alpha \wedge \beta$ als afkorting beschouwen van $\neg(\alpha \to \neg\beta)$, en $\alpha \vee \beta$ als afkorting van $(\neg\alpha) \to \beta$. Alternatief kun je wel werken met alle vier de symbolen $\neg \wedge \vee \to$ en de tautologieën (3.1) en (3.2) toevoegen als axioma's of als deductieregels. Een mogelijke keuze van de resterende axioma's voor $\neg$ en $\to$, afkomstig van de logicus Alonzo Church (1903–1995), is dan:

  Axioma 1. $\beta \to (\alpha \to \beta)$;

  Axioma 2. $(\beta \to (\gamma \to \delta)) \to ((\beta \to \gamma) \to (\beta \to \delta))$;

  Axioma 3. $(\neg\alpha \to \neg\beta) \to ((\neg\alpha \to \beta) \to \alpha)$.

Deze axioma's gelden voor alle uitspraken α, β, γ, δ die volgens de regels **i)** en **ii)** zijn gemaakt. De eerste twee zullen we zo leren kennen. Het derde axioma reguleert het gebruik van de negatie $\neg$ en rechtvaardigt, samen met de *modus ponens*, in het bijzonder het *bewijs uit het ongerijmde*. In zo'n bewijs wil je α bewijzen door een tegenspraak af te leiden uit de aanname niet-α. Stel dat je daaruit zowel β als $\neg\beta$ kunt afleiden, zodat je uitspraken $\neg\alpha \to \beta$ en $\neg\alpha \to \neg\beta$ hebt bewezen. Uit de laatste en Axioma 3 volgt, met de *modus ponens*, $(\neg\alpha \to \beta) \to \alpha$. Uit de eerste en *modus ponens* volgt dan α.

Een *bewijs* van een bepaalde uitspraak is een afleiding van deze uitspraak uit de axioma's en de *modus ponens*. Hoe ziet zo'n bewijs er uit? Als illustratie bewijzen we de voor de hand liggende stelling $\alpha \to \alpha$, maar zelfs dat bewijs vereist al enig nadenken! Je hebt alleen axioma's 1 en 2 nodig. Axioma 1 met β vervangen door α (notatie: $\beta \rightsquigarrow \alpha$) en tevens de substitutie $\alpha \rightsquigarrow (\alpha \to \alpha)$ geeft

$$\alpha \to ((\alpha \to \alpha) \to \alpha). \tag{3.3}$$

Axioma 2 met $\beta \rightsquigarrow \alpha$, $\gamma \rightsquigarrow (\alpha \to \alpha)$, $\delta \rightsquigarrow \alpha$ geeft

$$(\alpha \to ((\alpha \to \alpha) \to \alpha)) \to ((\alpha \to (\alpha \to \alpha)) \to (\alpha \to \alpha)). \tag{3.4}$$

Modus ponens, i.e uit $\alpha \to \beta$ en α volgt β, met $\alpha \rightsquigarrow (\alpha \to ((\alpha \to \alpha) \to \alpha))$ (dit is precies (3.3) en tevens het linkerlid van (3.4)) en $\beta \rightsquigarrow ((\alpha \to (\alpha \to \alpha)) \to (\alpha \to \alpha))$ (dit is het rechterlid van (3.4)) geeft dan

$$(\alpha \to (\alpha \to \alpha)) \to (\alpha \to \alpha). \tag{3.5}$$

Nu gebruiken we nogmaals Axioma 1 met $\beta \rightsquigarrow \alpha$ en $\alpha \rightsquigarrow \alpha$, dus $\alpha \to (\alpha \to \alpha)$. Maar dit is precies het linkerlid van (3.5). Modus ponens met $\alpha \rightsquigarrow (\alpha \to (\alpha \to \alpha))$ en $\beta \rightsquigarrow (\alpha \to \alpha)$ geeft ten slotte $\alpha \to \alpha$, QED.

Zonder bewijs geven we een handig hulpmiddel, dat je bij het formele bewijzen mag gebruiken:[5]

Stelling 3.2 *1. Uit $\beta \to \gamma$ en $\gamma \to \delta$ volgt $\beta \to \delta$;*

2. Uit $\beta \to (\gamma \to \delta)$ en γ volgt $\beta \to \delta$.

Het hele formalisme is opgezet om te zorgen dat de stellingen, met andere woorden de bewijsbare uitspraken, precies de tautologieën zijn. Is dit doel nu ook bereikt? Jawel! Er geldt namelijk:

Stelling 3.3 *Een uitspraak in de propositielogica is een tautologie desda zij bewijsbaar is.*

5. Voor de liefhebbers: deze stelling volgt uit de zgn. "deductie-stelling" over propositielogica (voor een bewijs zie college Logica): Als een bepaalde uitspraak β volgt uit een andere uitspraak α en uit mogelijk eerder bewezen uitspraken γ_1 t/m γ_n (en de axioma's en de *modus ponens*), dan volgt de uitspraak $\alpha \to \beta$ uit γ_1 t/m γ_n (en de axioma's en de *modus ponens*).

We bewijzen hier alleen dat stellingen tautologieën zijn; het omgekeerde is lastiger (zie college Logica). De eenvoudigste stellingen zijn de axioma's (waarin de deductieregel nul keer is gebruikt), en deze zijn inderdaad tautologieën (opgave). Vervolgens behoudt de *modus ponens* waarheid, in de zin dat als α en $\alpha \to \beta$ waar zijn, dan ook β waar is (zie de vierde rij van de waarheidstabel voor $\alpha \to \beta$). Een stelling moet in een eindig aantal stappen door toepassing van de *modus ponens* worden verkregen uit de axioma's. Iedere stap behoudt volgens het bovenstaande argument het tautologische karakter van de axioma's. Een stelling uit de propositielogica is dus een tautologie. Q.E.D.

Maar toch zijn de begrippen 'stelling' en 'tautologie' conceptueel totaal verschillend: stellingen zijn syntactisch gedefinieerd en hebben dus alles te maken met de symbolen, de axioma's, en de afleidingsregels (en niets met de interpretatie), terwijl tautologieën semantisch zijn gedefinieerd via de mogelijke (on)waarheid van de atomaire proposities p_i die in een uitspraak voorkomen.

Voor de volledigheid geven we ook axioma's voor andere mogelijke keuzes van de onafhankelijke logische symbolen. We hebben boven $\neg$ and $\to$ genomen, maar ook mogelijk zijn:

- $\vee$ en $\neg$, waarbij de andere twee worden ingevoerd door de tautologieën

$$\alpha \to \beta \quad \leftrightarrow \quad \neg\alpha \vee \beta; \tag{3.6}$$
$$\alpha \wedge \beta \quad \leftrightarrow \quad \neg(\neg\alpha \vee \neg\beta). \tag{3.7}$$

  De enige afleidingsregel is de modus ponens en de axioma's zijn (Hilbert en Ackermann):

  Axioma 1: $(\beta \vee \beta) \to \beta$;

  Axioma 2: $\beta \to (\beta \vee \gamma)$;

  Axioma 3: $(\gamma \vee \beta) \to (\beta \vee \gamma)$;

  Axioma 4: $(\gamma \to \delta) \to ((\beta \vee \gamma) \to (\beta \vee \delta))$.

- $\wedge$ en $\neg$, waarbij de andere twee worden ingevoerd door de tautologieën

$$\alpha \to \beta \quad \leftrightarrow \quad \neg(\alpha \wedge \neg\beta); \tag{3.8}$$
$$\alpha \vee \beta \quad \leftrightarrow \quad \neg(\neg\alpha \wedge \neg\beta). \tag{3.9}$$

  De enige afleidingsregel is de modus ponens en de axioma's zijn (Rosser):

  Axioma 1: $\beta \to (\beta \wedge \beta)$;

  Axioma 2: $(\beta \wedge \gamma) \to \beta$;

  Axioma 3: $(\beta \to \gamma) \to (\neg(\gamma \wedge \delta) \to \neg(\beta \wedge \delta))$.

- Omdat deze axiomaschema's niet zo heel inzichtelijk zijn, zou je kunnen denken dat het eenvoudiger is om axioma's te geven in termen van alle vier de logische symbolen $\neg$, $\vee$, $\wedge$, en $\to$. Dat kan inderdaad, met slechts de modus ponens, maar dan krijg je wel tien axioma's (Kleene):

  Axioma 1: $\beta \to (\beta \vee \gamma)$;

  Axioma 2: $(\beta \to (\gamma \to \delta)) \to ((\beta \to \gamma) \to (\beta \to \delta))$;

  Axioma 3: $(\beta \wedge \gamma) \to \beta$;

  Axioma 4: $(\beta \wedge \gamma) \to \gamma$;

  Axioma 5: $\beta \to (\gamma \to (\beta \wedge \gamma))$;

  Axioma 6: $\beta \to (\beta \vee \gamma)$;

  Axioma 7: $\gamma \to (\beta \vee \gamma)$;

  Axioma 8: $(\beta \to \delta) \to ((\gamma \to \delta) \to ((\beta \vee \gamma) \to \delta))$;

  Axioma 9: $(\beta \to \gamma) \to ((\beta \to \neg\gamma) \to \neg\beta)$;

  Axioma 10: $\neg\neg\beta \to \beta$.

Opgave 3.1

*Alleen **e)** en **f)** inleveren, de rest is om zelf te oefenen!*

a) Geef de waarheidstabel voor $\leftrightarrow$ en bewijs daarmee Stelling 3.1.
b) Laat zien dat (3.1), (3.2), (3.6), en (3.7) tautologieën zijn.
c) Laat zien dat de drie axioma's van Church tautologieën zijn.
d) Laat zien dat $\alpha \vee (\neg\alpha)$ een tautologie is.
e) Laat zien dat $(\alpha \wedge (\alpha \to \beta)) \to \beta$ een tautologie is (vgl. de de *modus ponens*).
f) Bewijs vanuit de axioma's 1 t/m 3 en de *modus ponens* dat

$$\neg\neg\alpha \to \alpha \tag{3.10}$$

en vervolgens dat

$$\alpha \to \neg\neg\alpha. \tag{3.11}$$

N.B. je mag hier niet Stelling 3.3 gebruiken, maar wel Stelling 3.2.

Opgave 3.2

Voor latere toepassingen in de informatica blijkt het volgende probleem interessant te zijn: gegeven even uitspraak γ die atomaire proposities p_1 t/m p_n bevat, bestaat er een waarheidstoekenning aan de p_i zodat $\gamma = 1$? In dat geval heet γ *verzadigbaar* (Engels: *satisfiable*). Voor kleine uitspraken kun je alle mogelijkheden uitproberen, maar voor grote is dat exponentieel in n en praktisch onmogelijk. Er is een nauw verband tussen satisfactie en het begrip tautologie:

Stelling 3.4 *Een uitspraak γ is verzadigbaar desda $\neg\gamma$ géén tautologie is.*

a) Bewijs Stelling 3.4.
b) Bepaal of the uitspraak $((p_1 \to p_2) \vee \neg((\neg p_1 \leftrightarrow p_3) \vee p_4)) \wedge \neg p_2$ verzadigbaar is.

Opgave 3.3

Het is zelfs mogelijk om met één enkel logisch symbool te werken! De *Sheffer stroke* $|$ (in de computerwereld vaak NAND genoemd) maakt uit twee bestaande uitspraken α en β een nieuwe uitspraak $\alpha|\beta \equiv \neg(\alpha \wedge \beta)$.

a) Geef de waarheidstabel van de Sheffer stroke.
b) Laat zien dat $\neg\alpha \leftrightarrow (\alpha|\alpha)$ en $\alpha \vee \beta \leftrightarrow (\alpha|\alpha)|(\beta|\beta)$ tautologieën zijn (je mag hierbij zonder bewijs (3.6) t/m (3.9) gebruiken).
c) Geef soortgelijke tautologieën die $\alpha \to \beta$ en $\alpha \wedge \beta$ uitdrukken in $|$.

Opgave 3.4

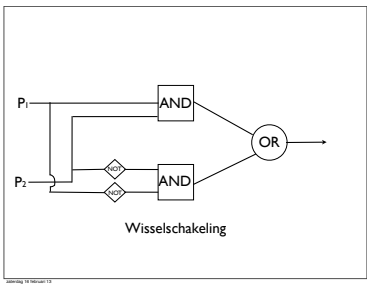
Er bestaat een voor de hand liggend maar interessant verband tussen propositielogica en elektronische circuits.[6] Zo'n circuit heeft ruw gezegd als doel om bij iedere mogelijke stand van n aan/uit schakelaars een lamp wel of niet te doen branden. Het circuit bestaat uit drie soorten poorten, genaamd OR, AND, en NOT, verbonden door draden: de OR en AND poorten hebben twee ingangen en één uitgang, en de NOT part heeft één ingang en één uitgang.[7] Het circuit als geheel heeft n ingangen p_1 t/m p_n, dat zijn de aan/uit schakelaars, en één uitgang, die de lamp voedt. Door alle draden gaat wel of geen stroom, aangegeven met 1 resp. 0.; als p_i aan staat geeft die stroom 1, en als hij uit staat stroom 0, aangegeven met $p_i = 0$ of $p_i = 1$.

6. Ontdekt door Claude Shannon, volgens velen de grondlegger van het informatietijdperk, zie het boek in voetnoot 1.
7. In diagrammen kun je de poorten desgewenst met een cirkel, vierkant, e.d. aangeven

Een draad kan vertakken (opsplitsen) en bij vertakking houden alle takken dan dezelfde waarde van de stroom. De schakelingen gedragen zich volgens de waarheidstabellen van de bijbehorende logische symbolen: $\vee$ bij OR, $\wedge$ bij AND, and $\neg$ bij NOT (voorbeelden: als 1 in NOT gaat komt er 0 uit, als 1 en 0 in OR gaat komt er 1 uit, enzovoort).
Er zijn nu twee soorten problemen. Het ene is om een circuit te bouwen dat bij iedere mogelijke stand van de schakelaars een gegeven uitgangsstroom heeft. Een klassiek voorbeeld is de wisselschakeling: deze verbindt twee schakelaars ('beneden' en 'boven') met een lamp, die brandt als beide schakelaars aan staan of beide uit staan, maar niet brandt als een van de twee aan staat en de ander uit. Het andere probleem is om bij een gegeven circuit te bepalen of er stroom uit het circuit komt, als functie van de waarden van de p_i. Om dergelijke problemen op te lossen identificeren we iedere schakelaar met een atomaire propositie, iedere poort met het bijbehorende logische symbool (het symbool $\rightarrow$ wordt hier dus niet gebruikt), en het circuit C met een uitspraak γ uit de propositielogica. Bij gegeven waarden van de p_i komt er stroom uit C desda $\gamma = 1$. De wisselschakeling correspondeert bijvoorbeeld met de uitspraak

$$\gamma \equiv (\neg p_1 \wedge \neg p_2) \vee (p_1 \wedge p_2), \tag{3.12}$$

en het bijbehorende circuit is



a) Geef de waarheidstabel voor de uitspraak (3.12) en ga na dat dit circuit inderdaad de wisselschakeling realiseert.

b) Geef een uitspraak en een circuit dat de volgende schakeling realiseert: er zijn opnieuw twee schakelaars, maar nu brandt de lamp als één van de twee aan is en de andere uit (en brandt niet als ze beide aan of beide uit staan).

4

Predikaatlogica

De propositielogica is te eenvoudig om bijv. rekenkunde te beschrijven, laat staan verzamelingenleer, omdat in de syntax geen variabelen en geen kwantoren zoals 'er is' ($\exists$) en 'voor alle' ($\forall$) voorkomen.[1] Die zijn er wel in de *predikaatlogica*, ook genoemd *eerste-orde logica*, waar dit hoofdstuk over gaat. We bespreken zowel de rekenkunde als de verzamelingenleer als voorbeelden van een eerste-orde logisch systeem. Het gebruikelijke eerste-orde systeem voor de rekenkunde heet *Peano Aritmetiek* (ofschoon Peano zelf het nooit in deze formele vorm opschreef) en wordt afgekort als **PA**. Het gangbare eerste-orde systeem voor de verzamelingenleer is genoemd naar Zermelo en Fraenkel en wordt afgekort als **ZF**.

- De notatie van een eerste-orde logisch systeem is opgebouwd uit *symbolen* in twee groepen.

  1. De *zuiver logische symbolen* hangen niet af van het gebied van de wiskunde dat wordt beschreven. Dit zijn de symbolen $\neg, \wedge, \vee, \rightarrow$ uit de propositielogica, aangevuld met het gelijkteken $=$ en met de kwantoren $\forall$ en $\exists$, voor resp. 'voor alle' en 'er bestaat'. Ook nu bestaan er relaties tussen deze symbolen, waardoor het in principe voldoende is om bijvoorbeeld slechts $\neg$, $\rightarrow$, $=$, en $\forall$ te gebruiken. De eliminatie van $\vee$ en $\wedge$ is hetzelfde als in de propositielogica en $\exists_x$ (zie onder) kan worden vervangen door $\neg\forall_x\neg$ (denk hier even over na!).

  2. De *niet-logische sysmbolen* hangen af van het gebied van de wiskunde dat je probeert te axiomatiseren. Ze zijn in detail dus verschillend voor bijv. rekenkunde en verzamelingenleer, maar het meest algemene formaat van niet-logische symbolen is als volgt.

     (a) Aftelbaar veel *variabelen* $a, b, c, \ldots, x, y, z, x_1, x_2, \ldots$.

     Bij **PA** kun je bij deze variabelen denken aan de natuurlijke getallen, maar deze interpretatie is *geen* onderdeel van het logische systeem en dient slechts ter motivatie.
     In **ZF** kunnen de variabelen evenzo worden geïnterpreteerd als verzamelingen.

     (b) *Constanten*, die je kunt noteren hoe je wilt.

     In **PA** is er slechts één constante, genaamd **0**, later te interpreteren als het getal nul.

     Ook in **ZF** is er één constante, $\emptyset$, later te interpreteren als de lege verzameling.

     (c) *Functiesymbolen*. Ieder functiesymbool f heeft een zogenaamde *ariteit* $a(f)$, een natuurlijk getal dat aangeeft hoeveel variabelen de desbetreffende functie als input heeft.[2]

     In **PA** zijn er drie functiesymbolen, namelijk S, $+$, en $\times$, met ariteiten resp. $a(S) = 1$, $a(+) = 2$, en $a(\times) = 2$. Ook hier geven we alvast de latere interpretatie als resp. de successorfunctie $k \mapsto k + 1$, optelling, en vermenigvuldiging, maar opnieuw is deze interpretatie *geen* onderdeel van het formele logische systeem.
     ZF heeft (verrassenderwijs) geen functiesymbolen.[3]

     (d) *Predikaatsymbolen*, eveneens met bijbehorende ariteiten $a \in \mathbb{N}$ (inclusief 0). De predikaatsymbolen spelen een rol bij het definiëren van formules; zie onder. Voorbeelden:
     PA heeft (verrassenderwijs) geen predikaatsymbolen.[4]
     In **ZF** is het enige predikaatsymbool $\in$, eveneens met ariteit 2.

---

1. Zoals we zullen zien zijn de atomaire proposities p_i technisch gesproken geen variabelen maar zgn. predikaatsymbolen.
2. Deze naam komt van het Engelse *arity*; vgl. un*ary*, bin*ary*, etc. Een functiesymbool f met $a(f) = 0$ is een constante.
3. We zullen later zien dat functies $f : X \rightarrow Y$ in de verzamelingenleer worden gedefinieerd als deelverzamelingen van $X \times Y$.
4. Soms wordt in **PA** ook $<$ als predikaat met ariteit 2 gebruikt. Sommige auteurs rekenen $=$ tot de predikaatsymbolen.

- Uit deze symbolen worden eerst volgens bepaalde regels *termen* gemaakt, die op hun beurt aanleiding geven tot *formules*, meestal genoteerd als φ of ψ, etc. Speciale formules zijn vervolgens *uitspraken*, die kandidaten zijn voor stellingen (dus al dan niet bewijsbaar zijn). Het verschil tussen formules en uitspraken blijkt uit een eenvoudig voorbeeld: je kunt niet eisen dat een uitdrukking als $x^2 = 1$ wel of niet bewijsbaar is; dat is dan ook 'slechts' een formule. Dat kun je wel eisen van $\exists_x(x^2 = 1)$ of $\forall_x(x^2 = 1)$; dat zijn dan ook uitspraken. We geven nu de algemene formatieregels voor termen en formules, en de regel die bepaalt welke formules uitspraken zijn.

  1. De iteratieve procedure om *termen* te produceren is als volgt:
     (a) iedere variabele x_i is een term;
     (b) iedere constante is een term;
     (c) een functiesymbool f en $a(f) = k$ termen $(t_1, \ldots, t_k)$ bepalen een term $f(t_1, \ldots, t_k)$.

     In **PA** betekent dit dat $S(t)$ een term is en dat $t_1 + t_2 \equiv +(t_1, t_2)$ en $t_1 \times t_2 \equiv \times(t_1, t_2)$ termen zijn, tenminste als t, t_1, en t_2 dat zijn. Dit is niet zo ingewikkeld als het lijkt! De constante $\mathbf{0}$ is bijvoorbeeld een term, zodat $S(\mathbf{0})$ dat ook is. Voor deze term voeren we de naam $\mathbf{1}$ in. Dit kunnen we herhalen: $S^n(\mathbf{0})$ is een term, die we afkorten als $\mathbf{n}$ (waarbij bijv. $S^2(\mathbf{0}) \equiv S(S(\mathbf{0}))$, etc.). Daaruit kunnen we de term $\mathbf{n} + \mathbf{m}$ maken, of $\mathbf{n} \times x_i$, en vervolgens $(\mathbf{n} + \mathbf{m}) \times (\mathbf{n} \times x_i)$, enz. Dit soort dingen doe je in de wiskunde de hele dag! Wat je niet als term kunt maken is iets als $S(+)$ of $\mathbf{n}\times$ en dergelijke onzin.

     In **ZF** zijn de enige termen $\emptyset$ en de variabelen (er zijn immers geen functiesymbolen).

  2. Uit de termen maken we als volgt (iteratief) *formules* m.b.v. $=$ en de predikaatsymbolen:
     (a) Als t_1 en t_2 termen zijn, is $t_1 = t_2$ een formule.
     (b) Een predikaatsymbool P en $a(P) = k$ termen $(t_1, \ldots, t_k)$ bepalen een formule $P(t_1, \ldots, t_k)$.

     In **PA** is $t_1 = t_2$ een formule, als t_1 en t_2 termen zijn.

     In **ZF** zijn $t_1 \in t_2$ en $t_1 = t_2$ formules, als t_1 en t_2 termen zijn.

     (c) Nu komen de andere zuiver logische symbolen aan bod:
        i. Ten eerste geldt net als in de propositielogica dat als φ en ψ formules zijn, de uitdrukkingen $\neg\varphi$, $\varphi \vee \psi$, $\varphi \wedge \psi$, en $\varphi \to \psi$ dat ook zijn.
        ii. Bovendien zijn nu ook $\exists_x\varphi$ en $\forall_x\varphi$ formules, voor een willekeurige variabele x.

     De variabele x hoeft niet in φ voor te komen om $\exists_x\varphi$ en $\forall_x\varphi$ correct te kunnen opschrijven. Zo is de uitspraak $\exists_x S(\mathbf{0}) + S(\mathbf{0}) = S(S(\mathbf{0}))$ grammaticaal correct (en ook nog eens waar!).

     – Een variabele x in een formule φ heet *gebonden* als er deelformules $\forall_x\psi_i(x)$ van φ bestaan met de eigenschap dat x uitsluitend in deze deelformules voorkomt.[5]
     – Een variabele x in een formule φ heet *vrij* als deze niet gebonden is.

     Voorbeelden:

     (a) in de formule $x + y = y + x$ zijn zowel x als y vrije variabelen;
     (b) in $\forall_x\forall_y(x + y = y + x)$ zijn ze daarentegen beide gebonden;
     (c) in $\exists_x x + S(\mathbf{0}) = y$ is x gebonden en y vrij.
     (d) in $(\forall_x\alpha(x)) \wedge \beta(x)$, waarin x vrij is in zowel $\alpha(x)$ als in $\beta(x)$, is x vrij.
     (e) in $\forall_x(\alpha(x) \wedge \beta(x))$, waarin x vrij is in zowel $\alpha(x)$ als in $\beta(x)$, is x gebonden.

     Om aan te geven dat φ tenminste de variabele x vrij bevat schrijven we soms $\varphi(x)$ i.p.v. φ, en analoog bijv. $\varphi(x_1, \ldots, x_n)$ als φ tenminste de variabelen $(x_1, \ldots, x_n)$ vrij bevat. Dit is nuttig als je de rol van juist deze vrije variabelen wilt benadrukken.[6] Je zou de formule in (a) dus φ of $\varphi(x, y)$ mogen noemen, die in (b) $\forall_x\forall_y\varphi$ of $\forall_x\forall_y\varphi(x, y)$, die in (c) ψ of $\psi(y)$, maar niet $\psi(x)$. Er zijn dus twee soorten formules:

     – in een *open formule* komt minstens één vrije variabele voor.
     – In een *gesloten formule* zijn alle variabelen gebonden, of zijn er geen variabelen.

     Een *uitspraak* is hetzelfde als een gesloten formule.

5. Een *deelformule* van een formule φ is een (ook op zichzelf zinvolle) formule die in φ voorkomt (inclusief φ zelf). Volgens de formatieregels kan een variabele uitsluitend in een formule terechtkomen via een uitdrukking van de vorm $t_1 = t_2$ of van de vorm $R(t_1, \ldots, t_k)$. Uiteraard zijn dit zelf al deelformules van φ, waaruit door de formatieregels weer nieuwe deelformules kunnen ontstaan die x bevatten. Als alle deelformules $t_1 = t_2$ of $R(t_1, \ldots, t_k)$ die x bevatten uiteindelijk terecht komen in deelformules van de vorm $\forall_x\psi_i(x)$, dan is x gebonden.
6. Sommige logicaboeken schrijven juist $\varphi(x_1, \ldots, x_n)$ als de werkelijke vrije variabelen in φ bevat zijn in $(x_1, \ldots, x_n)$.

- *Axioma's* zijn syntactisch een speciaal geval van formules. We gaan er hier vanuit dat $\wedge$, $\vee$, en $\exists$ afkortingen zijn, met betekenis (i.e. eliminatieregels, geldig voor alle formules α, β, φ)

$$\alpha \wedge \beta \quad \rightsquigarrow \quad \neg(\alpha \to \neg\beta); \tag{4.1}$$
$$\alpha \vee \beta \quad \rightsquigarrow \quad (\neg\alpha) \to \beta; \tag{4.2}$$
$$\exists_x \varphi \quad \rightsquigarrow \quad \neg\forall_x \neg\varphi. \tag{4.3}$$

  Net als bij de propositielogica komen de axioma's in twee groepen: *zuiver logische* en *domeinspecifieke*. We geven de laatste in de volgende twee hoofdstukken voor **PA** en **ZF**. De eerste drie zuiver logische axioma's komen letterlijk uit de propositielogica: voor alle formules $\alpha, \beta, \gamma, \delta$ geldt

  Axioma 1. $\beta \to (\alpha \to \beta)$;

  Axioma 2. $(\beta \to (\gamma \to \delta)) \to ((\beta \to \gamma) \to (\beta \to \delta))$;

  Axioma 3. $(\neg\alpha \to \neg\beta) \to ((\neg\alpha \to \beta) \to \alpha)$.

  Deze worden in de predikaatlogica aangevuld met de volgende vier nieuwe axioma's:

  Axioma 4. $(\forall_x \varphi(x)) \to \varphi(t)$ voor iedere term t die x vrij of niet bevat;[7]

  Axioma 5. $(\forall_x(\varphi \to \psi)) \to (\varphi \to \forall_x \psi)$ als φ de variabele x gebonden of niet bevat;

  Axioma 6. $\forall_x(x = x)$;

  Axioma 7. $\forall_x \forall_y((x = y) \to (\varphi(x) \to \varphi(y)))$ als φ variabele x vrij en y vrij of niet bevat.

  Deze axioma's gelden voor alle formules φ en ψ onder de gegeven beperkingen.

- De deductieregels voor formules φ, ψ zijn (de eerste herken je uit de propositielogica):
  1. *modus ponens*: uit $\varphi \to \psi$ en φ volgt ψ;
  2. *generalisatie*: uit $\varphi(x)$ volgt $\forall_x \varphi(x)$, indien als x als vrije variabele in φ voorkomt.[8]

Deze generalisatie-regel zegt dat als je iets bewijst voor vaste maar willekeurige x, het dan geldt voor alle x. Ook Axioma's 4 t/m 7 liggen redelijk voor de hand (al kan Axioma 6 soms hoon opwekken). Opmerkelijk is echter dat dit stelsel afdoende is om de hele wiskunde te kunnen bedrijven (zie onder).

Het begrip *stelling* is hetzelfde als in de propositielogica: een uitspraak (gedefinieerd als een gesloten formule) is een stelling desda zij met behulp van de deductieregels in eindig veel stappen uit de axioma's kan worden bewezen. Een simpel voorbeeld is $(\forall_x \varphi(x)) \to \varphi(x)$ of kort: $\forall_x \varphi \to \varphi$: deze volgt door in Axioma 4 te kiezen $t \equiv x$. Een ander voorbeeld: voor een willekeurige term t is $t = t$ een stelling. Kies in Axioma 4 nl. $\varphi(x) \equiv (x = x)$, dan heb je $\forall_x(x = x) \to (t = t)$, en pas daarop Axioma 6 en *modus ponens* toe. Je ziet hieruit dat je ook bepaalde open formules kunt bewijzen, zoals $x = x$. Dat is geen stelling (omdat x vrij voorkomt), maar door generalisatie wordt het een stelling. Deze stap geldt algemeen.

Het begrip *waarheid* heeft ook nu weer te maken met de interpretatie van formules in de "werkelijkheid", en is daarmee afhankelijk van de theorie die is geaxiomatiseerd. Er bestaat een algemene theorie over interpretatie en waarheid, genaamd *Modeltheorie*, die we echter aan gevorderde logicacolleges overlaten: we zullen de interpretatie en eventuele waarheid van uitspraken in dit college alleen behandelen voor de theorieën **PA** en **ZF**. De rol van de tautologieën wordt in de predikaatlogica gespeeld door de uitspraken die onder alle mogelijke interpretaties waar zijn. Deze 'altijd ware' uitspraken zijn volgens de *volledigheidsstelling van Gödel* precies de bewijsbare uitspraken (vgl. Stelling 3.3).

Ten slotte geven we aan hoe de propositielogica een speciaal geval van de predikaatlogica is. De propositielogica heeft dan geen variabelen, geen constanten, geen functiesymbolen, en uitsluitend predikaatsymbolen met ariteit 0: deze laatste zijn de atomaire proposities $p_1, p_2, \ldots$. De regels voor termformatie geven in dit geval aan dat er geen termen bestaan. In de formatieregels voor formules is in dat geval stap 2(a) niet mogelijk, en geeft stap 2(b) uitsluitend formules van de vorm p_i. Deze kunnen dan met stap 2(c) worden gecombineerd tot samengestelde formules. De mogelijkheden zijn daarbij precies hetzelfde als in de propositielogica, omdat de symbolen $\exists_x$ en $\forall_x$ niet voorkomen vanwege de afwezigheid van variabelen x. De formules vallen samen met de uitspraken, omdat er geen variabelen zijn.[9]

---

7. Hier betekent $\varphi(t)$ dat in φ de vrije variabele x overal door t wordt vervangen. Dit wordt soms genoteerd als $\varphi(x/t)$.
8. Het (al geleverde) bewijs van φ mag dan geen enkele aanname over de vrije variabele x bevatten.
9. Het is niet mogelijk om de variabelen in de predikaatlogica de rol van elementaire proposities in de propositielogica te laten spelen, omdat je dan formules van de vorm $p_i = p_j$ krijgt. Het symbool = komt in de propositielogica echter niet voor.

Opgave 4.1

Waarom is $\varphi = \varphi$ geen stelling?

Opgave 4.2

Maak een tabel waarin voor de propositielogica (gezien als een speciaal geval van de predikaatlogica), voor **PA**, en voor **ZF** staat wat de symbolen zijn, gesorteerd naar de aangegeven mogelijkheden: zuiver logische symbolen, niet-logische symbolen, constanten, functiesymbolen, predikaatsymbolen. Schrijf daarna per geval op welke regels voor de formatie van termen en formules niet-triviaal zijn. (Voorgedaan op college, maar extreem nuttig om zelf nog eens uit te werken!)

Opgave 4.3

Bewijs dat $\forall_y \forall_x \varphi$ volgt uit $\forall_x \forall_y \varphi$ (m.a.w., neem de laatste aan en deduceer daaruit de eerste).
N.B. Dit rechtvaardigt de afkorting $\forall_{x,y}$ voor $\forall_x \forall_y$; de volgorde maakt immers niet uit.

Opgave 4.4

Geef een formule $\varphi(x)$ in de taal van **PA** met de betekenis: "x is een priemgetal" en formaliseer vervolgens de uitspraak: "er is geen grootste priemgetal" in **PA**.

Opgave 4.5

Geef niet-logische symbolen en domeinspecifieke axioma's voor een *partiële ordening*. Doe dit eerst zonder, en vervolgens met de eis dat er een minimaal element en een maximaal element bestaan (waarbij deze niet identiek zijn). Geef voor twee van je axioma's aan hoe ze volgens bovenstaande formatieregels een uitspraak (i.e. gesloten formule) zijn.

Toelichting: In de gebruikelijke wiskunde is een partiële ordening op een verzameling een relatie $\leq$ die voldoet aan:

a) $x \leq x$ (reflexiviteit);
b) als $x \leq y$ en $y \leq x$, dan volgt $x = y$ (antisymmetrie);
c) als $x \leq y$ en $y \leq z$, dan volgt $x \leq z$ (transitiviteit).

Een (mogelijk) minimaal element, genaamd $\bot$, voldoet aan $\bot \leq x$ voor alle x. Een (mogelijk) maximaal element, genaamd $\top$, voldoet aan $x \leq \top$ voor alle x.
Voorbeelden: de verzameling $\mathbb{Z}$ heeft de voor de hand liggende partiële ordening en heeft geen minimaal en geen maximaal element. De verzameling $\mathbb{N}$ heeft een minimaal element (nul) maar geen maximaal element. De verzameling van getallen 1 t/m n, $n < \infty$, heeft zowel een minimaal als een maximaal element.

5

Peano Aritmetiek

De domeinspecifieke axioma's van de 'rekenkunde' zijn jullie *in woorden* al bekend uit *Getallen*, en zo werden ze historisch ook door Peano geformuleerd. Met behulp van de notatie en begrippen uit het vorige hoofdstuk kan het stelsel **PA** ook als volgt in de taal van eerste-orde logica worden uitgedrukt:

PA1 $\forall_x(\neg(S(x) = \mathbf{0}))$;
PA2 $\forall_x\forall_y(S(x) = S(y) \to x = y)$;
PA3 $\forall_x(x + \mathbf{0} = x)$;
PA4 $\forall_x\forall_y(x + S(y) = S(x + y))$;
PA5 $\forall_x(x \times \mathbf{0} = \mathbf{0})$;
PA6 $\forall_x\forall_y(x \times S(y) = (x \times y) + x)$;
PA7 $(\varphi(0) \wedge (\forall_x(\varphi(x) \to \varphi(S(x)))) \to \forall_x\varphi(x)$, voor alle formules $\varphi(x)$ met vrije variabele (tenminste) x.

Het laatste axioma is het inductie-axioma; het is eigenlijk een zogenaamd *axioma-schema*, omdat het voor willekeurige formules $\varphi(x)$ geldt. In die zin zijn ook alle axioma's uit het vorige hoofdstuk (m.u.v. Axioma 6) axioma-schema's. De axioma's **PA1** t/m **PA6** zijn dan wel echte, individuele axioma's.

Wat is nu het verband tussen de Peano-axioma's in Getallen en de bovenstaande formele versie? Dit verband wordt gegeven door de *semantiek* voor **PA**, waarin deze theorie "in de natuurlijke getallen $\mathbb{N}$ wordt geïnterpreteerd." Dit is wat je onbewust doet als je geen wiskunde hebt gestudeerd (en is ook wat Peano zelf deed)! Het is extreem belangrijk om te beseffen dat *bij iedere vorm van semantiek een syntactische structuur wordt vertaald naar iets wat al als bekend wordt verondersteld*. Dat kan weer een andere gedachtenconstructie zijn (zoals je vaak ziet in de wiskunde), of iets uit "de werkelijkheid".

We kijken eerst naar de logische symbolen $\neg, \wedge, \vee, \to$ en $=$ (we behandelen $\exists$ en $\forall$ zo dadelijk. Deze worden altijd, dus ook in andere eerste-orde theorieën dan **PA**, geïnterpreteerd door respectievelijk "niet", "en", "of", 'impliceert", en "is gelijk aan". Deze begrippen worden dus bekend verondersteld!

Bij de interpretatie van **PA** gaan we er tevens vanuit de de natuurlijke getallen $\mathbb{N} = \{0, 1, 2, \ldots\}$ al bekend zijn, evenals het rekenen ermee. Dit uitgangspunt kan op minstens twee manieren worden opgevat. Ten eerste zullen we $\mathbb{N}$ later construeren binnen de verzamelingenleer **ZF**, dus als je die laatste accepteert heb je volgens die constructie ook $\mathbb{N}$. Dan hang je een relatief eenvoudig begrip als de natuurlijke getallen echter op aan een veel ingewikkeldere theorie. Daarom is het ten tweede mogelijk en acceptabel om aan te nemen dat de natuurlijke getallen simpelweg "bestaan"; veel wiskundigen denken er ook zo over.

Definitie 5.1 *De interpretatie $[[\varphi]]_{\mathbb{N}}$ in de natuurlijke getallen $\mathbb{N}$ van een formule φ in de eerste-orde taal **PA** uit het vorige hoofdstuk houdt in dat binnen φ:*

1. *de logische symbolen $\neg, \wedge, \vee, \to$ en $=$ hun gebruikelijke betekenis hebben, dus $\neg$ betekent "niet", $\wedge$ is "en", $\vee$ is "of", $\to$ betekent "impliceert", en = staat voor "is gelijk aan";*
2. *alle variabelen over de natuurlijke getallen $\mathbb{N}$ lopen (inclusief 0), zodat $\forall_x$ betekent "voor alle $x \in \mathbb{N}$", en $\exists_x$ staat voor "er bestaat een $x \in \mathbb{N}$";*
3. *de constante $\mathbf{0}$ als het getal 0 wordt geïnterpreteerd;*
4. *de functie S wordt geïnterpreteerd als $S(x) = x+1$, en de functies $+$ en $\times$ worden geïnterpreteerd als respectievelijk optelling en vermenigvuldiging van natuurlijke getallen.*

*Een uitspraak φ in de eerste-orde taal van **PA** heet* waar, *notatie $\vDash \varphi$, indien de uitspraak $[[\varphi]]_{\mathbb{N}}$ een ware eigenschap van de natuurlijke getallen uitdrukt.*

Voorbeeld: $[[\forall_x \forall_y (x+y = y+x)]]_{\mathbb{N}}$ betekent dat voor alle natuurlijke getallen $x, y \in \mathbb{N}$ de volgorde waarin zij worden opgeteld niet uitmaakt. Die uitspraak is dus waar, want optelling heeft die eigenschap. Ander voorbeeld: de formele uitspraak $\mathbf{1} + \mathbf{1} = \mathbf{2}$ is een afkorting voor $S(\mathbf{0}) + S(\mathbf{0}) = S(S(\mathbf{0}))$. De interpretatie $[[\mathbf{1}+\mathbf{1} = \mathbf{2}]]_{\mathbb{N}}$ is dus $1+1 = 2$. Dat is zo, zodat de uitspraak $\mathbf{1}+\mathbf{1} = \mathbf{2}$ waar is. De uitspraak $\forall_y \exists_x (x+\mathbf{2} = y)$ is daarentegen niet waar, omdat voor $y = 0$ of $y = 1$ geen $x \in \mathbb{N}$ bestaat die voldoet aan $x + 2 = y$.

We nemen hierbij stilzwijgend aan dat uitspraken over $\mathbb{N}$ waar zijn of niet, i.e., de natuurlijke getallen hebben een bepaalde eigenschap of ze hebben die niet.[1] In het verlengde daarvan nemen we aan dat $\mathbb{N}$ *consistent* is: een uitspraak over natuurlijke getallen kan niet tegelijk waar en onwaar zijn.[2]

Na dit uitstapje naar de semantiek van **PA** komen we nu terug op haar syntax. Als je de axioma's **PA1** t/m **PA7** volgens Definitie 5.1 interpreteert krijg je de gebruikelijke, informele Peano-axioma's uit Getallen (ga na). Een *stelling* van **PA** is een uitspraak φ die in eindig veel stappen uit deze axioma's en de algemene axioma's en deductieregels uit het vorige hoofdstuk kan worden bewezen, notatie: $\vdash \varphi$. Het begrip stelling heeft net als in de propositielogica *a priori* dus niets met de interpretatie te maken. We zouden vanwege het imago van de wiskunde echter wel graag zien dat alle stellingen waar zijn in de zin van Definitie 5.1. Daarvoor is het, net als in de propositielogica, noodzakelijk en voldoende dat:

1. alle axioma's waar zijn;
2. de deductieregels waarheid behouden.

Dat laatste is het geval voor de *modus ponens*, die het normale gebruik van een implicatie in de wiskunde (en zelfs daarbuiten) beschrijft: als een uitspraak φ waar is en tevens waar is dat deze uitspraak een andere uitspraak ψ impliceert, dan is ook ψ waar. Ook de generalisatieregel behoudt waarheid: als een uitspraak waar is voor een vast maar willekeurig getal, dan is zij waar voor ieder getal.

Met de waarheid van de axioma's ligt het iets gecompliceerder. We hebben eerder gezegd dat de natuurlijke getallen $\mathbb{N}$ en de operaties optelling en vermenigvuldiging bekend moeten worden verondersteld om überhaupt iets als Definitie 5.1 op te kunnen schrijven. Als $\mathbb{N}$ en de functies S, $+$, en $\times$ binnen **ZF** wordt gedefinieerd, dan zijn **PA1** t/m **PA7** inderdaad waar in de technische zin van Definitie 5.1 (zie later). Bij andere constructies van $\mathbb{N}$, en al helemaal als de natuurlijke gevallen eenvoudigweg aan de werkelijkheid worden ontleend (of aan God, zoals de bekende 19e eeuwse wiskundige Leopold Kronecker dacht), is de geldigheid van de Peano-axiom's eerder op te vatten als een *eis* op $\mathbb{N}$. Deze opmerking is met name relevant voor een goed begrip van het inductie-axioma **PA7**. Je kunt moeilijk volhouden dat dit een voor de hand liggende eigenschap van $\mathbb{N}$ is die uit het 'bestaan' van natuurlijke getallen zou volgen. Het kent deze 'bestaande' getallen eerder een extra eigenschap toe en zou bovendien beter als deductieregel binnen **PA** kunnen worden opgevat (maar aan de andere kant willen we graag dat de deductieregels algemene logische geldigheid hebben en niet specifiek zijn voor een bepaalde theorie).

Hoe dan ook: we mogen net als bij de propositielogica concluderen dat een stelling (i.e. een bewijsbare uitspraak) in **PA** waar is. Dit is in de praktijk ook precies de manier waarop je er achter kunt komen of een uitspraak over natuurlijke getallen waar is: je bewijst hem gewoon! Maar al mag je bij het formele bewijzen gerust je intuïtie over getallen gebruiken, uiteindelijk is je bewijs pas zeker als je *op papier* uitsluitend vanuit de axioma's en de deductieregels hebt gewerkt en een computer kan controleren dat je geen fouten hebt gemaakt.

Net als in de propositielogica en in de algemene predikaatlogica zijn we ook hier weer het principiële verschil tussen waarheid (als semantisch begrip) en bewijsbaarheid (als syntactisch begrip). Desondanks ligt het voor de hand om te denken dat de klasse van ware uitspraken (over natuurlijke getallen) samenvalt met de klasse van bewijsbare uitspraken; dat is wat het wiskundige genie Hilbert (en iedereen vóór hem) ook dacht. Kurt Gödel bewees echter in zijn beroemde (eerste) onvolledigheidsstelling dat **PA** (en ook **ZF**) ware maar niet bewijsbare uitspraken kent. We gaan later uitvoerig op dit verrassende punt in.

Het formele bewijzen met de beperkte kennis van nu is erg lastig. Je mag daarom de volgende (meta)stellingen ui de eerste-orde logica gebruiken, die met enige moeite volgen uit de axioma's en deductieregels uit hoofdstuk 4 (en die je zonder er bij stil te staan voortdurend op informeel niveau gebruikt):

1. Hierover is een lange filosofische discussie mogelijk; volgens de meeste wiskundigen volgt dit uit het bestaan van de natuurlijke getallen, wat dit ook moge betekenen.
2. Veel wiskundigen menen dat ook dit volgt uit het bestaan van $\mathbb{N}$.

Steling 1: Uit $\vdash t_1 = t_2$ volgt $\vdash t_2 = t_1$ (voor alle termen t_1, t_2).

Steling 2: uit $\vdash t_1 = t_2$ en $\vdash t_2 = t_3$ volgt $\vdash t_1 = t_3$ (voor alle termen t_1, t_2, t_3).

Stelling 3: Als t_1 en t_2 termen zijn, en f is een functiesymbool van ariteit $a(f) = 1$, dan geldt de stelling:

$$\vdash (t_1 = t_2) \to (f(t_1) = f(t_2)). \tag{5.1}$$

Voor hogere ariteiten geldt iets soortgelijks, bijv. als $a(f) = 2$, dan geldt voor alle termen s_1, s_2, t_1, t_2

$$\vdash (s_1 = t_1) \to ((s_2 = t_2) \to (f(s_1, s_2) = f(t_1, t_2))). \tag{5.2}$$

Voor **PA** geeft dit:

- uit $\vdash t_1 = t_2$ volgt $\vdash S(t_1) = S(t_2)$;
- uit $\vdash s_1 = t_1$ en $\vdash s_2 = t_2$ volgt $\vdash s_1 + s_2 = t_1 + t_2$ alsook $\vdash s_1 \times s_2 = t_1 \times t_2$.

Stelling 4 (conjunctiestelling): Uit $\vdash \varphi$ en $\vdash \psi$ volgt $\vdash \varphi \wedge \psi$.

Stelling 5 (deductiestelling): Als ψ kan worden afgeleid uit een aanname φ, dan geldt $\vdash \varphi \to \psi$.
Let op! De formule φ hoeft hierbij zelf geen stelling te zijn! Bij het gebruik van de deductiestelling in een bewijs mogen de bovenstaande stellingen ook op aannamen worden toegepast (bijvoorbeeld: uit de *aanname* $t_1 = t_2$ volgt $t_2 = t_1$).[3]

Uit de deductiestelling en Axioma 3 van de eerste-orde logica volgt

Steling 6 (bewijs uit het ongerijmde): als je uit $\neg\alpha$ zowel β als $\neg\beta$ af kunt leiden, dan volgt $\vdash \alpha$.

Als illustratie tonen we, met de notatie $\mathbf{n} = S(^{n\,\text{keer}}\cdots S(\mathbf{0})\,^{n\,\text{keer}}\cdots)$, aan dat $\mathbf{1} + \mathbf{1} = \mathbf{2}$, oftewel

$$\vdash S(\mathbf{0}) + S(\mathbf{0}) = S(S(\mathbf{0})). \tag{5.3}$$

Bewijs.

1. **PA4** met de substitutie $x \rightsquigarrow S(\mathbf{0})$ geeft[4]

$$\vdash \forall_y(S(\mathbf{0}) + S(y) = S(S(\mathbf{0}) + y)). \tag{5.4}$$

2. Vgl. (5.4) met de substitutie $y \rightsquigarrow \mathbf{0}$ geeft[5]

$$\vdash S(\mathbf{0}) + S(\mathbf{0}) = S(S(\mathbf{0}) + \mathbf{0}). \tag{5.5}$$

3. **PA3** met de substitutie $x \rightsquigarrow S(\mathbf{0})$ geeft[6]

$$\vdash S(\mathbf{0}) + \mathbf{0} = S(\mathbf{0}). \tag{5.6}$$

4. Stelling 3 boven (eerste •) toegepast op (5.6), dus met $t_1 \rightsquigarrow S(\mathbf{0}) + \mathbf{0}$ en $t_2 \rightsquigarrow S(\mathbf{0})$, geeft

$$\vdash S(S(\mathbf{0}) + \mathbf{0}) = S(S(\mathbf{0})). \tag{5.7}$$

5. Stelling 2 boven toegepast op (5.5) en (5.7) geven ten slotte (5.3). Q.E.D.

We kunnen niet vaak genoeg zeggen dat je bij deze puur formele bewijstechniek nergens gebruikt dat $\mathbf{0}$ het getal nul is, de variabelen x en y in de bovenstaande axioma's natuurlijke getallen zijn, het functiesymbool $+$ iets te maken heeft met het optellen van getallen van de lagere school, de logische symbolen $\neg$ etc. iets te maken hebben met de begrippen "niet", etc. We hebben dus formeel bewezen dat $\mathbf{1}+\mathbf{1} = \mathbf{2}$, maar niet *in de normale betekenis van deze symbolen*. We hebben echter gezien dat stellingen van **PA** waar zijn, zodat $\mathbf{1} + \mathbf{1} = \mathbf{2}$ na interpretatie van **PA** in $\mathbb{N}$ volgens Definitie 5.1 impliceert dat $1 + 1 = 2$. Je kunt dus nu thuis gaan uitleggen dat je dat na ruim een half jaar wiskundestudie kunt bewijzen, haha.

---

3. Als je ψ afleidt uit aannamen φ_1 t/m φ_n (en de relevante axioma's en deductieregels) wordt dat vaak genoteerd als $\varphi_1, \ldots, \varphi_n \vdash \psi$. Er geldt dus bijvoorbeeld $(t_1 = t_2) \vdash (t_2 = t_1)$.
4. Deze substitutie is toegestaan dankzij Axioma 4 met $\varphi(x) \rightsquigarrow \forall_y(x + S(y) = S(x + y))$ en $t \rightsquigarrow S(\mathbf{0})$.
5. Dit mag wegens Axioma 4 met $x \rightsquigarrow y$, $\varphi(y) \rightsquigarrow S(\mathbf{0}) + S(y) = S(S(\mathbf{0}) + y)$, en $t \rightsquigarrow \mathbf{0}$.
6. Gebruik axioma 4 met $\varphi(x) \rightsquigarrow (x + \mathbf{0} = x)$, $t \rightsquigarrow S(\mathbf{0})$.

Een voorbeeld van het gebruik van **PA7** is het bewijs van

$$\vdash \forall_x(\mathbf{0} + x = x), \tag{5.8}$$

dat overigens de Om (5.10) te bewijzen nemen we in **PA7** de formule $\varphi(x) \equiv (\mathbf{0} + x = x)$. We bewijzen dan eerst $\vdash \varphi(\mathbf{0})$ en vervolgens $\vdash (\forall_x(\varphi(x) \to \varphi(S(x)))$. De conjunctiestelling boven en de *modus ponens* geven dan de gewenste conclusie $\vdash \forall_x\varphi(x)$. De eerste stelling $\vdash \mathbf{0} + \mathbf{0} = \mathbf{0}$ volgt uit **PA3** met $x \rightsquigarrow \mathbf{0}$.

Opgave 5.1

Toon aan dat voor iedere term t in **PA** geldt: $\vdash t + S(\mathbf{0}) = S(t)$.

Opgave 5.2

Bewijs dat $\vdash \mathbf{1} \times \mathbf{1} = \mathbf{1}$.

Opgave 5.3

De eerste stap op weg is naar het bewijs van de commutativiteit van optelling, i.e.,

$$\vdash \forall_x\forall_y(x + y = y + x), \tag{5.9}$$

is

$$\vdash \forall_x(\mathbf{0} + x = x). \tag{5.10}$$

Bewijs (5.10) met behulp van **PA7**. *Hint:* Bewijs eerst $\vdash \varphi(\mathbf{0})$. Laat dan zien dat $\varphi(S(x))$ volgt uit de aanname $\varphi(x)$. De deductiestelling geeft dan $\vdash \varphi(x) \to \varphi(S(x))$ en generalisatie geeft $\vdash (\forall_x(\varphi(x) \to \varphi(S(x)))$. Gebruik ten slotte de conjunctiestelling en *modus ponens*.

Opgave 5.4

Bekijk de volgende vreemde interpretatie van de taal van **PA**. We volgen Definitie 5.1 met uitzondering van punt 2: we laten de variabelen nu lopen over $\mathbb{Q}^+$ (i.e. de positieve rationale getallen inclusief nul), zodat $\forall_x$ betekent "voor alle $x \in \mathbb{Q}^+$", en $\exists_x$ staat voor "er bestaat $x \in \mathbb{Q}^+$". *Welke van de axioma's **PA1–PA7** zijn in deze interpretatie waar en waarom?*

6

Zermelo–Fraenkel axioma's

De moderne wiskunde berust op het volgende stelsel van axioma's, dat in de periode 1900–1925 werd opgesteld.[1] Deze axioma's (met de deductieregels van de eerste-orde logica) bepalen dus wat een correct wiskundig bewijs is. Gek genoeg zouden weinig professionele wiskundigen in staat zijn ze op te dreunen en in veel wiskundeopleidingen worden ze pas in de master of nooit behandeld. De reden daarvoor is dat niet al deze axioma's ook echt worden gebruikt in de alledaagse wiskunde (zoals de meeste delen van de Algebra, Analyse, Meetkunde, en Stochastiek). In de praktijk gaat het vooral om **ZF1** t/m **ZF7** en soms om **AC**. Zelfs dan worden wiskundigen zo getraind dat ze de bewijzen automatisch goed doen zonder de precieze rechtvaardiging vanuit **ZF** te kennen. Toch is het goed om **ZF** al in je eerste jaar een keer gezien te hebben en om indruk op vriendjes of vriendinnetjes te maken (of als je je daarbij verveelt) zou je ze boven je bed kunnen hangen. We gebruiken de volgende afkortingen:

$$\forall_{x,y} \equiv \forall_x \forall_y; \tag{6.1}$$
$$\alpha \leftrightarrow \beta \equiv (\alpha \to \beta) \wedge (\beta \to \alpha); \tag{6.2}$$
$$x \neq y \equiv \neg(x = y); \tag{6.3}$$
$$x \notin y \equiv \neg(x \in y). \tag{6.4}$$

Andere notaties worden in de toelichting na de axioma's uitgelegd. **ZF2** en **ZF8** (die φ bevatten) zijn axioma-schema's (vgl. **PA7**). Deze gelden voor alle formules φ met de aangegeven vrije variabelen.

ZF1 $\forall_{x,y}\,((\forall_z(z \in x \leftrightarrow z \in y)) \leftrightarrow x = y)$ (*Extensionaliteitsaxioma*);

ZF2 $\forall_x \exists_y \forall_z(((z \in x) \wedge \varphi(z)) \leftrightarrow z \in y)$ (*Scheidingssaxioma*);

ZF3 $\neg\exists_x x \in \emptyset$ (*Axioma van de lege verzameling*);

ZF4 $\forall_{v,w} \exists_y \forall_z(z \in y \leftrightarrow (z = v) \vee (z = w))$ (*Paringsaxioma*);

ZF5 $\forall_x \exists_y \forall_z(z \in y \leftrightarrow \exists_{w \in x} z \in w)$ (*Verenigingsaxioma*);

ZF6 $\forall_x \exists_y \forall_z(z \in y \leftrightarrow z \subset x)$ (*Machtsverzamelingsaxioma*);

ZF7 $\exists_x(\emptyset \in x \wedge \forall_y(y \in x \to y^+ \in x))$ (*Oneindigheidsaxioma*);

ZF8 $\forall_u((\forall_{x \in u} \exists!_z \varphi(x,z)) \to \exists_y \forall_z(z \in y \leftrightarrow \exists_{x \in u} \varphi(x,z)))$ (*Substitutieaxioma*);

ZF9 $\forall_{v \neq \emptyset}\, \exists_{x \in v}\, \forall_y(y \in x \to y \notin v)$ (*Regulariteitsaxioma*);

AC $\forall_u \exists_w((w \subset P(u) \times u) \wedge (\forall_{x \in P(u)}(x \neq \emptyset \to \exists!_{y \in x} < x, y > \in w)))$ (*Keuzeaxioma*).

Schrik niet! De eerste zeven axioma's zijn makkelijk(er) te begrijpen als we alvast aan echte verzamelingen denken (officieel vormen die pas de semantiek van deze theorie, die nu nog in een formeel syntactisch stadium verkeert).[2] De laatste vier zijn een stuk technischer. De axioma's vallen inhoudelijk in twee andere groepen uiteen. De eerste groep geeft informatie over *gegeven* verzamelingen. Deze groep bestaat uit **ZF1**, dat zegt dat een verzameling wordt bepaald door haar elementen, **ZF3**, dat zegt dat de constante $\emptyset$ de lege verzameling is, en **ZF9** en **AC**, die zeer technisch zijn. De tweede groep (dus **ZF2**, **ZF4**, **ZF5**, **ZF6**, **ZF7**, en **ZF8**) bestaat uit axioma's die *nieuwe* verzamelingen genereren uit bestaande.

---

1. Dit stelsel heet **ZFC**. Axioma's **ZF1** t/m **ZF7** werden in 1908 door Zermelo geformuleerd. Axioma **ZF8** werd in 1922 onafhankelijk door Abraham Fraenkel (1891–1965) en Thoralf Skolem (1887–1963) voorgesteld. Axioma **ZF9** is van von Neumann (1925). Axioma **AC** komt weer van Zermelo (1904), maar was Russell en anderen al eerder opgevallen. Het stelsel **ZF1** t/m **ZF9** heet **ZF**. Zie ook D. van Dalen, H.C. Doets, en H.C.M. de Swart, *Verzamelingen: naïef, axiomatisch en toegepast* (Utrecht, 1975).
2. Maar let op: vanwege de moderne axiomatische aanpak hoeven we niet te definiëren wat een verzameling is (zoals Frege en Cantor wanhopig probeerden, en zoals Euclides al even weinig overtuigend definieerde wat een punt is, enz.).

ZF1: $\forall_{x,y}\,((\forall_z(z \in x \leftrightarrow z \in y)) \leftrightarrow x = y)$ zegt dat als het voor twee verzamelingen x en y zo is dat z in x ligt desda z in y ligt, dan geldt $x = y$. Een verzameling is dus bepaald door haar elementen (die zelf ook weer verzamelingen moeten zijn, want in de wiskunde volgens **ZF** is er niets anders!).

ZF2: $\forall_x\exists_y\forall_z(((z \in x) \wedge \varphi(z)) \leftrightarrow z \in y)$ is een correcte versie van het naïeve idee van Cantor, Dedekind, en Frege dat iedere eigenschap (of technischer: ieder predikaat) een verzameling definieert. Als we een predikaat zien als een formule $\phi(z)$, die uitdrukt dat z een bepaalde eigenschap heeft, dan zou $y = \{z \mid \varphi(z)\}$ dus een verzameling moeten zijn. In het soort notatie van **ZF2** zou dit idee worden uitgedrukt door het axioma $\exists_y\forall_z(\varphi(z) \leftrightarrow z \in y)$, maar dit leidt tot de Paradox van Russell (kies $\varphi(z) \equiv z \notin z$). Het cruciale verschil tussen **ZF2** en deze naïeve versie is dat we ons nu beperken tot alle z die voldoen aan $\varphi(z)$ *én element zijn van een al gegeven verzameling* x. De verzameling y die in dit axioma wordt gedefinieerd is volgens **ZF1** uniek en wordt genoteerd als

$$y \equiv \{z \in x \mid \varphi(z)\}. \tag{6.5}$$

Let op! Dit is de eerste keer dat de bekende verzamelingstheoretische haakjes $\{\cdots\}$ officieel worden ingevoerd, en wel als onderdeel van een notatie die afkort wat er in axioma **ZF2** gebeurt. Deze haakjes behoren dus niet bij de formele taal **ZF**: ze spelen een totaal andere rol dan de ronde haakjes $(,)$ en vallen evenmin onder enige klasse van symbolen die in hoofdstuk 4 zijn ingevoerd. Voorbeeld: voor willekeurige verzamelingen x en v (preciezer gezegd: variabelen in de logische taal van **ZF**) is $x \cap v$ een afkorting voor de verzameling y die in axioma **ZF2** wordt gedefinieerd door voor $\varphi(z)$ de formule $z \in v$ te nemen. Met de notatie (6.5) geeft dit als *definitie* van het symbool $\cap$ voor de doorsnede dus

$$x \cap v \equiv \{z \in x \mid z \in v\}. \tag{6.6}$$

ZF3: $\neg\exists_x x \in \emptyset$ zegt dat $\emptyset$, de enige constante in de formele taal van **ZF**, geen elementen heeft en dat er dus een lege verzameling bestaat. Volgens **ZF1** is deze verzameling uniek, vandaar dat $\emptyset$ dé lege verzameling is.[3] Het volgt dus uit axioma **ZF3** dat er überhaupt een verzameling bestaat![4]

ZF4: $\forall_{v,w}\exists_y\forall_z(z \in y \leftrightarrow (z = v) \vee (z = w))$ zegt dat er voor gegeven verzamelingen v en w een verzameling y met precies deze twee elementen bestaat, die we verder aanduiden als $y = \{v, w\}$. Dit is de tweede keer dat de haakjes $\{\cdots\}$ worden gedefinieerd, consistent met de eerste keer: neem in **ZF2** namelijk $\varphi(z)$ als $(z = v) \vee (z = w)$ en x als de verzameling y die volgens **ZF4** bestaat.[5]
Dit proces kan worden herhaald, zodat we $\{x_1, \ldots, x_n\}$ kunnen schrijven voor de verzameling y die voldoet aan $\forall_{x_1,\ldots,x_n}\exists_y\forall_z(z \in y \leftrightarrow (z = x_1) \vee \cdots \vee (z = x_n))$. Deze y is wegens **ZF1** uniek: haar elementen zijn zojuist vermeld. Met andere woorden, in de notatie van **ZF2** kunnen we schrijven

$$\{x_1, \ldots, x_n\} \equiv \{z \in y \mid (z = x_1) \vee \cdots \vee (z = x_n)\}, \tag{6.7}$$

waarbij y de verzameling is die volgens axioma **ZF4** bestaat (en gelijk is aan $\{x_1, \ldots, x_n\}$).

ZF5: $\forall_x\exists_y\forall_z(z \in y \leftrightarrow \exists_{w\in x} z \in w)$ postuleert het bestaan van een verzameling y met als elementen precies *de elementen van de elementen van* x. In de formulering van het axioma staat de afkorting

$$\exists_{w\in x}\psi \equiv \exists_w((w \in x) \wedge \psi), \tag{6.8}$$

voor een willekeurige formule ψ, waarvoor wij in **ZF5** dus nemen $\psi \equiv z \in w$. We schrijven $y = \cup x$, en dit is de *definitie* van het symbool $\cup$ (dat je al informeel kent en gebruikt als het verenigingssymbool voor verzamelingen). Je kunt dus ook noteren

$$\cup x \equiv \{z \in y \mid \exists_{w\in x} z \in w\}, \tag{6.9}$$

waar y de verzameling is waarvan axioma **ZF5** het bestaan garandeert (en die gelijk is aan $\cup x$). In het speciale geval $x = \{x_1, \ldots, x_n\}$ noteren we

$$x_1 \cup \cdots \cup x_n \equiv \cup\{x_1, \ldots, x_n\}. \tag{6.10}$$

Stel bijvoorbeeld dat $x_1 = \{x_3, x_4\}$ en $x_2 = \{x_5\}$, dan is $x_1 \cup x_2 = \{x_3, x_4, x_5\}$ ($\neq \{x_1, x_2\}$!).

---

3. Je kunt het symbool $\emptyset$ hier definiëren als afkorting, i.p.v. het eerst als constante in de logische taal van **ZF** op te nemen.
4. Een equivalente vorm van axioma **ZF3** is: $\forall_x\neg(x \in \emptyset)$, ook genoteerd als $\forall_x x \notin \emptyset$. Gegeven **ZF1** en **ZF2** kun je tevens **ZF3** vervangen door het schijnbaar zwakkere axioma dat er een verzameling x bestaat; met deze x in **ZF2** en $\varphi(z) \equiv (z \neq z)$ (waarbij $s \neq t$ een afkorting is voor $\neg(s = t)$) is $y = \{z \in x \mid z \neq z\}$ de lege verzameling $\emptyset$.
5. **ZF4** volgt niet uit **ZF2**, omdat het niet *a priori* duidelijk is wat je in dat laatste axioma voor x mag kiezen.

ZF6: $\forall_x \exists_y \forall_z (z \in y \leftrightarrow z \subset x)$ eist dat iedere verzameling x een machtsverzameling y heeft. De notatie

$$z \subset x \equiv \forall_y (y \in z \rightarrow y \in x), \tag{6.11}$$

voert het symbool $\subset$ voor "deelverzameling" in.[6] De verzameling y is volgens **ZF1** weer uniek en wordt genoteerd als $P(x)$; de elementen van de machtsverzameling $P(x)$ zijn dus de deelverzamelingen z van x. We kunnen dit ook in de vorm van (6.5) schrijven als

$$P(x) \equiv \{z \in y \mid z \subset x\}, \tag{6.12}$$

waarbij y de verzameling is die volgens **ZF6** bestaat (en samenvalt met $P(y)$).

ZF7: $\exists_x (\emptyset \in x \wedge \forall_y (y \in x \rightarrow y^+ \in x))$ postuleert het bestaan van een verzameling met de elementen

$$\emptyset, \emptyset^+ = \{\emptyset\}, \{\emptyset\}^+ = \{\emptyset, \{\emptyset\}\}, \{\emptyset, \{\emptyset\}\}^+ = \{\emptyset, \{\emptyset\}, \{\emptyset, \{\emptyset\}\}\}, \ldots \tag{6.13}$$

Hierbij is de notatie

$$y^+ \equiv \bigcup \{y, \{y\}\} = y \cup \{y\}, \tag{6.14}$$

uiteindelijk gedefinieerd via **ZF5**. De elementen van y^+ zijn dus de elementen van y, aangevuld met het ene element y. Met von Neumann noemen we de verzamelingen in (6.13) respectievelijk $\dot{0}, \dot{1}, \dot{2}, \dot{3}, \ldots$. Hier wordt $\dot{0}$ dus geïdentificeerd met de lege verzameling, en $n > 0$ met een verzameling van n zorgvuldig uitgekozen elementen. Axioma **ZF7** zegt dan dat er een verzameling is die de elementen $\dot{0}, \dot{1}, \dot{2}, \dot{3}, \ldots$ bevat. De doorsnede van alle verzamelingen met deze eigenschap is de kleinste verzameling die $\dot{0}, \dot{1}, \dot{2}, \dot{3}, \ldots$ bevat; deze kleinste oneindige verzameling heet ω. In de gebruikelijke semantiek van de verzamelingenleer is ω een kopie van de natuurlijke getallen $\mathbb{N}$.

ZF8: $\forall_u ((\forall_{x \in u} \exists!_z \varphi(x,z)) \rightarrow \exists_y \forall_z (z \in y \leftrightarrow \exists_{x \in u} \varphi(x,z)))$, waarin φ niet van y af mag hangen, eist dat als een formule $\varphi(x,z)$ precies één z aan een gegeven x toekent zolang x door een verzameling u loopt, dan al deze z een verzameling vormen. Je kunt zo'n formule φ als een soort functie f beschouwen die aan het "origineel" x het "beeld" z toekent. De term rechts in **ZF8** zegt dat er een verzameling $y \equiv f(u)$ is die bestaat uit alle z die het beeld zijn van een of andere x in u. Dit axioma postuleert dus ruw gezegd dat het beeld van een verzameling onder een functie weer een verzameling is. In de notatie (6.5) hebben we dan

$$f(u) = \{z \in y \mid \exists_{x \in u} \varphi(x,z)\}, \tag{6.15}$$

waarbij y bestaat volgens **ZF8** en natuurlijk hetzelfde is als $f(u)$.

ZF9: $\forall_{v \neq \emptyset} \exists_{x \in v} \forall_y (y \in x \rightarrow y \notin v)$ zegt dat iedere niet-lege verzameling v een element x bevat dat disjunct is met x. Hierbij is de generieke afkorting

$$\forall_{v \neq \emptyset} \psi \equiv \forall_v ((\exists_z z \in v) \rightarrow \psi) \tag{6.16}$$

gebruikt. Met het doorsnedesymbool $\cap$ uit(6.6) kun je gemakkelijk nagaan dat de uitdrukking $\forall_y (y \in x \rightarrow y \notin v)$ niets anders betekent dan $x \cap v = \emptyset$. Het axioma luidt dan: $\forall_{v \neq \emptyset} \exists_{x \in v} (x \cap v = \emptyset)$. Dit impliceert $x \notin x$ voor alle x, en bovendien dat er geen oneindig dalende ketens van elementen $\cdots \in x_n \in x_{n-1} \in \cdots \in x_0$ bestaan (we laten het bewijs weg). Dit sluit niet alleen allerlei paradoxen uit, maar maakt tevens een krachtige ('transfiniete') vorm van inductie mogelijk.

AC: $\forall_u \exists_w ((w \subset P(u) \times u) \wedge (\forall_{x \in P(u)} (x \neq \emptyset \rightarrow \exists!_{y \in x} < x, y > \in w)))$ stelt dat je aan iedere niet-lege deelverzameling van een verzameling een element van die deelverzameling toe kunt kennen. Schrijf de uitdrukking $\exists!_{y \in x} (x,y) \in w$ in **AC** namelijk als $\exists!_{y \in u} ((x,y) \in w \wedge y \in x)$. Dan luidt **AC**:

$$\forall_u \exists_w ((w \subset P(u) \times u) \wedge (\forall_{x \in P(u)} (x \neq \emptyset \rightarrow \exists!_{y \in u} (x,y) \in w \wedge y \in x))). \tag{6.17}$$

In het volgende hoofdstuk zal blijken dat hieruit volgt dat er een functie $f : P(u) \longrightarrow u$ bestaat in de normale zin, die $x \in P(u)$ dus afbeeldt op $f(x) \in u$, zodanig dat $\forall_{x \in P(u)} (x \neq \emptyset \rightarrow f(x) \in x)$. *Informeel* mag je **AC** daarom schrijven als

$$\forall_u \exists_{f : P(u) \longrightarrow u} \forall_{x \in P(u), x \neq \emptyset} f(x) \in x),$$

maar $\exists_f$ is niet gedefinieerd in de eerste-orde taal van **ZF**, omdat je $\exists$ (en $\forall$) alleen aan variabelen mag koppelen, en niet aan deelverzamelingen (in hogere-orde logica kan dat wel).

6. Het is dus mogelijk dat $z = x$, zodat $\subset$ vaak als $\subseteq$ wordt geschreven.

Opgave 6.1

Bewijs dat $u \cap v = v \cap u$ (preciezer: $\vdash \forall_u \forall_v (u \cap v = v \cap u)$).

Opgave 6.2

Bewijs dat $u \cup v = v \cup u$.

Opgave 6.3

Bewijs dat $\vdash (u \subset v) \wedge (v \subset u) \leftrightarrow u = v$.

7

Cartesisch product en functies

Met de **ZF**- axioma's achter de kiezen kunnen we nu het raadselachtige feit ophelderen dat de halve wiskunde op het begrip functie berust, terwijl dat in de taal van **ZF** niet voorkomt (deze heeft namelijk geen functiesymbolen, i.t.t. **PA**). Hiertoe moeten we eerst het Cartesisch product officieel invoeren.

Lemma 7.1 *In **ZF** geldt:*

$$\vdash \forall_{u,v}\forall_{x,y}\left((x \in u) \wedge (y \in v)\right) \rightarrow \{\{x\},\{x,y\}\} \in P(P(u \cup v)). \tag{7.1}$$

*Met andere woorden, stel u en v zijn twee verzamelingen (i.e., variabelen in **ZF**), dan geldt: als $x \in u$ en $y \in v$, dan is $\{\{x\},\{x,y\}\}$ een element van de dubbele machtsverzameling $P(P(u \cup v))$.*

Het *bewijs* gaat in de volgende stappen, die (zeer nuttige) opgaven zijn, vgl. **ZF4**, **ZF5**, en **ZF6**.

1. $\vdash \forall_{u,v}\forall_x\left((x \in u) \rightarrow (x \in u \cup v)\right)$ en (uiteraard) idem dito voor y, of in woorden: als $x \in u$ en $y \in v$, dan geldt $x \in u \cup v$ en $y \in u \cup v$.
2. $\vdash \forall_w\forall_x\left((x \in w) \rightarrow (\{x\} \in P(w))\right)$ en $\vdash \forall_w\forall_{x,y}\left((x \in w \wedge y \in w) \rightarrow (\{x,y\} \in P(w))\right)$. In woorden: Als $x \in w$ en $y \in w$ dan geldt $\{x\} \in P(w)$ en $\{x,y\} \in P(w)$.

Neem nu in deel 2 van dit lemma $w \rightsquigarrow u \cup v$, dan volgt: als $x \in u \cup v$ en $y \in u \cup v$ dan geldt $\{x\} \in P(u \cup v)$ en $\{x,y\} \in P(u \cup v)$. Gebruik nu opnieuw deel 2 van het lemma, maar deze keer met de substituties $w \rightsquigarrow P(u \cup v)$, $x \rightsquigarrow \{x\}$ en $y \rightsquigarrow \{x,y\}$. Dat geeft Lemma 7.1. Q.E.D.

We gebruiken voortaan de afkorting

$$< x,y > \equiv \{\{x\},\{x,y\}\}, \tag{7.2}$$

hetgeen volgens Lemma 7.1 een element van $P(P(u \cup v))$ is (aangenomen dat $x \in u$ en $y \in v$). Dit hele gedoe is bedoeld om van $< x,y >$ een *geordend* paar te maken, i.t.t. $\{x,y\}$, dat hetzelfde is als $\{y,x\}$.

Definitie 7.1 *Het* cartesisch product *van twee verzamelingen u en v is de verzameling*

$$u \times v \equiv \{z \in P(P(u \cup v)) \mid \exists_{x \in u}\exists_{y \in v}\, z =< x,y >\}, \tag{7.3}$$

*m.a.w., we kiezen in **ZF2**: $x \rightsquigarrow P(P(u \cup v))$ en $\varphi(z) \rightsquigarrow \exists_{x \in u}\exists_{y \in v}\, z =< x,y >$ en noteren de unieke verzameling y die zo is gedefinieerd als $u \times v$. Informeel schrijven we vaak*

$$u \times v = \{< x,y > \mid x \in u, y \in v\}. \tag{7.4}$$

Het Cartesisch product komt vaak in de wiskunde voor, maar de belangrijkste toepassing is de volgende.

Definitie 7.2 *Een* functie $f : u \longrightarrow v$ *is een deelverzameling $G_f \subset u \times v$ waarvoor de volgende eis geldt:*

$$\forall_{x \in u}\exists!_{y \in v} < x,y > \in G_f. \tag{7.5}$$

Hier is volgende afkorting gebruikt, (vgl. (6.8)), die via de substitutie $\psi(y) \rightsquigarrow < x,y > \in G_f$ (7.5) geeft:

$$\exists!_{y \in v}\psi(y) \equiv \exists_y((y \in v) \wedge (\forall_z(\psi(z) \leftrightarrow z = y))). \tag{7.6}$$

Algemener schrijven we voor de formule "er is een *unieke* y met de eigenschap $\psi(y)$" het volgende:

$$\exists!_y\psi(y) \equiv \exists_y\forall_z(\psi(z) \leftrightarrow z = y). \tag{7.7}$$

In deze opzet wordt een functie f dus geïdentificeerd met haar grafiek G_f, en daarmee is de historische cirkel rond. In de 17e eeuw dacht Newton niet aan onze functies maar aan hun grafieken (die hij meestal weer als de beweging van een deeltje interpreteerde). Sinds Euler waren we gewend te beginnen met de toekenning van een functiewaarde $f(x) \in v$ aan $x \in u$, om vervolgens over te gaan tot de grafiek

$$G_f = \{< x, f(x) >\} \subset u \times v. \tag{7.8}$$

Nu, in **ZF**, beginnen we met G_f en noemen we de unieke y in (7.5) desgewenst $f(x)$; daarmee zijn we weer terug bij Newton!

Opgave 7.1

Bewijs de twee tussenstappen 1. en 2. in het bewijs van Lemma 7.1.

Opgave 7.2

Kies de formule $\varphi(x, z)$ in axioma **ZF8**, dus

$$\forall_u((\forall_{x\in u}\exists!_z\varphi(x, z)) \to \exists_y\forall_z(z \in y \leftrightarrow \exists_{x\in u}\varphi(x, z))),$$

zodanig dat dit axioma uitdrukt dat het beeld van een verzameling u onder een functie $f : u \longrightarrow v$ weer een verzameling is.

8

Het verzamelingstheoretisch universum

We gaan het "papieren" formalisme van **ZF** nu interpreteren in "echte" verzamelingen, analoog aan de interpretatie van **PA** in de "echte" natuurlijke getallen. De gebruikelijke interpretatie (semantiek) van **ZF** is het *verzamelingstheoretisch universum* V, ook wel genoemd de *cumulatieve hiërarchie*.[1] De rol van de natuurlijke getallen $\mathbb{N}$ in de semantiek van de rekenkunde **PA** wordt voor de verzamelingenleer **ZF** dus gespeeld door V. Ook de constructie van V lijkt enigszins op een bepaalde constructie van $\mathbb{N}$, waarbij de successor-operatie $S : x \mapsto x + 1$ aftelbaar vaak word toegepast op nul (zie onder).

In het vervolg noteren we "echte" verzamelingen met hoofdletters $V, W, \ldots$ (i.t.t. tot de variabelen $v, w, \ldots$ in **ZF**). Analoog gebruiken we in de interpretatie $\bigcap$, $\bigcup$, en $\subseteq$ in plaats van de formele symbolen $\cap$, $\cup$ en $\subset$ zoals gedefinieerd als afkortingen in de formele taal van **ZF**.

Het idee is om alle verzamelingen in V te maken uit de lege verzameling (waarvan het bestaan wordt aangenomen), en wel door "herhaald gebruik" van de volgende drie operaties:

- de opvolgoperatie $V \mapsto V^+ \equiv V \bigcup \{V\}$, vgl. **ZF7**;
- de verenigingsoperatie $V \mapsto \bigcup V$, vgl. **ZF5**;
- de machtsoperatie $V \mapsto P(V)$, vgl. **ZF6**.

De woorden "herhaald gebruik" zijn een *understatement*. Om het universum V te construeren moeten de drie genoemde operaties niet alleen aftelbaar vaak worden toegepast, maar moet het resultaat daarvan als "voltooid" worden beschouwd, waarna een nieuw proces van aftelbaar veel toepassingen van de operaties begint. Dit proces van aftelbaar veel toepassingen op het resultaat van een aftelbaar aantal operaties wordt ook weer aftelbaar vaak herhaald, enzovoort.[2]

In de geest van axioma **ZF1** is een verzameling V bepaald door haar elementen. Om met dit uitgangspunt de bovenstaande verzamelingen V^+, $\bigcup V$, en $P(V)$ te definiëren, moeten we zeggen wat daar de elementen van zijn, gegeven de elementen van V. We voeren daartoe inductief het symbool ε in (dat straks de interpretatie van het symbool $\in$ uit **ZF** wordt), volgens de regels:

1. er bestaat geen Z zodat $Z \varepsilon \emptyset$ (dus de lege verzameling heeft geen elementen);
2. $Z \varepsilon V^+$ desda $Z \varepsilon V$ of $Z = V$ (de elementen van V^+ zijn dus de elementen *van* V plus V *zelf*);
3. $Z \varepsilon \bigcup V$ desda er een $W \varepsilon V$ is met $Z \varepsilon W$ (de elementen van $\bigcup V$ zijn dus de elementen van de elementen van V);
4. $Z \varepsilon P(V)$ desda $Z \subseteq V$, waarbij we het van ε afgeleide symbool $\subseteq$ definieren door $Z \subseteq V$ desda voor alle $Y \varepsilon Z$ geldt dat $Y \varepsilon V$ (de elementen van $P(V)$ zijn dus de deelverzamelingen van V).

Hierbij staan V, Y, en Z voor verzamelingen in het universum V. Door dit voorschrift iteratief toe te passen kan van ieder paar verzamelingen X en Y in V worden vastgesteld of $X \varepsilon Y$. Daarmee wordt de betekenis van het symbool ε *tenminste binnen* V als bekend verondersteld. Hetzelfde geldt voor de verzamelingstheoretische haakjes: de notatie $Y = \{\ldots, Z, \ldots\}$ betekent (binnen V) dat $Z \varepsilon V$.

---

1. Dit werd in 1929 voorgesteld door von Neumann, die echter niet met pure verzamelingsleer werkte. De huidige formulering is afkomstig van Zermelo (1930). Zie H.-D. Ebbinghaus, *Ernst Zermelo: An Approach to His Life and Work* (Springer, 2007).
2. Het schier eindeloze karakter van deze constructie maakt het bestaan van V dan ook omstreden onder sommige wiskundigen en filosofen. Het is bijvoorbeeld nooit bewezen dat de constructie van V niet tot een tegenspraak leidt, en volgens de onvolledigheidsstellingen van Gödel (zoals later in dit college behandeld) kan dit ook niet binnen de verzamelingenleer worden bewezen. Je begrijpt nu ook waarom Cantor, de grondlegger van de verzamelingenleer, uiteindelijk gek werd en in een inrichting verdween.

We kunnen de gebruikelijke semantiek voor de verzamelingenleer dan als volgt formuleren.[3]

Definitie 8.1 *De interpretatie* $[[\varphi]]_{\mathsf{V}}$ *in het verzamelingstheoretisch universum van een formule* φ *in de eerste-orde taal* ***ZF*** *houdt in dat binnen* φ*:*

1. *de logische symbolen* $\neg, \wedge, \vee, \to$ *en* $=$ *hun gebruikelijke betekenis hebben, dus* $\neg$ *betekent "niet",* $\wedge$ *is "en",* $\vee$ *is "of",* $\to$ *betekent "impliceert", en = staat voor "is gelijk aan";*
2. *de variabelen over* V *lopen, zodat* $\forall_x \varphi(x)$ *betekent "voor alle verzamelingen* V *in* V *geldt de eigenschap* $\varphi(V)$*, enzovoort;*
3. *de constante* $\emptyset$ *als de lege verzameling wordt geïnterpreteerd;*
4. *Het symbool* $\in$ *als* ε *wordt geïnterpreteerd.*

Een uitspraak φ *in de eerste-orde taal van* ***ZF*** *heet* waar*, notatie* $\vDash \varphi$*, indien de uitspraak* $[[\varphi]]_{\mathsf{V}}$ *een ware eigenschap van verzamelingen uitdrukt.*

Alle axioma's van **ZFC** zijn in deze interpretatie waar, al is dit anders dan bij **PA** lastig te bewijzen.

- Je kunt nu al zien dat V zo gedefinieerd is dat axioma's **ZF1**, **ZF3**, **ZF5**, **ZF6**, en **ZF7** kloppen.
- Als we meer details over ordinalen hadden gegeven zou daaruit ook axioma **ZF8** volgen.[4]
- Ten slotte heeft axioma **ZF9** een andere status: het is (zoals alle axioma's) waar in V, maar impliceert tevens dat V niet verder uit te breiden is zonder dit axioma te schenden.

De constructie van V begint zoals gezegd bij $\emptyset$. Voor de n-voudige iteratie van de opvolgoperatie toegepast op $\emptyset$ noteren we $\dot{n}$, dus $\dot{n} = \emptyset^{+\cdots+}$ met n plussen. Voor kleine waarden van n komt er

$$\dot{0} \equiv \emptyset \equiv \{\}, \dot{1} \equiv \dot{0}^+ = \{\emptyset\}, \dot{2} \equiv \dot{1}^+ = \{\emptyset, \{\emptyset\}\}, \dot{3} \equiv \dot{2}^+ = \{\emptyset, \{\emptyset\}, \{\emptyset, \{\emptyset\}\}\}, \dot{4} \equiv \dot{3}^+ = \cdots \text{ (schrijf zelf op!).}$$

In het algemeen volgt (zie opgave)

$$\dot{n} = \{\dot{0}, \dot{1}, \ldots, n \dot{-} 1\}. \tag{8.1}$$

Je ziet dat de verzameling $\dot{n}$ precies n elementen heeft, hetgeen ook onmiddellijk uit de definitie volgt: volgens regel 1 (in de definitie van ε op de vorige pagina) heeft $\emptyset$ geen elementen, volgens regel 2 heeft $\dot{1}$ één element meer dan $\emptyset$, dus 1 element, enzovoort. Von Neumann stelde daarom voor om het natuurlijke getal n "uit het dagelijks leven" te identificeren met de verzameling $\dot{n}$, hetgeen navolging vond.

Vervolgens komt het erop aan hoe vaak de opvolgoperatie in de definitie van V "herhaald" mag worden.[5] Dit wordt gereguleerd door de axioma's van **ZF**. De verzameling

$$\mathbb{N} = \bigcup_n \dot{n} \equiv \dot{0} \bigcup \dot{1} \bigcup \cdots = \{\dot{0}, \dot{1}, \ldots\} \tag{8.2}$$

bestaat in V en is de interpretatie van ω uit de toelichting bij axioma **ZF7**: $\mathbb{N}$ is de kleinste "echte" verzameling die $\emptyset$ bevat en gesloten is onder de opvolgoperatie. De elementen van $\mathbb{N}$ zijn precies de verzamelingen $\dot{n}$ voor willekeurige natuurlijke getallen n, en hiermee is $\mathbb{N}$ binnen V geconstrueerd. Als we **ZF** en haar interpretatie in V accepteren, hoeven we de natuurlijke getallen voortaan dus niet meer als "gegeven" te beschouwen. In het bijzonder hebben we een interpretatie voor het formele symbool **0** voor nul, namelijk de lege verzameling $\dot{0} \equiv \emptyset$.

Om de interpretatie **PA** in $\mathbb{N}$ volgens Definitie 5.1 te completeren moeten we nu nog laten zien dat ook de opvolgfunctie, optelling, en vermenigvuldiging binnen V kunnen worden geïnterpreteerd (en dus evenmin als "gegeven" hoeven te worden beschouwd). Uiteraard heeft dit alleen zin als de axioma's **PA1** t/m **PA7** onder deze interpretatie waar zijn, en dat zullen we dan ook (gedeeltelijk) bewijzen.

Voor $S : \mathbb{N} \to \mathbb{N}$ nemen we uiteraard de opvolgoperatie $\dot{n} \mapsto \dot{n}^+$, $\dot{n} \varepsilon \mathbb{N}$; dit is per definitie $S(\dot{n}) = n \dot{+} 1$.

---

3. Net als bij **PA** bestaan er ook andere interpretaties van **ZFC**, maar die laten we graag over aan logici. Een belangrijk doel daarvan is de studie van de *Continuümhypothese* van Cantor, die inhoudt dat de verzamelingen $P(\omega)$ en ω_1 isomorf zijn. Na eerdere bijdragen van Gödel toonde Paul Cohen in 1963 aan dat deze hypothese in **ZFC** bewezen noch weerlegd kan worden.
4. Axioma's **ZF2** en **ZF4** zijn daar gevolgen van.
5. Hier gebeurt iets dat in de constructie van het universum V steeds terugkomt: er wordt een enigszins twijfelachtige stap gezet, namelijk het samenvoegen van *aftelbaar* veel elementen tot een nieuwe verzameling, die vervolgens wordt opgehangen aan een (of meer) van de axioma's van **ZF** (in dit geval **ZF7**). Twee koorddansers, beiden in levensgevaar, houden elkaar zo in evenwicht!

We definiëren optelling en vermenigvuldiging *recursief*, vanuit de volgende ware uitspraak in **ZF**.

Stelling 8.1 *Bij een gegeven functie $h : \mathbb{N} \to \mathbb{N}$ en element $\dot{n}_0 \varepsilon \mathbb{N}$ bestaat een unieke functie $f : \mathbb{N} \to \mathbb{N}$ die voldoet aan $f(\dot{0}) = \dot{n}_0$ en $f(S(\dot{n})) = h(f(\dot{n}))$.*

We laten het officiële bewijs met inductie weg, maar merken wel op dat het bewijzen door inductie geldig is vanwege axioma **PA7**, dat we straks zullen bewijzen in V. Informeel zie je direct dat

$$f(\dot{1}) = f(S(\dot{0})) = h(f(\dot{0})) = h(\dot{n}_0),\ f(2) = h(h(\dot{n}_0)),\ \ldots, f(\dot{n}) = h^n(\dot{n}_0).$$

Nu kunnen we optelling met een vast getal $\dot{n}_0$ (als functie van $\mathbb{N}$ naar $\mathbb{N}$, dus $f_{\dot{n}_0} : \dot{n} \mapsto \dot{n}_0 + \dot{n}$) recursief definiëren door de keuze $h = S$: ga na dat dan geldt $f_{\dot{n}_0}(\dot{n}) = \dot{n}_0 + \dot{n}$. Ten slotte is $\dot{n}_1 + \dot{n}_2$ per definitie $f_{\dot{n}_1}(n_2)$. Daarmee is optelling als functie van $\mathbb{N} \times \mathbb{N}$ naar $\mathbb{N}$ gedefinieerd. Evenzo vermenigvuldiging, in eerste instantie weer met vaste $\dot{n}_0$ (zie opgave) en vervolgens van $\mathbb{N} \times \mathbb{N}$ naar $\mathbb{N}$.

We bewijzen nu als illustratie enige van de Peano-axioma's in V; de andere zijn oefeningen.

[[**PA1**]]$_{\mathbb{N}}$: $\forall_{\dot{n}\varepsilon\mathbb{N}} \neg(S(\dot{n}) = \dot{0})$. Met $S(\dot{n}) = \dot{n}^+ = \dot{n} \cup \{\dot{n}\}$ volgt $\dot{n}\varepsilon\dot{n}^+$. De verzameling $\dot{n}^+$ is dus niet leeg en daarmee niet gelijk aan $\emptyset$. Dus $S(\dot{n}) \neq \dot{0}$.

[[**PA3**]]$_{\mathbb{N}}$: $\forall_{\dot{n}_0\varepsilon\mathbb{N}}(\dot{n}_0 + 0 = \dot{n}_0)$. Dit is de ene helft van onze recursieve definitie van optelling: $f(\dot{0}) = \dot{n}_0$.

[[**PA4**]]$_{\mathbb{N}}$: $\forall_{\dot{n}_0\varepsilon\mathbb{N}} \forall_{\dot{n}\varepsilon\mathbb{N}}(\dot{n}_0 + S(\dot{n}) = S(\dot{n}_0 + \dot{n}))$. En dit is de andere helft: $h = S$ en dus $f(S(\dot{n})) = S(f(\dot{n}))$.

[[**PA7**]]$_{\mathbb{N}}$: $\varphi(0) \wedge (\forall_{\dot{n}\varepsilon\mathbb{N}}(\varphi(\dot{n}) \to \varphi(S(\dot{n}))) \to \forall_{\dot{n}\varepsilon\mathbb{N}}\varphi(\dot{n})$. Volgens **ZF2** is $\{\dot{n}\varepsilon\mathbb{N} \mid \varphi(\dot{n})\}$ een bepaalde deelverzameling $V \subseteq \mathbb{N}$. Ten eerste volgt uit $\varphi(0)$ dat $\emptyset\varepsilon V$. Ten tweede volgt uit $\varphi(\dot{n}) \to \varphi(S(\dot{n}))$ dat als $\dot{n}\varepsilon V$, dan $\dot{n}^+\varepsilon V$. Maar $\mathbb{N}$ is de kleinste verzameling die $\emptyset$ bevat en gesloten is onder de opvolgoperatie. Dus $V = \mathbb{N}$, en daarmee is $\varphi(\dot{n})$ waar voor alle $\dot{n}\varepsilon\mathbb{N}$.

Opgave 8.1

a) Bewijs (8.1).
b) Wat zijn de elementen van de verzameling $\bigcup \dot{n}$? Bewijs je antwoord.

Opgave 8.2

Bewijs dat axioma **PA2** waar is in V, met $[[\mathbf{PA2}]]_{\mathbb{N}} \equiv \forall_{\dot{n}\varepsilon\mathbb{N}} \forall_{\dot{m}\varepsilon\mathbb{N}}(S(\dot{n}) = S(\dot{m}) \to \dot{n} = \dot{m})$.

Opgave 8.3

a) Geef een recursieve definitie van vermenigvuldiging met een vast getal $\dot{n}_0$.
b) Bewijs vanuit die definitie de axioma's **PA5** en **PA6**.

Voor de liefhebbers geven we nu nog wat meer informatie over V (geen tentamenstof).

Een verzameling die je uit $\emptyset$ kunt maken door herhalingen van de opvolgoperatie én de verenigingsoperatie heet een *ordinaal*. I.h.b. is de lege verzameling $\emptyset \equiv \dot{0}$ een ordinaal, verkregen door nul keer toepassen van de genoemde operaties. Vervolgens zijn alle verzamelingen $\dot{n}$ als boven ordinalen, verkregen door n keer de opvolgoperatie toe te passen op $\emptyset$. De vereniging van al deze ordinalen is ω. Daarna wordt het proces om nieuwe ordinalen te construeren moeizaam: voor vezamelingstheoretici is het een feest.[6] In principe gaat het als volgt verder:

- Met de notatie $\alpha + n$ als n'de opvolger van α (dus $\alpha + 1 \equiv \alpha^+$, $\alpha + 2 \equiv (\alpha^+)^+$, etc.), maken we nu uit ω de ordinalen $\omega + 1, \omega + 2, \ldots$. Die vormen samen het volgende ordinaal, genaamd $\omega \cdot 2$.
- Dan $\omega \cdot 2 + 1, \omega \cdot 2 + 2, \ldots$, met limiet $\omega \cdot 3$. Evenzo $\omega \cdot 4, \omega \cdot 5, \ldots$, met limiet $\omega \cdot \omega \equiv \omega^2$.
- Vervolgens $\omega^2 + 1, \omega^2 + 2, \ldots$, met limiet $\omega^2 + \omega$. Dan $\omega^2 + \omega \cdot 2, \omega^2 + \omega \cdot 3, \ldots$, met limiet $\omega^2 + \omega^2 \equiv \omega^2 \cdot 2$. De rij $\omega^2 \cdot 2, \omega^2 \cdot 3, \ldots$ leidt tot ω^3, enz. De limiet van $\omega^2, \omega^3, \ldots$, heet ω^ω.

6. Voor een populaire uiteenzetting zie J. Stillwell, *Roads to Infinity* (A K Peters, 2010).

- Daaruit ω^{ω^ω}, en zo ontstaat een diagonaal met n machten ω. Deze diagonalen hebben limiet ε_0.
- Dit laatste ordinaal is gigantisch, maar nog steeds aftelbaar (als verzameling). We herhalen al deze stappen nu *ad nauseam* en krijgen zo uiteindelijk alle aftelbare ordinalen.
- De verzameling van alle *aftelbare* ordinalen is zelf een ordinaal genaamd ω_1, nu *overaftelbaar*.
- Dit proces begint opnieuw vanuit ω_1: je krijgt 'uiteindelijk' (haha) alle ordinalen door eindeloos de opvolgoperatie en het nemen van verenigingen van alle voorgaande ordinalen toe te passen.

Gelukkig is er ook een directe en hanteerbare karakterisatie van ordinalen (het had ook een definitie kunnen zijn), die we zonder bewijs geven.[7] We noemen een verzameling z *transitief* als $x \varepsilon\, y \varepsilon\, z$ impliceert dat $x \varepsilon\, z$.

Stelling 8.2 *Een* ordinaal *is een transitieve verzameling (binnen* V*) waarvan alle elementen zelf ook weer transitieve verzamelingen zijn. M.a.w., een ordinaal* α *heeft de volgende twee eigenschappen:*

1. *als* $x \varepsilon\, y \varepsilon\, \alpha$ *(i.e.* $y \varepsilon\, \alpha$ *en* $x \varepsilon\, y$*), dan* $x \varepsilon\, \alpha$ *(equivalent: als* $y \varepsilon\, \alpha$*, dan* $y \subset \alpha$*).*
2. *als* $x \varepsilon\, y \varepsilon\, z \varepsilon\, \alpha$*, dan* $x \varepsilon\, z$ *(equivalent: als* $y \varepsilon\, z \varepsilon\, \alpha$*, dan* $y \subset z$*).*

Ordinalen hebben de volgende fantastische eigenschappen:

Stelling 8.3 *1. Als* α *een ordinaal is en* $\beta \varepsilon\, \alpha$*, dan is* β *eveneens een ordinaal.*
2. *Als* α *een ordinaal is, dan is* α^+ *dat ook.*
3. *Als* α *een verzameling ordinalen is, dan is* $\cup\alpha$ *een ordinaal.*
4. *Als* α *een ordinaal is, dan geldt ofwel* $\cup\alpha \varepsilon\, \alpha$ *ofwel* $\cup\alpha = \alpha$ *(en dus in beide gevallen* $\cup\alpha \subset \alpha$*).*
5. *Als* α *en* β *ordinalen zijn, dan zijn er slechts de volgende drie mogelijkheden:*
   (a) $\alpha = \beta$*;*
   (b) $\alpha \varepsilon\, \beta$*;*
   (c) $\beta \varepsilon\, \alpha$*.*

Om de eerder genomen stap van de eindige ordinalen $\dot{n}$ naar het oneindige ordinaal ω beter te begrijpen, stellen we vast dat ieder ordinaal γ *totaal geordend* is door ε, met andere woorden, als $\alpha \varepsilon\, \gamma$ en $\beta \varepsilon\, \gamma$, dan geldt precies één van de mogelijkheden (a), (b), of (c) uit deel 4 van Stelling 8.3 (volgens deel 1 van deze stelling zijn α en β immers zelf ordinalen). Er zijn daarom twee verschillende soorten ordinalen γ:

1. γ heeft een (noodzakelijk uniek) grootste element β t.o.v. ε, i.e., voor $\alpha \varepsilon\, \gamma$ geldt $\alpha \varepsilon\, \beta$ of $\alpha = \beta$. Dit is het geval bij alle $\dot{n} \neq \dot{0}$. Dan gelden $\beta = \cup\gamma$, $\beta \varepsilon\, \gamma$, en $\gamma = \beta^+$, en heet γ een *opvolger*.
2. γ heeft *geen* grootste element t.o.v. ε. Dan is $\cup\gamma = \gamma$, bestaat geen β als in 1., en γ heet een *limiet*.

Een limiet γ is de kleinste bovengrens van de verzameling van al haar elementen, geordend volgens ε, of met andere woorden: als een ordinaal δ voldoet aan $\alpha \varepsilon\, \delta$ voor alle $\alpha \varepsilon\, \gamma$, dan geldt $\delta = \gamma$ of $\gamma \varepsilon\, \delta$.
Het is (hopelijk) duidelijk dat bijv. ieder ordinaal $\dot{n}$ voor $n > 0$ een opvolger is, terwijl ω een limiet is.

We hebben nu alle *ordinalen*, maar om alle *verzamelingen* in V te krijgen is ook de machtsoperatie nodig. Voor ieder ordinaal γ definiëren we iteratief een verzameling V_γ door middel van de volgende stappen:

$$\mathsf{V}_0 = \emptyset; \tag{8.3}$$

$$\mathsf{V}_{\beta+} = P(\mathsf{V}_\beta); \tag{8.4}$$

$$\mathsf{V}_\gamma = \bigcup_{\beta \varepsilon\, \gamma} \mathsf{V}_\beta \text{ als } \gamma \text{ een limiet (i.t.t. een opvolger) is.} \tag{8.5}$$

Hier is $\bigcup_{\beta \varepsilon\, \gamma} \mathsf{V}_\beta$ de vereniging $\cup$ van de (ene) verzameling die alle vezamelingen V_β, met $\beta \in \gamma$, als elementen heeft: de elementen van $\bigcup_{\beta \varepsilon\, \gamma} \mathsf{V}_\beta$ zijn dus de elementen van V_β voor willekeurige $\beta \in \gamma$.

Net als bij de ordinalen beginnen we dus bij de lege verzameling en bouwen gestaag een gigantische klasse verzamelingen op. Na $\mathsf{V}_1 = \dot{1}$, en $\mathsf{V}_2 = \dot{2}$ valt $\mathsf{V}_n = P^n(\emptyset)$ niet meer samen met $\dot{n}$, maar bevat deze verzameling wel. Dan komt $\mathsf{V}_\omega = \bigcup_n P^n(\emptyset)$, die (als verzameling) isomorf is met ω en met $\mathbb{N}$, vervolgens $\mathsf{V}_{\omega^+} = P(\mathsf{V}_\omega)$, waar de reële getallen een kopie van zijn, en ten slotte $\mathsf{V}_{\omega^{++}} = P(P(\mathsf{V}_\omega))$, waarin alle deelverzamelingen van $\mathbb{R}$ bevat zijn. Meer zul je in de alledaagse praktijk van de wiskunde niet tegenkomen. Hoe dan ook is het 'verzamelingstheoretisch universum' als volgt gedefinieerd:

$$\mathsf{V} = \bigcup_\gamma \mathsf{V}_\gamma, \tag{8.6}$$

waarbij de vereniging over alle ordinalen γ is. Het object V speelt de rol van de klasse van alle verzamelingen en is zelf geen verzameling. De notatie $\cup$ in (8.6) is dan ook symbolisch: de elementen van V, dus de verzamelingen die samen het universum vormen, zijn de elementen van V_γ, voor een willekeurig ordinaal γ. Aangezien de V_γ wél verzamelingen zijn, zijn de elementen van V dus goed gedefinieerde verzamelingen (i.t.t. V zelf).

7. Als definitie is Stelling 8.2 afkomstig van von Neumann. Het begrip ordinaal komt echter al prominent bij Cantor voor.

9

Berekenbare functies

Je zou misschien denken dat het voorafgaande materiaal hooguit van belang is voor de zuivere wiskunde en daarmee, net als bijvoorbeeld muziek, niet of nauwelijks van praktisch belang is voor de maatschappij. Het tegendeel is waar: dieper nadenken over axioma's en bewijsbaarheid leidde tot niets minder dan de moderne computer! We danken deze dus niet aan zakenmannetjes als Bill Gates en Steve Jobs, maar aan wiskundigen als David Hilbert, Kurt Gödel, Alan Turing, en John von Neumann.[1]

De cruciale eigenschap van iedere moderne computer (inclusief de iPhone etc.) is dat deze 'universeel' is, in de zin dat willekeurige programma's (tegenwoordig ook genaamd *Apps*) in het geheugen kunnen worden opgeslagen en worden uitgevoerd. Een moderne computer is dus hetzelfde als een *stored-program computer*. Een programma leest meestal zelf ook weer data in, maar in principe is er (tenminste onder de zgn. von Neumann architectuur waarop vrijwel alle computers gebaseerd zijn) geen verschil tussen dergelijke data en programma's zelf. Dit was een zeer diep idee, met de volgende geschiedenis.

1. In 1900 stelde Hilbert een beroemde lijst van 23 wiskundige problemen op, die enorme invloed had op de ontwikkeling van de wiskunde in de 20e eeuw. Het tiende probleem van Hilbert was: vind een algorithme om te bepalen of een Diophantine vergelijking een oplossing heeft.[2]
   Op dat moment bestond er overigens nog geen precieze definitie van een 'algoritme', zodat de exacte wiskundige betekenis van dit probleem zelf ook nog moest worden opgehelderd.
2. In 1928 formuleerde Hilbert (met zijn leerling Wilhelm Ackermann, 1896–1962) het *Entscheidungsproblem*, dat neerkomt op de vraag naar een algoritme dat beslist of een willekeurige uitspraak in eerste-orde logica bewijsbaar is.
3. Dit probleem was onderdeel van een groot onderzoeksprogramma naar de grondslagen van de wiskunde, waarin Hilbert als doel had om te bewijzen dat gangbare axiomatische systemen als **PA** en **ZF** zowel *consistent* als *volledig* waren.[3] Dit lukte hem en zijn medewerkers (zoals Ackermann, Paul Bernays (1888–1977), von Neumann, en Gerhard Gentzen (1909–1945) echter niet.
4. Totaal onverwacht bewees Gödel in 1931 dat deze pogingen niet voor niets steeds mislukten:
   (a) Zijn eerste onvolledigheidsstelling stelt dat (in systemen als **PA** of **ZF**, onder de aanname van consistentie) *ware* maar binnen dat systeem *niet bewijsbare* uitspraken bestaan.
   (b) Zijn tweede onvolledigheidsstelling geeft een voorbeeld van zo'n uitspraak, namelijk dat het gegeven logische systeem consistent is (aangenomen dat dit het geval is).
5. Gebruik makend van technieken van Gödel, met name van diens fundamentele idee om logische formules te coderen door natuurlijke getallen en logische operaties zoals het bewijzen van stellingen te coderen door rekenkundige operaties, bewezen Church en Turing (onafhankelijk) in 1936

---

1. Ook de 19e eeuwse wiskundige en uitvinder Charles Babbage (1791–1871) wordt in dit verband vaak genoemd. Zijn *Analytical Engine* was echter geen *stored-program computer* in de moderne zin, zie onder, maar kon worden geprogrammeerd met behulp van ponskaarten. Het was er wel een belangrijke voorloper van. Zie bijvoorbeeld H. Goldstine, *The computer: from Pascal to von Neumann* (Princeton University Press, 1993).
2. Een Diophantine vergelijking heeft de vorm $p(x_1, \ldots, x_N) = 0$, waarin p een n-de graads polynoom in N variabelen is met coefficiënten in $\mathbb{Z}$, en $(x_1, \ldots, x_N) \in \mathbb{N}^N$. Meestal wordt geëist dat $x_i > 0$. Hier is $n = 1$ al interessant, zoals blijkt uit het Algoritme van Euclides om $ax_1 + bx_2 = c$ op te lossen (hier is dus $p(x_1, x_2) = ax_1 + bx_2 - c$). Een voorbeeld met $n = 2$ en $N = 3$ is $p(x_1, x_2, x_3) = x_1^2 + x_2^2 - x_3^2$. Uiteraard heeft de vergelijking $p(x_1, x_2, x_3) = 0$ vele niet-triviale oplossingen, zoals $(3, 4, 5)$. Het *Laatste Theorema van Fermat* is van Diophantine-vorm: met $p(x_1, x_2, x_3) = x_1^n + x_2^n - x_3^n$ heeft de vergelijking $p(x_1, x_2, x_3) = 0$ voor alle heeltallige $n > 2$ geen niet-triviale oplossingen (x_1, x_2, x_3), zoals in 1637 beweerd door Pierre de Fermat en in 1993 bewezen door Andrew Wiles, met een correctie in 1994 door Richard Taylor.
3. Bovendien wilde hij dat binnen die systemen en met 'eindige' methoden bewijzen. Het laatste was een antwoord op L.E.J. Brouwer en Hermann Weyl, die niets moesten hebben van de verzamelingenleer van Cantor. Het bewijzen van de gewenste eigenschappen van bijv. **ZF** binnen **ZF** was nodig om oneindige regressie te voorkomen: als ingewikkeldere systemen dan **ZF** nodig waren om de consistentie en volledigheid van **ZF** te bewijzen, zou dat weinig zeggen over de betrouwbaarheid van **ZF**.

dat het *Entscheidungsproblem* geen oplossing heeft. Het belangrijkste onderdeel van hun oplossing was het preciseren van de begrippen 'algoritme' en 'berekening'. Bovendien kwam Turing met het idee van een 'Universele Turing Machine', dat een blauwdruk bleek te zijn van de latere *stored-program computer*. Von Neumann maakte hierbij gebruik van de ideeën van Turing, die hij ook persoonlijk kende.[4]

6. In 1945 schreef von Neumann het legendarische document *First Draft of a Report on the EDVAC*, dat voor het eerst de principes van een moderne computer beschrijft.[5]
7. Vanaf 1948 werden de eerste *stored-program computers* volgens het model van von Neumann gebouwd (ook door hemzelf, nl. de IAS-computer in Princeton, die in 1952 werd voltooid).[6]
8. In 1970 bewees Yuri Matiyasevich dat het antwoord op Hilberts tiende probleem "nee" was.

Hoewel het programma van Hilbert dus niet is gelukt, is de moderne computer dankzij deze mislukking ontstaan. Bovendien heeft de ontwikkeling van de logica dankzij Hilbert en zijn leerlingen een hoge vlucht genomen. Ten slotte staat het fundamentele inzicht van Hilbert dat bewijzen *in principe* (i.e., voor zover het discussies over de grondslagen van de wiskunde betreft) een formele, symbolische activiteit is, die gescheiden moet worden van de interpretatie van het formalisme, nog steeds als een huis.

Om deze ontwikkeling te begrijpen geven we eerst Turings antwoord op de vraag wat een algoritme precies is. Ruw gezegd transformeert een algoritme op en systematische manier discrete input in discrete output. Soms zijn deze al gegeven als natuurlijke getallen, bijvoorbeeld bij de vraag of er een algoritme is om het product of de deling van twee natuurlijke getallen te berekenen. Maar vaak moeten de input (bijv. twee gegeven plaatsen op de kaart) en de output (bijv. de kortste route tussen die plaatsen) als eerste stap worden vertaald naar natuurlijke getallen, en moet de gezochte transformatie worden vertaald naar een functie $f : \mathbb{N}^p \to \mathbb{N}$, voor zekere $p \in \mathbb{N}$ (bijv. $p = 2$). In principe volstaat het geval $p = 1$, omdat voor alle p een injectie $\tau_p : \mathbb{N}^p \to \mathbb{N}$ bestaat, nl.

$$\tau_p(x_1, \ldots, x_p) = 2^{x_1} + 2^{x_1+x_2+1} + 2^{x_1+x_2+x_3+2} + \cdots + 2^{x_1+\cdots+x_k+k-1} - 1, \tag{9.1}$$

die uit breidt tot een bijectie $\tau : \bigcup_{p>0} \mathbb{N}^p \to \mathbb{N}$ (welke bovendien berekenbaar is in de onderstaande zin). Hoe dan ook, voor deze vertaalslag bestaat geen algemeen wiskundig voorschrift, omdat het uitgangspunt zelf vaak niet wiskundig geformuleerd is (als je bijvoorbeeld een kortste-pad algoritme wilt vinden moet je eerste alle plaatsen en wegen nummeren).[7] Ook als het uitgangspunt wel al wiskundig van aard is, zoals bij het *Entscheidungsproblem*, is er meestal sprake van een zekere willekeur in de vertaling naar getallen; we zullen dit later expliciet zien bij de zgn. Gödel-codering.

Hoe dan ook lag Turings bijdrage in de volgende stap, namelijk het geven van een definitie van de eventuele *berekenbaarheid* van $f : \mathbb{N}^p \to \mathbb{N}$. Als een bepaalde taak/probleem na vertaling naar natuurlijke getallen door (de berekening van) een berekenbare functie kan worden uitgevoerd/opgelost, dan noemen we de taak algoritmisch uitvoerbaar/oplosbaar. Zulke taken kunnen in principe door een computer worden uitgevoerd, en dat is ook precies wat Turings definitie van berekenbaarheid beoogt.

Vanwege de mogelijkheid dat een algoritme wel goed is gedefinieerd maar vastloopt c.q. oneindig lang duurt, is het belangrijk om te werken in de algemenere setting van *partiële* functies. In **ZF** houdt dit in:

Definitie 9.1 *Een* partiële *functie $f : u \to v$ is een functie van een* deelverzameling $D(f) \subset u$ *naar* v. *Met andere woorden: de grafiek G_f van f is een deelverzameling van $u \times v$ die voldoet aan de eis*

$$(((x, y) \in G_f) \wedge ((x, z) \in G_f)) \to (y = z).$$

Een totale *functie is een partiële functie met $D(f) = u$ (en is dus hetzelfde als een 'gewone' functie, die voldoet aan de sterkere eis $\forall_{x\in u}\exists!_{y\in v}(x, y) \in G_f$).*

De notatie $f(x)\downarrow$ betekent $x \in D(f)$, in welk geval de waarde $f(x) \in v$ bestaat. Voor $x \notin D(f)$ is $f(x)$ niet gedefinieerd*, en noteren we $f(x)\uparrow$.*

4. Zie W. Aspray, *John von Neumann and the Origins of Modern Computing* (MIT Press, 1990).
5. Zie `http://qss.stanford.edu/~godfrey/vonNeumann/vnedvac.pdf`.
6. Zie behave Aspray ook G. Dyson, *Turing's Cathedral: The Origins of the Digital Universe* (Pantheon Books, 2012). Voor latere ontwikkelingen zie P.E. Ceruzzi, *Computing: A Concise History* (MIT Press, 2012).
7. Iets dergelijks geldt voor alle toepassingen van de wiskunde: deze beginnen met een stap die het probleem mathematiseert.

Wij gaan deze definitie meestal gebruiken voor $u = \mathbb{N}^p$ en $v = \mathbb{N}$ (soms ook met $v = \underline{2} \equiv \{0, 1\}$). Neem bijvoorbeeld de functie $f : \mathbb{N} \to \mathbb{N}$ met $f(n) = n/2$. Deze functie neemt uiteraard alleen op even getallen weer waarden aan in $\mathbb{N}$, en we kiezen hier dus $D(f) = \{n \in \mathbb{N} \mid n = 2m, m \in \mathbb{N}\}$. We schrijven dan dus $f(n)\downarrow$ als n even is, terwijl $f(n)\uparrow$ als n oneven is. De reden dat we niet gewoon zeggen dat f een functie is van $D(f)$ naar v, is dat we vaak willen spreken over de verzameling van *alle* partiële functies f van u naar v, waarbij het domein evt. van f af kan hangen.

Om het idee precies te maken dat een (partiële) functie $f : \mathbb{N}^p \to \mathbb{N}$ berekenbaar is als deze door een computer kan worden berekend, gaf Turing als eerste een wiskundig model (beter gezegd: een karikatuur) van een computer en van een computerprogramma.[8] Turings model heet tegenwoordig een *Turing machine*, maar het is eenvoudiger om met een later model te werken, genaamd een *Registermachine*.[9]

Definitie 9.2 *Een registermachine bestaat uit de volgende onderdelen* hardware*:*

- *Een eindig maar willekeurig uit te breiden aantal* geheugenplaatsen *(registers)* $(R_1, R_2, \ldots)$*, waarin natuurlijke getallen* $(m_1, m_2, \ldots)$ *kunnen worden opgeslagen. We noteren* $m_i \in R_i$*, waarbij op ieder moment slechts een eindig aantal* m_i *ongelijk nul is.*
- *Een* lees/schrijfkop *die een (door een instructie in een programma) voorgeschreven geheugenplaats kan bezoeken en de inhoud daarvan kan lezen en veranderen.*

Een programma P *van lengte* $N < \infty$ *bestaat uit een eindig aantal regels niet-triviale code* $P_1, \ldots, P_N$*, aangevuld met een lege regel* P_0 *(genaamd de '*halting state*). Iedere regel met* $N \neq 0$ *bevat een code voor een actie van de kop. Deze code is van de vorm* (k, p_+) *of* (k, p_0, p_-)*, waarbij* $k \in \mathbb{N}\backslash\{0\} = \{1, 2, 3, \ldots\}$ *naar een geheugenplaats verwijst en* p_+*,* p_0*, en* p_- *de waarden van 0 t/m* N *aan kunnen nemen en dus naar regels in* P *verwijzen. Deze codes staan voor de volgende instructies.*

- (k, p_+) *betekent: tel 1 op bij de inhoud van* R_k *(i.e.,* $m_k \mapsto m_k + 1$*) en spring naar regel no.* p_+*.*
- (k, p_0, p_-) *betekent:*[10]
  - *als* $m_k = 0$*: spring naar regel no.* p_0 *(en laat* m_k *zoals het is).*
  - *als* $m_k > 0$*: trek 1 af van de inhoud van* R_k *(i.e.,* $m_k \mapsto m_k - 1$*) en spring naar regel no.* p_-*.*

Het programma begint met P_1*, vanuit een bepaalde beginconfiguratie of* input*, genoteerd als* $(n_1, n_2, \ldots)$*, dus* $(m_i = n_i)$ *aan het begin. De instructie* P_1 *wordt uitgevoerd, waarna het programma volgens deze instructie naar een andere (of dezelfde) regel springt, enzovoort.*[11] *Er zijn dan twee mogelijkheden:*

1. *Regel* P_0 *wordt bereikt. Einde programma, met als output de geheugeninhoud* $(m_1, m_2, \ldots)$ *na verwerking van de laatste regel vóór* P_0 *werd bereikt.*
2. *Regel* P_0 *wordt nooit bereikt. De computer draait dol en er is geen output.*

Een gegeven programma P *berekent voor iedere* $p \in \mathbb{N}$ *een* partiële functie $f_P^p : \mathbb{N}^p \to \mathbb{N}$*, als volgt:*

- *Het domein* $D(f_P^p)$ *bestaat uit alle* $\vec{n} \equiv (n_1, n_2, \ldots, n_p)$*, waarvoor* P *op input* $(n_1, n_2, \ldots, n_p, 0, 0, \ldots)$*, dus* $m_i = n_i$ *voor alle* $i = 1, \ldots, p$ *en* $m_i = 0$ *voor alle* $i > p$*, uiteindelijk stopt;*
- *Voor* $\vec{n} \in D(f_P^p)$ *is de waarde* $f_P^p(\vec{n})$ *per definitie de inhoud* m_1 *van register* R_1 *in zodra* P_0 *is bereikt (de inhoud van de andere registers doet er op dat moment dus niet meer toe).*
- *Voor* $\vec{n} \notin D(f_P^p)$ *is de waarde* $f_P^p(\vec{n})$ *niet gedefinieerd, oftewel* $f_P^p(\vec{n})\uparrow$*.*

---

8. In de jaren '30, toen Turing zijn definitie gaf, waren computers nog mensen, meestal vrouwen, die in lange rijen in een klaslokaal gezeten een grote berekening uitvoerden. Er is echter geen principieel verschil tussen zulke levende computers en onze elektronische computers, tenminste als de elementaire stappen in een berekening foutloos worden uitgevoerd (beide kunnen natuurlijk ook fouten maken, de eerste als ze niet goed opletten en de tweede als ze kapot zijn). Zoals gezegd hadden de ideeën van Turing, al waren ze op menselijke computers gebaseerd, een enorme invloed op de ontwikkeling van elektronische computers.
9. Bij een Turing machine heb je i.p.v. de registers een potentieel oneindig lange tape verdeeld in vakjes, met in ieder vakje een 0 of een 1, waarbij slechts eindig veel enen mogen voorkomen. Iedere regel P_i is van de vorm $(\pi_0, \varphi_0, p_0; \pi_1, \varphi_1, p_1)$, waarbij (π_0, φ_0, p_0) de regel is als het zojuist afgelezen vakje een 0 bevat, en (π_1, φ_1, p_1) de regel bij 1. Hierbij is $\pi_0 \in \{0, 1\}$, $\varphi_0 \in \{-1, 0, 1\}$, en $p_0 \in \underline{N} \equiv \{1, \ldots, N\}$; *idem dito* voor (π_1, φ_1, p_1). Stel dat het vakje een p bevat ($p = 0, 1$), zodat de regel (π_p, φ_p, p_p) wordt uitgevoerd. Deze bestaat uit drie stappen: 1. print π_p in het zojuist afgelezen vakje; 2. verschuif de leeskop een vak naar rechts/links als $\varphi_p = 1/-1$, en schuif niet als $\varphi_p = 0$; 3. spring naar regel no. p_p. In de begintoestand P_1 leest de kop het meest linkse vakje dat een 1 bevat.
10. De actie die door (k, p_+) gecodeerd wordt hangt dus niet af van de inhoud van de registers, terwijl de actie n.a.v. (k, p_0, p_-) afhangt van de inhoud m_k van R_k.
11. Het is dus niet zo dat na P_1 automatisch P_2 volgt, enz.

In deze definitie stond het 'gegeven' programma P voorop, dat vervolgens een hele rits functies $f_P^1, f_P^2, \ldots$ blijkt te berekenen. Nu stellen we een 'gegeven' partiële functie voorop, en bereiken Turings doel:

Definitie 9.3 *Een partiële functie $f : \mathbb{N}^p \to \mathbb{N}$ heet berekenbaar als er een programma P op een registermachine bestaat dat f berekent, met andere woorden, waarvoor geldt $f_P^p = f$.*

Stel bijvoorbeeld $N = 2$, met $P_1 = (2, 0, 2)$, en $P_2 = (1, 1)$. Dan verloopt het programma als volgt:

- Bij P_1 leest de kop het register R_2 en kijkt of $m_2 = 0$.
  - Zo ja, dan springt het naar de *halting state* P_0 en is het klaar.
  - Zo nee, dan wordt m_2 vervangen door $m_2 - 1$ en springt het programma naar P_2.
- Daarin vervangt het m_1 door $m_1 + 1$ en springt terug naar P_1.
- Deze stappen worden herhaald tot $m_2 = 0$, waarna het programma stopt.

De output is dus $m_1 = n_1 + n_2$, $m_2 = 0$, en $m_k = n_k$ voor alle $k > 2$, en we zien dat $f_P^2(n_1, n_2) = n_1 + n_2$. Het is duidelijk dat het programma altijd stopt, zodat optelling als totale functie is gedefinieerd.

Deze definitie *lijkt* af te hangen van de keuze van een registermachine als model voor een computer, maar dat is niet het geval: het blijkt dat alle 'redelijke' modellen voor computers, inclusief de nu bestaande computers, dezelfde klasse van berekenbare functies geven.[12] De zogenaamde *Church–Turing thesis* zegt zelfs dat *alle* manieren om het begrip 'algoritme' of 'berekenbaarheid' wiskundig te definieren equivalent zijn. Omdat de begrippen 'algoritme' etc. in eerste instantie intuïtief zijn, is dit niet echt een stelling of zelfs maar een vermoeden, maar eerder een "gevoel" dat we niet verder hoeven te zoeken: Turing heeft de vraag wat 'berekenbaarheid' is met Definitie 9.3 definitief beantwoord.

De volgende drie elementaire functies zullen verder een grote rol spelen:

1. de *nulfunctie* $Z : \mathbb{N} \to \mathbb{N}$, gedefinieerd door $Z(n) = 0$ voor alle $n \in \mathbb{N}$;
2. de *opvolgfunctie* $S : \mathbb{N} \to \mathbb{N}$, gedefinieerd door$S(n) = n + 1$;
3. de *projecties* $\pi_i^p : \mathbb{N}^p \to \mathbb{N}$, gegeven door $\pi_i^p(n_1, \ldots n_p) = n_i$ voor $p \geq 1$ en $i = 1, \ldots, p$.

In no. 3 is het speciale geval $p = i = 1$ waard apart op te noemen: we hebben dan de functie $\pi_1^1(n) = n$ en schrijven deze functie ook wel als id, zodat $\mathrm{id}(n) = n$.

Een programma voor de berekening van de functie Z is bijv. $P_1 = (1, 0, 1)$ (dus $N = 1$), ga na!

Opgave 9.1

Geef programma's voor de berekening van de functies S en π_i^p.

Opgave 9.2

Stel dat een programma P een bepaalde totale functie $f : \mathbb{N} \to \mathbb{N}$ berekent, die slechts twee waarden 0 en 1 aanneemt, zodat feitelijk $f : \mathbb{N} \to \{0, 1\}$. Geef een programma dat de volgende partiële functie g berekent:

- $g(n) = 0$ desda $f(n) = 0$;
- $g(n)\uparrow$ desda $f(n) = 1$.

12. Turing machines en registermachines zoals boven gedefinieerd geven dus dezelfde berekenbare functies. Maar ook de definitie van een registermachine kent variaties. Zo kunnen de twee soorten regels code (k, p_+) en (k, p_0, p_-) in onze behandeling worden vervangen door de volgende vier soorten regels (zie N.J. Cutland, *Computability: An Introduction to Recursive Function Theory* (Cambridge University Press, 1980)).

- $Z(k)$ zet $m_k \mapsto 0$ en springt dan naar de volgende regel (dus van P_p naar P_{p+1});
- $S(k)$ verricht $m_k \mapsto m_k + 1$ en springt dan naar de volgende regel;
- $T(k, l)$ vervangt $m_l \mapsto m_k$ en springt dan naar de volgende regel;
- $J(k, l, q)$ springt naar de volgende regel als $m_k \neq m_l$ en springt naar regel P_q als $m_k = m_l$.

10

Partieel recursieve functies

Vanuit Definitie 9.3 is het vaak niet eenvoudig vast te stellen of een gegeven functie berekenbaar is. Daarom geven we in het volgende hoofdstuk een complete karakterisatie van berekenbare functies door te laten zien dat een functie berekenbaar is desda zij *partieel recursief* is. De eerste stap op weg naar de definitie van dergelijke functies is de introductie van een eenvoudigere klasse, als volgt. [1]

Definitie 10.1 *Een* primitief recursieve functie *is een functie $f : \mathbb{N}^q \to \mathbb{N}$ die kan worden verkregen uit de basisfuncties Z, S, en π_i^p door (eindige) combinaties van* samenstelling *en* recursie*, als volgt:*[2]

1. Samenstelling. *Uit l functies $h_i : \mathbb{N}^p \to \mathbb{N}$, $i = 1, \ldots, l$, voor vaste $p \geq 1$, oftewel een enkele functie $h : \mathbb{N}^p \to \mathbb{N}^l$, en één functie $g : \mathbb{N}^l \to \mathbb{N}$, kun je een nieuwe functie $f = g \circ h : \mathbb{N}^p \to \mathbb{N}$ maken. Symbolisch: $\mathbb{N}^p \xrightarrow{h} \mathbb{N}^l \xrightarrow{g} \mathbb{N}$, of in formulevorm, met de notatie $\vec{n} \equiv (n_1, \ldots, n_p)$:*

$$f(\vec{n}) = g(h_1(\vec{n}), \ldots, h_l(\vec{n})). \tag{10.1}$$

2. Recursie. *Een functie $f : \mathbb{N}^{p+1} \to \mathbb{N}$, voor vaste $p \geq 0$, is recursief gedefinieerd door twee functies $h : \mathbb{N}^{p+2} \to \mathbb{N}$ en $g : \mathbb{N}^p \to \mathbb{N}$ (met $g \in \mathbb{N}$ als $p = 0$) door middel van*

$$f(0, \vec{n}) = g(\vec{n}); \tag{10.2}$$

$$f(S(n_0), \vec{n}) = h(f(n_0, \vec{n}), n_0, \vec{n}). \tag{10.3}$$

Vanuit Definitie 10.1 kunnen we optelling, dus

$$f(n_0, n_1) = n_0 + n_1, \tag{10.4}$$

als primitief recursieve functie maken door te kiezen $p = 1$, $g = \pi_1^1$ oftewel $g(n_1) = n_1$, en $h = S \circ \pi_1^3$ oftewel $h(n_1, n_2, n_3) = S(n_1) = n_1 + 1$. Volgens resp. (10.2) en (10.3) geldt dan

$$f(0, n_1) = g(n_1) = n_1; \tag{10.5}$$

$$f(n_0 + 1, n_1) = S(f(n_0, n_1)) = f(n_0, n_1) + 1. \tag{10.6}$$

Inderdaad voldoet (10.4) daar aan en deze functie is bovendien uniek bepaald door (10.5) en (10.6).

Als tweede illustratie (doe vermenigvuldiging zelf) laten we zien dat de functie $f(n) = n!$ primitief recursief is. Deze voldoet aan $f(0) = 1$ en $f(n + 1) = f(n) \times (n + 1)$. In Definitie 10.1 kiezen we daarom $p = 0$, $g = 1$, en $h(n_1, n_2) = n_1 \times (n_2 + 1)$. Deze laatste functie is zelf weer gedefinieerd via deel 1 van Definitie 10.1 door daarin te kiezen $p = 2$, $f \rightsquigarrow h$, $g \rightsquigarrow \times$, $h_1 \rightsquigarrow \pi_1^2$ en ten slotte $h_2 \rightsquigarrow S \circ \pi_2^2$, ga na!

Een ander voorbeeld van een primitief recursieve functie is $f(n) = m^n$ voor vaste $m \in \mathbb{N}$. Deze volgt namelijk uit recursie met $g = 1$ en $h(n_1, n_2) = n_1 \times m$. Deze laatste functie is preciezer gedefinieerd als $h = \times_m \circ \pi_1^2$, waarbij de functie $\times_m : \mathbb{N} \to \mathbb{N}$ voor vaste $m \in \mathbb{N}$ is gedefinieerd als $\times_m(n) = n \times m$. Deze functie is inderdaad primitief recursief, zie opgave.

Om de partieel recursieve functies te definiëren is een nieuwe operatie nodig, genaamd *minimalisatie*. Waar de primitief recursieve functies uit het vorige hoofdstuk totaal waren (i.e., voor ieder argument gedefinieerd), kan minimalisatie een totale functie eventueel overvoeren in een partiële functie. Ofschoon minimalisatie ook op partiële functies kan worden toegepast, geven we als inleiding eerst de definitie op totale functies (zoals we zullen zien is het zelfs voldoende om dit speciale geval te begrijpen).

---

1. Stelling 8.1 is een speciaal geval van deel 2 van Definitie 10.1 met $p = 0$, $g = n_0$, en $h \equiv h \circ \pi_1^3$.
2. We moeten eigenlijk officieel bewijzen dat bij gegeven g en h een unieke functie f bestaat met de eigenschappen 10.2 en (10.3), maar dit is eenvoudig te doen met inductie en we laten dit weg.

Definitie 10.2 *Voor een gegeven totale functie $g : \mathbb{N}^{p+1} \to \mathbb{N}$, waarbij $p \geq 1$, is de partiële functie $\mu g : \mathbb{N}^p \to \mathbb{N}$, genaamd de* minimalisatie *van g, gedefinieerd door:*

$$\mu g(\vec{n}) \quad = \quad \min\{n_0 \in \mathbb{N} \mid g(n_0, \vec{n}) = 0\} \text{ (als deze } n_0 \text{ bestaat)}; \tag{10.7}$$

$$\mu g(\vec{n}) \uparrow \qquad \text{als } g(n_0, \vec{n}) > 0 \text{ voor alle } n_0 \in \mathbb{N}. \tag{10.8}$$

Minimalisatie zoekt dus het kleinste nulpunt van de functie $n_0 \mapsto g(n_0, \vec{n})$ bij gegeven $\vec{n}$. Een nulpunt is een minimum van g (waarom?), vandaar de naam 'minimalisatie'. Neem bijv. $p = 1$ en $g : \mathbb{N}^2 \to \mathbb{N}$ optelling. Dan geldt $\mu g(n) = 0$ als $n = 0$ en $\mu g(n) \uparrow$ als $n > 0$. Je ziet dus dat minimalisatie al uit een heel simpele totale functie een partiële functie kan maken. De algemene definitie is:

Definitie 10.3 *Voor een gegeven partiële functie $g : \mathbb{N}^{p+1} \to \mathbb{N}$ ($p \geq 1$) is de partiële functie $\mu g : \mathbb{N}^p \to \mathbb{N}$, opnieuw genaamd de* minimalisatie *van g, gedefinieerd door:*

$$\mu g(\vec{n}) \quad = \quad n_0 \text{ als } g(n_0, \vec{n}) = 0 \text{ én } g(m, \vec{n}) > 0 \text{ (dus i.h.b. } g(m, \vec{n}) \downarrow) \text{ voor alle } 0 \leq m < n_0; \tag{10.9}$$

$$\mu g(\vec{n}) \quad \uparrow \quad \text{als zo'n } n_0 \text{ niet bestaat.} \tag{10.10}$$

Het tweede geval (10.10) kan dus in twee verschillende situaties optreden: ten eerste als $g(n_0, \vec{n}) > 0$ voor alle $n_0 \in \mathbb{N}$, en ten tweede als er wel degelijk een n_0 (en daarmee een kleinste n_0) bestaat zodat $g(n_0, \vec{n}) = 0$, maar er dan tevens een $m < n_0$ waarvoor $g(m, \vec{n})$ niet is gedefinieerd. Als g totaal is kan de tweede situatie niet optreden, zodat Definitie 10.2 een speciaal geval is van Definitie 10.3.

Nu komen we bij de centrale definitie van dit hoofdstuk:

Definitie 10.4 *Een* partieel recursieve functie *is een partiële functie die kan worden verkregen uit de basisfuncties Z, S, en π_i^p door (eindige) combinaties van* samenstelling, recursie, *en* minimalisatie.

Deze definitie is iets minder onschuldig dan zij lijkt, omdat Definitie 10.1 van primitief recursieve functies nu ook moet worden uitgebreid naar partiële functies. Met andere woorden, om alle partieel recursieve functies te verkrijgen lijkt het noodzakelijk om niet alleen minimalisatie, maar ook samenstelling en recursie toe te passen op partiële functies. In de praktijk is dat gelukkig alleen noodzakelijk voor samenstelling, vanwege de volgende handige stelling van Kleene, die we zonder bewijs geven.[3]

Stelling 10.1 *Een partiële functie $f : \mathbb{N}^p \to \mathbb{N}$ is partieel recursief desda deze van de vorm (vgl.* (10.1)*)*

$$f(\vec{n}) = g(\mu\chi(\vec{n}), h(\vec{n})) \tag{10.11}$$

is, waarbij $g : \mathbb{N}^2 \to \mathbb{N}$, $\chi : \mathbb{N}^{p+1} \to \mathbb{N}$, en $h : \mathbb{N}^p \to \mathbb{N}$ primitief recursief zijn, en $D(f)$ bestaat uit alle $\vec{n} \in D(\mu\chi)$ en dus uit alle $\vec{n} \in \mathbb{N}^p$ waarvoor $\chi(n_0, \vec{n}) = 0$ voor zekere $n_0 \in \mathbb{N}$ (zie Definitie 10.2).

In het bijzonder kan een partieel recursieve functie f worden verkregen uit primitief recursieve functies door hooguit één keer de μ-operatie toe te passen. Dit laatste kan dan zowel tot een totale als tot een 'echte' (i.e. niet overal gedefinieerde) partiële functie leiden. Het is dus niet zo dat een overal gedefinieerde (i.e. totale) partieel recursieve functie noodzakelijk primitief recursief is: het kan gebeuren dat de μ-operatie moet worden toegepast (maar dan weer tot een totale functie leidt). Uiteraard moeten ook de primitief recursieve functies onder Stelling 10.1 vallen: in dat geval neem je simpelweg $g = \pi_2^2$, zodat $f = h$. De stelling is dan leeg.

3. Het gaat hier om een voor ons doel nuttige herformulering van het zogenaamde *Kleene normal form theorem*, een van de hoofdstellingen uit de recursietheorie. Zie bijv. Cutland, Corollary 1.4 op p. 89.

Opgave 10.1

Toon (d.m.v. een expliciete constructie) aan dat de volgende functies primitief recursief zijn:[4]

a) Vermenigvuldiging met vaste $m \in \mathbb{N}$, dus $\times_m : \mathbb{N} \to \mathbb{N}$ gedefinieerd als $\times_m(n) = n \times m$.

b) Vermenigvuldiging, dus $\times : \mathbb{N}^2 \to \mathbb{N}$ gedefinieerd door $\times(n_0, n_1) = n_0 \times n_1$.

c) De voorgangerfunctie $V : \mathbb{N} \to \mathbb{N}$, gedefinieerd door $V(0) = 0$ en $V(n) = n - 1$ voor $n > 0$.

d) De delta-functie δ_0, gedefinieerd door $\delta_0(0) = 1$ en $\delta_0(n) = 0$ voor $n > 0$.

e) De functie g_2, gedefinieerd door $g_2(n) = 0$ voor alle even n, en $g_2(n) = 1$ voor alle oneven n.

Opgave 10.2

Een *relatie* is een deelverzameling $R \subset \mathbb{N}^2$. Een relatie heet *recursief* (of *berekenbaar*) als de karakteristieke functie χ_R partieel recursief (of berekenbaar) is. Laat zien dat als R recursief is, dan de volgende partiële functie partieel recursief is:

$$f(n) \quad = \quad \min\{n_0 \in \mathbb{N} \mid (n, n_0) \in R\}; \tag{10.12}$$

$$f(n) \quad \uparrow \quad \text{als zo'n } n_0 \text{ niet bestaat.} \tag{10.13}$$

Opgave 10.3

Stel $f(n_1, n_2) = |n_2 - n_1^2|$; deze functie is berekenbaar. Wat is μf?

4. Je mag hierbij steeds eerder geconstrueerde primitief recursieve functies gebruiken(zoals bij **a)** bijv. optelling).

11

Partieel recursief = berekenbaar

Nu komt de stelling waar het allemaal om te doen was.

Stelling 11.1 *Een partiële functie $f : \mathbb{N}^p \to \mathbb{N}$ is berekenbaar desda zij partieel recursief is.*

Als we de laatste twee stellingen combineren vinden we uiteraard:

Gevolg 11.1 *Een partiële functie $f : \mathbb{N}^p \to \mathbb{N}$ is berekenbaar desda deze van de vorm* (10.11) *is, waarbij de functies g, χ, en h partieel recursief zijn.*

Een volledig bewijs van Stelling 11.1 is lang en deels ook saai, zodat we hier alleen het idee geven.[1]
Ten eerste beargumenteren we dat een partieel recursieve functie berekenbaar is.

1. We zagen in hoofdstuk 9 dat de basisfuncties Z, S, en π_i^p berekenbaar zijn.
2. Samenstelling van berekenbare (partiële) functies kan worden geprogrammeerd door programma's op een slimme manier te combineren. Als $g : \mathbb{N} \to \mathbb{N}$ en $h : \mathbb{N} \to \mathbb{N}$ beide berekenbaar en totaal zijn, met programma's resp. P_g en P_h (m.a.w., $g = f^1_{P_g}$ etc.), dan is een programma $P_{g\circ h}$ dat $g \circ h$ berekent bijvoorbeeld als volgt.
   (a) Verander in P_h (van lengte N) overal de combinaties $p_+ = 0$, $p_- = 0$ en $p_0 = 0$ door resp. $p_+ = N + 1$, $p_- = N + 1$ en $p_0 = N + 1$. Dit heeft het effect dat als P_h klaar is, niet wordt gesprongen naar P_0 maar naar P_{N+1}. De uitkomst staat dan wel in R_1.
   (b) Voeg, te beginnen met P_{N+1}, regels toe die alle registers behalve R_1 schoonvegen.
   (c) Plak P_g daar achteraan, uiteraard met hernummering van het label k op iedere regel.[2]
3. Recursie vanuit gegeven berekenbare functies is berekenbaar: begin met (10.2), dan $f(1, \vec{n}) = h(g(\vec{n}), 1, \vec{n})$, dan $f(2, \vec{n}) = h(f(1, \vec{n}), 2, \vec{n})$, enzovoort, tot het gewenste argument bereikt is.
4. De minimalisatie van een berekenbare (partiële) functie f is berekenbaar (voor gegeven $\vec{n}$):
   - Begin met het bepalen van $g(0, \vec{n})$ Als $g(0, \vec{n}) = 0$, dan ben je klaar: $\mu g(\vec{n}) = 0$.
   - Als $g(0, \vec{n})$ daarentegen niet gedefinieerd is, dus $g(0, \vec{n})\uparrow$, ben je ook klaar: $\mu g(\vec{n})\uparrow$ (waarom?).
   - Als $g(0, \vec{n}) > 0$ bereken je $g(1, \vec{n})$, met weer deze drie mogelijkheden:
     - als $g(1, \vec{n}) = 0$ dan is $\mu g(\vec{n}) = 1$;
     - als $g(1, \vec{n})\uparrow$ dan is $\mu g(\vec{n})\uparrow$;
     - als $g(1, \vec{n}) > 0$ dan moet je verder en bereken je $g(2, \vec{n})$, enzovoort:
   - Als $g(m, \vec{n}) > 0$ voor alle $m < l$ en $g(l, \vec{n}) = 0$, dan is $\mu g(\vec{n}) = l$;
   - Als $g(m, \vec{n}) > 0$ voor alle $m < l$ en $g(l, \vec{n})\uparrow$, dan is $\mu g(\vec{n})\uparrow$;
   - Als $g(l, \vec{n}) > 0$ voor alle l, blijf je eeuwig zoeken naar het nulpunt en geldt eveneens $\mu g(\vec{n})\uparrow$.

Om te bewijzen dat omgekeerd een berekenbare functie f^p_P (voor een *gegeven* programma P en $p \in \mathbb{N}$) partieel recursief is, voeren we eerst de volgende functies $\rho_k : \mathbb{N}^{p+1} \to \mathbb{N}$ in, voor iedere $k \in \mathbb{N}$:

---

1. Zie bijv. het boek van Cutland voor een volledig bewijs. Het geven van een dergelijke bewijsschets is overigens heel gebruikelijk in de literatuur over berekenbaarheid: je geeft niet de programma's zelf, maar een overduidelijk systematische aanpak die met extra werk makkelijk in een programma kan worden omgezet.
2. In het algemene geval (10.1) worden eerst l verschillende segmenten in het geheugen gemaakt d.m.v. (9.1) met $p \rightsquigarrow l$: het eerste segment S_1 bestaat uit alle R_k met $k \in \tau_l(n, 1, \ldots, 1)$, het tweede uit alle R_k met $k \in \tau_l(1, n + 1, \ldots, 1)$, …, en het laatste segment S_l bestaat uit alle R_k met $k \in \tau_l(1, 1, \ldots, n + l - 1)$, $n = \{1, 2, 3, \ldots\}$, steeds met $n = \{1, 2, 3, \ldots\}$. Dan worden achter elkaar h_i voor $i = 1, \ldots, l$ binnen segment S_i uitgerekend door omlabeling van de geheugenplaatsen in het programma P_{h_i}. Daarna worden de antwoorden geschreven naar R_1 t/m R_l, worden alle volgende registers schoongeveegd, en begint P_g.

- Voor $k = 0$ is $\rho_0(n_0, \vec{n})$ het nummer van de regel die na n_0 stappen op input $\vec{n}$ is bereikt;[3]
- Voor $k > 0$ is $\rho_k(n_0, \vec{n})$ de inhoud m_k van register R_k na n_0 stappen op input $\vec{n}$.

Uit deze definities volgen enige eigenschappen, waarvan vooral de laatste belangrijk is:

$$\begin{aligned} \rho_0(0, \vec{n}) &= 1; && (11.1)\\ \rho_k(0, \vec{n}) &= n_k \ (1 \leq k \leq p); && (11.2)\\ \rho_k(0, \vec{n}) &= 0 \ (k > p); && (11.3)\\ \rho_1(\mu\rho_0(\vec{n}), \vec{n}) &= f_P^p(\vec{n}). && (11.4) \end{aligned}$$

(11.1) geldt: het programma begint (na nul stappen) per definitie bij P_1, met nummer 1 dus.

(13.3) geldt: de n_k zijn de beginwaarden van R_k.

(11.3) geldt: per definitie zijn bij de berekening van f_P^p de registers R_k hoger dan $k = p$ leeg.

(11.4) geldt: als het programma na n_0 stappen voor het eerst regel P_0 bereikt op input $\vec{n}$, geldt per definitie $\mu\rho_0(\vec{n}) = n_0$. De inhoud van R_1 is dan de output, oftewel $f_P^p(\vec{n})$.

Als voorbeeld geven we de functies ρ_0 en ρ_1 voor het programma $P_1 = (1, 0, 1)$ met $p = 1$; dan rekent P de functie Z uit. Als $n_1 = 0$, dan doet P_1 niets met $m_1 = 0$ en springt P direct naar P_0, zodat $\rho_0(1, 0) = 0$ en $\rho_1(1, 0) = 0$. Als $n_1 = 1$ dan wordt m_1 op 0 gezet en blijft P in P_1, zodat $\rho_0(1, 1) = 0$ en $\rho_1(1, 1) = 1$. Maar dan treedt het vorige scenario in werking, zodat $\rho_0(2, 1) = 0$ en $\rho_1(2, 1) = 0$. Voor willekeurige $n_1 > 0$ blijft het programma n_1 keer in regel P_1 steken, waar het steeds de inhoud van R_1 met 1 vermindert, om daarna naar P_0 te springen; dan bevat R_1 het antwoord 0. Daaruit volgt $\rho_0(0, n) = 1$ voor alle n, $\rho_0(n_0, 0) = 0$ voor $n_0 > 0$, $\rho_0(n_0, n) = 1$ voor $n > 0$ en $0 \leq n_0 < n$ en $\rho_0(n_0, n) = 0$ voor $n_0 \geq n$, terwijl $\rho_1(n_0, n) = n - n_0$ voor $0 \leq n_0 \leq n$ en $\rho_0(n_0, n) = 0$ voor $n_0 \geq n$. Samengevat geeft dit

$$\begin{aligned} \rho_0(n_0, n_1) &= \delta_0(n_0 \dot{-} n); && (11.5)\\ \rho_1(n_0, n_1) &= n_1 \dot{-} n_0, && (11.6) \end{aligned}$$

waarbij de functie $\dot{-}$: $\mathbb{N}^2 \to \mathbb{N}$, genaamd *cut-off subtraction*, is gedefinieerd als $n_1 \dot{-} n_0 = n_1 - n_0$ als $n_1 \geq n_0$ en $n_1 \dot{-} n_0 = 0$ als $n_1 \leq n_0$. De functie $\delta_0 : \mathbb{N} \to \mathbb{N}$ was al in Opgave 10.1 d) ingevoerd als $\delta_0(0) = 1$ en $\delta_0(n) = 0$ voor $n > 0$, waar ook bewezen werd dat deze primitief recursief is. Op soortgelijke manier als in Opgave 10.1 c) volgt ook dat $\dot{-}$ primitief recursief is: de conclusie is dat ρ_0 en ρ_1 eveneens primitief recursief zijn.

Het punt is nu dat alle functies ρ_k *altijd*, i.e., voor ieder programma P, primitief recursief zijn. Om dat volgens Definitie 10.4 te bewijzen is het noodzakelijk om al deze functies samen te voegen in één enkele functie $C : \mathbb{N}^{p+1} \to \mathbb{N}$, genaamd de *configuratie* van de computer, d.m.v.

$$C(n_0, \vec{n}) = \prod_{k=0}^{n} \pi_k^{\rho_k(n_0, \vec{n})}, \tag{11.7}$$

waarbij $\pi_0, \pi_1, \pi_2, \ldots \equiv 2, 3, 5, \ldots$ de rij priemgetallen is. Uit de unieke ontbinding van een getal in priemfactoren volgt dat iedere $\rho_k(n_0, \vec{n})$ uit het ene getal $C(n_0, \vec{n})$ te reconstrueren is, en zonder bewijs stellen we dat zowel deze reconstructie als de 'codering' (11.7) *primitief recursieve functies* zijn.[4] Een *update* $C(n_0, \vec{n}) \mapsto C(n_0 + 1, \vec{n})$ van de configuratie bestaat dan uit de volgende drie stappen:

1. Reconstructie van de getallen $\rho_0(n_0, \vec{n}), \rho_1(n_0, \vec{n}), \rho_2(n_0, \vec{n}), \ldots$ uit (11.7);
2. Toepassen van de regel op regel no. $\rho_0(n_0, \vec{n})$ op de zojuist bepaalde waarden $\rho_k(n_0, \vec{n})$, $k = 1, 2, \ldots$, geïnterpreteerd als de inhouden van de registers R_k na n_0 stappen op input $\vec{n}$;
3. Berekening van $C(n_0 + 1, \vec{n})$ via (11.7) uit de nieuwe waarden $\rho_k(n_0 + 1, \vec{n})$, $k = 0, 1, 2, \ldots$.

---

3. Als het programma op input $\vec{n}$ al na minder dan n_0 stappen gestopt is, dan geldt $\rho_0(n_0, \vec{n}) = 0$. In de volgende regel geldt in die situatie iets analoogs: voor $k > 0$ is $\rho_k(n_0, \vec{n})$ in dat geval gelijk aan de inhoud m_k van register R_k op het moment dat de *halting state* P_0 is bereikt. Het bewijs functioneert echter ook als de functies ρ_k in deze situatie niet zijn gedefinieerd in $(n_0, \vec{n})$.

4. Zie bijv. *Computability: Computable Functions, Logic, and the Foundations of Mathematics* door R. Epstein en W. Carnielli (Wadsworth & Brooks/Cole, 1989) of *Computability and Logic* door G. Boolos, J. Burgess, en R. Jeffrey (Cambridge, 2007).

Omdat de stappen 1 en 3 zoals gezegd primitief recursief zijn en stap 2 berust op de in alle opzichten uiterst primitieve (en i.h.b. lokale) werking van het programma P, volgt (conceptueel duidelijk maar toch nog met enig werk) dat er een primitief recursieve functie $h_P : \mathbb{N} \to \mathbb{N}$ bestaat zodat

$$C(n_0 + 1, \vec{n}) = h_P(C(n_0, \vec{n})). \tag{11.8}$$

De reden voor het invoeren van C is nu hopelijk duidelijk: vergelijking (11.8) is van de vereiste vorm (10.2) - (10.3) voor recursie, en wel met $f = C$ en $h = h_P \circ P^1_{p+2}$, en beginwaarde $g(\vec{n}) = 2 \prod_{k=1}^{n} \pi_k^{n_k}$.

We weten nu dus dat C primitief recursief is, en daarmee ook alle functies ρ_k (die primitief recursief uit C verkregen worden). We gebruiken dit eerst voor ρ_0, waardoor de minimalisatie $\mu\rho_0$ partieel recursief is (vgl. Definitie 10.4). Vervolgens is ρ_1 primitief recursief, zodat de samenstelling $\vec{n} \mapsto \rho_1(\mu\rho_0(\vec{n}), \vec{n})$ partieel recursief is (zie opgave). Maar daarmee is f^p_P volgens (11.4) eveneens partieel recursief. Q.E.D.

Je ziet uit dit bewijs dat f^p_P een (totale) functie is desda de minimalisatie $\mu\rho_0$ van een totale tot een totale functie leidt, en dat is het geval desda de *halting state* wordt bereikt. In dat geval is de functiewaarde $f^p_P(\vec{n})$ gedefinieerd, en anders niet!

Opgave 11.1

Welke functies moet je kiezen voor g, h en χ in (10.11) opdat het linkerlid van (11.4) van die vorm is?

Opgave 11.2

a) Bereken de functies ρ_0 en ρ_1 voor het programma $P_1 = (1, 0)$ (dat de functie S uitrekent) en $p = 1$.

b) Laat zien dat deze functies primitief recursief zijn.

12

Gödel-codering

De definitie (11.7) van de configuratie van een registermachine is een speciaal geval van een techniek die rond 1930 door het genie Kurt Gödel werd ingevoerd en die vele belangrijke toepassingen heeft. In dit college zijn dat de constructie van universele computers, de daarmee nauw samenhangende oplossing van het *Halting Problem* van Alan Turing, en de codering van logische systemen en formele bewijzen door natuurlijke getallen. Deze inzichten zullen ons ten slotte leiden tot de beroemde onvolledigheidsstellingen van Gödel (die echter ook zonder een beroep op universele computers kunnen worden bewezen, hetgeen de historische gang van zaken was).

De techniek van Gödel-codering kan worden losgelaten in de volgende algemene situatie:

- Er is een *alfabet*, i.e., een lijst symbolen of *letters* $\sigma_1, \sigma_2, \ldots$ (eindig of hoogstens aftelbaar).
- Daaruit ontstaan *woorden*, i.e., eindig veel achter elkaar geplaatste symbolen $w = \sigma_{i_1} \cdots \sigma_{i_m}$.
- Daaruit ontstaan *zinnen* van eindig veel achter elkaar geplaatste woorden $Z = (w_1, w_2, \ldots)$.
- Uit zinnen kun je weer hoofdstukken maken, daaruit boeken, daaruit bibliotheken ...

Ieder te coderen systeem of 'taal' heeft speciale regels voor de vorming van woorden, zinnen, enz. uit het vorige niveau. We illustreren de abstracte procedure van Gödel-codering met twee voorbeelden:

1. De codering van programma's op een registermachine door natuurlijke getallen;
2. De codering van het logische systeem **PA** door natuurlijke getallen.

Voor deze twee voorbeelden zijn de eerste drie niveaus afdoende.

1. Bij de codering van programma's op een registermachine zijn:
   - de symbolen σ_n de gehele getallen $n-1$ (die hier toevallig al in numerieke vorm staan);
   - de woorden regels, dus $kp_+ \equiv (k, p_+)$ met twee letters of $kp_0p_- \equiv (k, p_0, p_-)$ met drie letters;
   - de zinnen de programma's P gezien als opeenvolging van instructies als boven.[1]
2. Bij de codering van **PA** zijn:
   - de symbolen (willekeurig) gedefinieerd als $\sigma_1 \equiv \neg$, $\sigma_2 \equiv \rightarrow$, $\sigma_3 \equiv \forall$, $\sigma_5 \equiv ($, $\sigma_6 \equiv)$, $\sigma_7 \equiv =$, $\sigma_8 \equiv S$, $\sigma_9 \equiv +$, $\sigma_{10} \equiv \times$, $\sigma_{11} \equiv \mathbf{0}$, $\sigma_{12} \equiv x$, $\sigma_{13} \equiv x_1$, $\sigma_{14} \equiv x_2$, ..., $\sigma_{12+i} \equiv x_i$, etc.[2]
   - de woorden termen of formules (inclusief uitspraken);
   - de zinnen achter elkaar geplaatste woorden.

Het belangrijkste voorbeeld van een zin in **PA** is een *bewijs* $(\varphi_1, \varphi_2, \ldots)$, waarbij iedere formule φ_i uit de axioma's en voorgaande formules φ_j $(j < i)$ van de lijst kan worden afgeleid met behulp van de regels van **PA**, en het laatste woord van het bericht de te bewijzen uitspraak is.

In het vervolg is $(\pi_1, \pi_2, \pi_3, \ldots) \equiv (2, 3, 5, \ldots)$ weer de rij priemgetallen. De codering verloopt als volgt:

(i) het symbool σ_k krijgt code (of '*Gödel-getal*') $G(\sigma_k) = 2k + 1$;

(ii) het woord $w = \sigma_{i_1} \cdots \sigma_{i_m}$ krijgt code $G(w) = \prod_{l=1}^{m} \pi_l^{G(\sigma_{i_l})}$;

(iii) De zin $Z = (w_1, w_2, \ldots, w_n)$ ten slotte krijgt code

$$G(Z) = \prod_{j=1}^{n} \pi_j^{G(w_j)}. \tag{12.1}$$

1. De *halting* instructie P_0 komt in ieder programma voor en hoeft dus niet opgenomen of gecodeerd te worden.
2. Het aantal symbolen in **PA** is aftelbaar oneindig omdat het aantal variabelen in **PA** (als eerste-orde taal) aftelbaar is.

Voor een programma op een registermachine betekent dit dus:

- De getallen $n = \sigma_{n+1}$ worden gecodeerd door $G(n) = G(\sigma_{n+1}) = 2n + 3$.
- De coderingen van de mogelijke woorden, de regels van een programma dus, zijn

$$G(k, p_+) = 2^{2k+3} \cdot 3^{2p_+ +3}; \tag{12.2}$$
$$G(k, p_0, p_-) = 2^{2k+3} \cdot 3^{2p_0+3} \cdot 5^{2p_- +3}. \tag{12.3}$$

- Een programma P bestaande uit N regels P_1 t/m P_N wordt ten slotte gecodeerd door

$$G(P) = \prod_{j=1}^{N} \pi_j^{G(P_j)}. \tag{12.4}$$

Je kunt een enkel symbool σ_k als letter opvatten, maar ook als een woord dat slechts uit dat ene symbool bestaat, of zelfs als een zin met één woord dat uit die ene letter bestaat (enzovoort). De Gödel-codering maakt daar een verschil tussen, en meer in het algemeen kan van ieder getal worden vastgesteld van wat voor structuur (i.e., letter, woord, bericht, ...) het de code is. De code van σ_k is namelijk:

- als *letter* $2k + 1$, hetgeen een oneven getal is (zoals bij iedere letter);
- als *woord* 2^{2k+1}, wat even is met een oneven exponent van 2 (zoals bij ieder woord);
- als *bericht* $2^{2^{2k+1}}$, wat even is met een even exponent van 2 (zoals bij iedere zin).

Wat is nu de bedoeling van deze operatie? We leggen dit uit voor een programma.

1. De afbeelding $P \mapsto G(P)$ van de verzameling van alle mogelijke programma's (op een registermachine) naar $\mathbb{N}$ is injectief, m.a.w., ieder programma krijgt een uniek Gödel-getal toegewezen. Deze toewijzing is algoritmisch of berekenbaar en kan dus door een computer worden uitgevoerd.
2. Omgekeerd kan P uit $G(P)$ worden gereconstrueerd d.m.v. de hoofdstelling van de rekenkunde:
   (a) De unieke priemfactorisatie van $G(P)$ geeft een geordende lijst getallen $G(P_1)$ t/m $G(P_N)$; het aantal regels N is het aantal priemgetallen dat in de factorisatie van $G(P)$ voorkomt.
   (b) Ieder van deze getallen $G(P_i)$ heeft de vorm (12.2) of (12.3): in het laatste geval bevat $G(P_i)$ een factor 5 en in het eerste niet.[3] Opnieuw toepassen van de hoofdstelling geeft uit $G(P_i)$ ofwel twee getallen (n_1, n_2) ofwel drie getallen (n_1, n_2, n_3).
   (c) Omdat ofwel $(n_1 = 2k + 3, n_2 = 2p_+ + 3)$ ofwel $(n_1 = 2k + 3, n_2 = 2p_0 + 3, n_3 = 2p_- + 3)$ voor zekere getallen (k, p_+) resp. (k, p_0, p_-), kunnen deze laatste worden gereconstrueerd als $k = (n_1 - 3)/2$ enzovoort.

Het ene getal $G(P)$ bevat dus alle informatie over het hele programma P! Navenant kun je bijvoorbeeld de inhoud van alle boeken ter wereld (gezien als bibliotheek) door één enkel getal coderen, en de inhoud daarvan door een computer laten decoderen. En deze operaties zijn bovendien berekenbaar:

Stelling 12.1 *Voor een gegeven 'taal' zijn zowel de codering van een symbool (indien al numeriek),*[4] *woord, zin, etc., als de reconstructie of 'decodering' van bijvoorbeeld een zin Z (in al haar facetten, dus als geordende lijst van woorden die weer een geordende lijst van letters zijn) uit $G(Z)$, berekenbaar.*

Dit volgt uit een lemma dat we zonder bewijs geven en de implicatie primitief recursief $\Rightarrow$ berekenbaar:

Lemma 12.1 *1. De functies $f : \mathbb{N}^p \to \mathbb{N}$ met $f(n_1, \ldots, n_p) = \prod_{j=1}^{p} \pi_j^{n_j}$ zijn alle primitief recursief.*

2. De functies $f_j : \mathbb{N} \to \mathbb{N}$ die $n = \prod_j \pi_j^{n_j}$ afbeelden op $f_j(n) = n_j$ zijn alle primitief recursief.

Ook de vraag of een gegeven getal $n \in \mathbb{N}$ de codering is van een woord, letter, zin, enz. (en zo ja, van welke van deze mogelijkheden van toepassing is), is berekenbaar. Om dit precies te maken een definitie.

Definitie 12.1 *Een verzameling $S \subset \mathbb{N}$ van natuurlijke getallen heet* berekenbaar *als de karakteristieke functie χ_S berekenbaar is (waarbij $\chi_S(n) = 1$ als $n \in S$ en $\chi_S(n) = 0$ als $n \notin S$).*

3. Let op hoe belangrijk het hierbij is dat $p = 0$ niet door zichzelf gecodeerd wordt (maar door 1)!
4. Het omzetten van symbolen in getallen is niet berekenbaar in technische zin, omdat symbolen nog geen getallen zijn, maar ook die stap is in informele zin uiteraard algoritmisch uit te voeren.

Dit is een bijzondere eigenschap: we zullen later in zien dat het aantal berekenbare functies aftelbaar is. Het aantal berekenbaar deelverzamelingen van $\mathbb{N}$ moet dus ook aftelbaar zijn. Omdat het totale aantal deelverzamelingen van $\mathbb{N}$ overaftelbaar is, is de overweldigende meerderheid van deelverzamelingen van $\mathbb{N}$ dus niet berekenbaar! Maar met die meerderheid krijg je zelden te maken. Integendeel:

Stelling 12.2 *De verzameling $\mathcal{G}_\mathcal{P} = \{G(P) \mid P \in \mathcal{P}\}$, waarbij $\mathcal{P}$ de verzameling is van alle mogelijke programma's P op een registermachine, is berekenbaar.*

Deze verzameling is zelfs primitief recursief, in de zin dat χ_S dat is. We hebben dit resultaat nodig in het volgende hoofdstuk, maar er zijn vele vergelijkbare stellingen over bijv. **PA**.

Opgave 12.1

Je ziet dat de techniek van Gödel-codering algemeen toepasbaar is op symbolische talen. Stel bijvoorbeeld dat $\sigma_1, \ldots \sigma_{27}$ de 26 letters van het alfabet zijn, gevolgd door een vraagteken. Codeer het bericht $B =$ *wat is wiskunde?* en geef een schatting van de orde van grootte van $G(B)$.

Opgave 12.2

De Gödel-codering G zoals boven behandeld is gebaseerd op de unieke priemfactorisatie

$$n = \prod_l \pi_j^{n_j}, \tag{12.5}$$

van natuurlijke getallen n. Een alternatieve codering H ontstaat door uit te gaan van de unieke binaire representatie van n, dus

$$n = \sum_j 2^{n'_j}. \tag{12.6}$$

Ook dan geldt dat de codering en decodering primitief recursief zijn.

Geef aan hoe de codering H van een programma op een registermachine verloopt en geef i.h.b. een analogon van (12.2) t/m (12.4).

Opgave 12.3

Voor de liefhebbers, wordt nagekeken en telt alleen mee als bonus.
Bedenk zelf een berekenbare codering in dezelfde situatie waar de Gödel-codering voor bedoeld is (dus letters, woorden, zinnen, enzovoort). Geef ook de bijbehorende decodering.

13

Universele computers

In dit hoofdstuk laten we zien hoe de Gödel-codering leidt tot het idee van een universele computer. Hierbij is het van groot belang dat je een systematische lijst (i.e. opsomming) van alle programma's op een registermachine (of een willekeurige computer) kunt maken. Dit is mogelijk via de Gödel-codering, zoals we nu zullen laten zien. Daar is wel wat voorwerk voor nodig. Eerst een definitie.

Definitie 13.1 *Een verzameling $S \subset \mathbb{N}$ van natuurlijke getallen heet* recursief opsombaar *(*recursively enumerable*, afgekort als r.e.) als er een totale berekenbare functie $\varphi : \mathbb{N} \to \mathbb{N}$ bestaat met als beeld S.*

Een recursief opsombare deelverzameling van $\mathbb{N}$ is dus van de vorm $S = \varphi(\mathbb{N}) = \{\varphi(0), \varphi(1), \ldots\}$ met φ berekenbaar. De bijbehorende opsomming van S is dan uiteraard de geordende lijst $(\varphi(0), \varphi(1), \ldots)$, dikwijls ook geschreven als $(n_0, n_1, \ldots)$ met $n_k = \varphi(k)$. Let op: omdat niet wordt geëist dat φ injectief is, kan deze opsomming herhalingen bevatten, ook als S oneindig is (sommige of zelfs alle elementen van S kunnen zelfs oneindig vaak voorkomen in de opsomming).

De even getallen zijn bijvoorbeeld recursief opsombaar: neem $\varphi(n) = 2n$. Ook de verzameling priemgetallen blijkt recursief opsombaar. Recursieve opsombaarheid is zwakker dan berekenbaarheid:

Stelling 13.1 *Een verzameling $S \subset \mathbb{N}$ is berekenbaar desda zowel S als S^c recursief opsombaar zijn.*

Hier is S^c het complement van S. We nemen aan dat S een oneindige verzameling is: zo niet, dan is S automatisch berekenbaar (alle operaties op een eindige verzameling zijn berekenbaar). We geven een informele bewijsschets (zie Opgave 14.3 voor een precies bewijs). Stel dat we berekenbare opsommingen $\varphi : \mathbb{N} \to S$ en $\varphi^c : S^c \to \mathbb{N}$ hebben. Om te kijken om een gegeven n in S of in S^c ligt, hoeven we slechts om en om twee *eindige* lijsten $(\varphi(k))_k$ en $(\varphi(k'))_{k'}$ na te lopen, in de volgorde $(\varphi(0), \varphi^c(0), \varphi(1), \varphi^c(1), \ldots)$: de gekozen n komt gegarandeerd op één van de twee lijsten voor en wordt dus na eindig veel stappen gevonden. Als $n = \varphi(k)$ voor zekere k geldt $n \in S$ en dus $\chi_S(n) = 1$, en als $n = \varphi(k')$ volgt $\chi_S(n) = 0$. Omdat zowel φ als φ^c berekenbaar zijn, is dit een berekenbare procedure.

Omgekeerd geeft χ_S systematisch een *injectieve* functie $\varphi : \mathbb{N} \to \mathbb{N}$ met beeld S: om $\varphi(0)$ te bepalen pas je χ_S toe op alle getallen vanaf 0 tot je een n_0 hebt gevonden met $\chi_S(n_0) = 1$. Dit is een eindig proces (anders zou S leeg zijn). Dan kies je $\varphi(0) = n_0$. Vervolgens bepaal je $\varphi(1)$ op dezelfde manier, nu te beginnen bij $n_0 + 1$: de kleinste $n_1 > n_0$ met $\chi_S(n_1)$ is per definitie $\varphi(1)$. Enzovoort. Op dezelfde manier construeer je φ^c. Q.E.D.

Gevolg 13.1 *Als een oneindige deelverzameling $S \subset \mathbb{N}$ berekenbaar is, bestaat er een recursieve opsomming van S zonder herhalingen (i.e., een injectieve berekenbare functie $\varphi : \mathbb{N} \to \mathbb{N}$ met beeld S).*

Dit volgt uit het bewijs van de implicatie: S berekenbaar $\Rightarrow$ S recursief opsombaar in Stelling 13.1. Q.E.D.

De even getallen en de priemgetallen blijken berekenbaar te zijn. We zullen later voorbeelden zien van verzamelingen die wel recursief opsombaar zijn maar niet berekenbaar; deze zijn zelfs van groot belang!

We zouden ook graag definiëren wat een recursieve opsomming van een willekeurige (aftelbare) verzameling X is, niet noodzakelijk bestaand uit getallen. Dat zou zo iets moeten zijn als een berekenbare surjectieve functie $\varphi : \mathbb{N} \to X$, alleen weten we niet wat 'berekenbaar' hier inhoudt. De situatie is echter gunstig als er een injectieve functie $G : X \to \mathbb{N}$ bestaat, zodat $G(X) \subset \mathbb{N}$ feitelijk een kopie van X in de natuurlijke getallen is. Hierbij gaan we er vanuit dat deze functie G informeel algoritmisch berekenbaar

is.[1] In dat geval kunnen we de bovenstaande definities en constructies eenvoudig toepassen op $G(Y)$. Denk bij X aan een taal, zoals in het vorige hoofdstuk, i.h.b. aan de verzameling $\mathcal{P}$ van alle programma's P op registermachines, en denk bij G aan de Gödel-codering daarvan. Als $G(X)$ berekenbaar is, is de situatie helemaal perfect: in dat geval krijgen we een opsomming van X zonder herhalingen. Er is dan volgens Gevolg (13.1) namelijk een berekenbare injectie $\varphi : \mathbb{N} \to \mathbb{N}$ met $\varphi(\mathbb{N}) = G(X)$. Dit geeft een opsomming $(x_0, x_1, \ldots)$ van X met $G(x_k) = \varphi(k)$. Deze opsomming heeft geen herhalingen en is recursief in de zin dat φ berekenbaar is. Ons belangrijkste voorbeeld van deze constructie is:

Stelling 13.2 *De verzameling $\mathcal{P}$ van alle programma's op een registermachine is recursief opsombaar zonder herhalingen, zeg $\mathcal{P} = (P_{(0)}, P_{(1)}, P_{(2)}, \ldots)$.*

Let op: omdat P_k al regel no. k van programma P was, gebruiken we voor de opsomming $P_{(k)}$ in plaats van P_k. Deze stelling volgt direct uit Stelling 12.2 en het bovenstaande verhaal. Q.E.D.

Gevolg 13.2 *Voor iedere p bestaat er een recursieve opsomming $(\phi_0, \phi_1, \phi_2, \ldots)$ van $\mathcal{F}_p$. In het bijzonder is de verzameling $\mathcal{F}_p$ van alle berekenbare functies $f : \mathbb{N}^p \to \mathbb{N}$ aftelbaar.*

Bij een berekenbare functie $f : \mathbb{N}^p \to \mathbb{N}$ hoort per definitie minstens één programma P zodat $f = f^p_P$. De berekenbare lijst $(\phi_0, \phi_1, \ldots)$ met $\phi_e = f^p_{P_{(e)}}$ bevat dus alle berekenbare functies $f : \mathbb{N}^p \to \mathbb{N}$. Q.E.D.

Deze lijst bevat (i.t.t. $(P_{(0)}, P_{(1)}, P_{(2)}, \ldots)$) wel herhalingen: er zullen immers meerdere programma's zijn die dezelfde functie berekenen). Het blijkt zelfs dat iedere functie oneindig vaak voorkomt.[2]

Stelling 13.3 *Gegeven de lijst $(\phi_0, \phi_1, \ldots)$ van alle berekenbare functies $f : \mathbb{N}^p \to \mathbb{N}$ uit Gevolg 13.2, is de 'universele' partiële functie $U_p : \mathbb{N}^{p+1} \to \mathbb{N}$ gegeven door*

$$U_p(e, \vec{n}) = \phi_e(\vec{n}), \tag{13.1}$$

berekenbaar (de notatie $(e, n) \in \mathbb{N}^2$ i.p.v. $(n_0, \vec{n})$ is traditioneel in deze context).

We geven een bewijsschets. We weten dat ϕ_e (per definitie) wordt uitgerekend door het programma $P_{(e)}$. We definiëren nu naar analogie van het bewijs van Stelling 11.1 de volgende functies $\tilde{\rho}_k : \mathbb{N}^{p+2} \to \mathbb{N}$, voor iedere $k \in \mathbb{N}$, maar nu met $P = P_{(e)}$, dus:

- $\tilde{\rho}_0(n_0, \vec{n}, e)$ is het nummer van de regel van $P_{(e)}$ die na n_0 stappen op input $\vec{n}$ door $P_{(e)}$ is bereikt;
- $\tilde{\rho}_k(n_0, \vec{n}, e)$ voor $k > 0$ is de inhoud m_k van R_k na n_0 stappen door $P_{(e)}$ op input $\vec{n}$.

Analoog krijgt de functie C, nu geheten $\tilde{C}$, een extra argument e. Het kardinale punt is nu dat er opnieuw een primitief recursieve functie $\tilde{h} : \mathbb{N}^{p+2} \to \mathbb{N}$ bestaat zodanig dat naar analogie van (11.8) geldt

$$\tilde{C}(n_0 + 1, \vec{n}, e) = \tilde{h}(\tilde{C}(n_0, \vec{n}), e). \tag{13.2}$$

Het feit dat $\tilde{h}$ primitief recursief is, is een gevolg van het feit dat het programma $P_{(e)}$ berekenbaar kan worden gereconstrueerd uit e: ten eerste volgt de Gödel-codering $G(P_{(e)}) = \varphi(e)$ uit e via de berekenbare functie φ die volgens Stelling 13.2 bestaat, en ten tweede volgt $P_{(e)}$ berekenbaar uit $G(P_{(e)})$ via Gödel-decodering. Uit (13.2) volgt opnieuw dat $\tilde{C}$ primitief recursief is, en daar weer uit (vgl. Lemma 12.1) dat alle functies $\tilde{\rho}_k$ dat eveneens zijn. Ten slotte volgt uit het analogon van (11.4), namelijk

$$U_p(e, \vec{n}) = \tilde{\rho}_1(\mu\tilde{\rho}_0(\vec{n}), \vec{n}, e), \tag{13.3}$$

dat U_p partieel recursief en dus berekenbaar is. Q.E.D.

Omdat U_p berekenbaar is, is er per definitie dus een 'universeel' programma $\mathcal{P}_p$ met $U_p = f^{p+1}_{\mathcal{P}_p}$ dat al deze functies uit kan rekenen, terwijl we gewend waren dat één programma P voor iedere p ook slechts één functie $f : \mathbb{N}^p \to \mathbb{N}$ uit kan rekenen. In feite is het voldoende dat dit voor $p = 1$ kan, zie opgave.

---

1. We kunnen dit niet formeler zeggen omdat X meestal niet al direct is gegeven als verzameling getallen.
2. Het is mogelijk om deze lijst op berekenbare wijze te reduceren tot een berekenbare lijst $(\phi_0, \phi_1, \ldots)$ zonder herhalingen. Zie bijv. R.M. Friedberg, Three theorems on recursive enumeration, *J. Symbolic Logic* 23, 309–316 (1958). Een ander bewijs dat dit mogelijk is gaat uit van Stelling 11.1 en geeft dan een berekenbare opsomming van de partieel recursieve functies. Zie bijv. S.A. Terwijn, *Syllabus Computability Theory*, `www.math.ru.nl/~terwijn/publications/syllabus.ps`.

Stelling 13.3 (voor Turing Machines i.p.v. registermachines) was het theoretische basisidee achter de universele computer, ook wel genaamd *stored program computer* (wat weer nauw gerelateerd is aan de zgn. *von Neumann architectuur* van moderne computers). Daarbij is er geen principieel verschil tussen programma's en data: een programma is via zijn code ook zelf een vorm van data en beide kunnen in het geheugen worden opgeslagen en door de CPU worden verwerkt. We hebben de moderne computer dan ook niet te danken aan zakenmannetjes als Steve Jobs en Bill Gates maar aan wiskundigen als Hilbert en Gödel (die door middel van hun werk aan logica en bewijstheorie alleen theoretisch en indirect, maar dan wel op beslissende wijze aan de ontwikkeling van computers bijdroegen) en met name aan Turing en von Neumann (die beiden niet alleen baanbrekend theoretisch werk deden, met name de eerste, maar zelf ook werkende computers bouwden).

Stelling 13.3 is dus van groot historisch belang vanwege haar inspirerende rol voor de informatica. Je ziet hoe belangrijk het idee van de Gödel-codering is: zonder een dergelijke constructie is het niet mogelijk zelfs maar de definitie te geven van een berekenbare opsomming van programma's of functies, laat staan van een universele functie of computer.

Opgave 13.1

Laat precies zien hoe een (berekenbare) functie $f^{(p)} : \mathbb{N}^p \to \mathbb{N}$ via de (berekenbare) injectie τ_p in (9.1) kan worden omgetoverd in een (berekenbare) functie $f : \mathbb{N} \to \mathbb{N}$ (en let daarbij goed op het domein). Laat vervolgens zien hoe het programma $\mathcal{P}_1$ alle berekenbare functies kan uitrekenen.

Opgave 13.2

Definieer $S \subset \mathbb{N}$ als $n \in S$ desda ϕ_n totaal (i.e. overal gedefinieerd) is. Hierbij is $(\phi_0, \phi_1, \ldots)$ de opsomming van berekenbare functies $f : \mathbb{N} \to \mathbb{N}$ uit Gevolg 13.2 met $p = 1$.
Laat zien dat S niet berekenbaar is.

Hint: Bekijk de functie $f : \mathbb{N} \to \mathbb{N}$ gegeven door $f(n) = \phi_n(n) + 1$ als ϕ_n totaal is en $f(n) = 0$ als ϕ_n niet totaal is. Is f berekenbaar? Relateer f aan χ_S en aan U_1 en leid een tegenspraak af uit de aanname dat χ_S berekenbaar is.

14

Turing's Halting Theorem

In dit hoofdstuk leiden we een beroemde stelling af over (on)berekenbaarheid, het *Halting Theorem* van Turing. Met deze stelling loste Turing het *Entscheidungsproblem* van Hilbert (in negatieve zin) op en bovendien gaf de stelling zowel historisch as inhoudelijk gesproken een nieuwe (voor ons de eerste) manier om naar de (eerste) Onvolledigheidsstelling van Gödel te kijken, zoals we zullen zien.

Essentieel in dit alles is het verschil tussen een *berekenbare* deelverzameling $S \subset \mathbb{N}$, waarvan per definitie de karakteristieke functie χ_S berekenbaar is (zie Definitie 12.1), en een *recursief opsombare* deelverzameling $S \subset \mathbb{N}$, die per definitie het beeld is van een totale berekenbare functie φ (vgl. Definitie 13.1). Deze definities kunnen worden uitgebreid tot deelverzamelingen van $\mathbb{N}^p$ voor $p > 1$; zo zeggen we dat $R \subset \mathbb{N}^2$ berekenbaar is als χ_R dat is. Naast de karakteristieke functie χ_S van S, die uiteraard totaal is, blijkt het handig te zijn om de partiële functie $\tilde{\chi}_S : \mathbb{N} \to \mathbb{N}$ in te voeren, gegeven door

$$\tilde{\chi}_S(n) \quad = \quad 1 \text{ als } n \in S; \tag{14.1}$$

$$\tilde{\chi}_S(n) \quad \uparrow \quad \text{als } n \notin S. \tag{14.2}$$

Hieruit volgt dat $n \in S$ desda $n \in D(\tilde{\chi}_S)$, oftewel $S = D(\tilde{\chi}_S)$. Het volgende lemma is erg handig.[1]

Lemma 14.1 *De volgende eigenschappen van een deelverzameling $S \subset \mathbb{N}$ zijn equivalent:*

1. *S is recursief opsombaar;*
2. *$\tilde{\chi}_S$ is berekenbaar;*
3. *$S = D(f)$ voor een berekenbare functie $f : \mathbb{N} \to \mathbb{N}$;*
4. *Er is een berekenbare deelverzameling $R \subset \mathbb{N}^2$ zodat $n \in S$ desda $\exists_m(n, m) \in R$.*

$2 \Rightarrow 3$ is triviaal: neem $f = \tilde{\chi}_S$. Voor $3 \Rightarrow 2$, definieer $E : \mathbb{N} \to \mathbb{N}$ als $E(n) = 1$ voor alle n. Deze functie is (net als Z) berekenbaar. Dan is ook $\tilde{\chi}_S = E \circ f$ berekenbaar, met als domein $D(\tilde{\chi}_S) = D(E \circ f) = D(f)$.[2]

Om $4 \Rightarrow 3$ te bewijzen breiden we de μ-operatie uit van functies tot relaties, i.e., deelverzamelingen $R \subset \mathbb{N}^2$ (vgl. Opgave 10.2). Gegeven $R \subset \mathbb{N}^2$ definiëren we een partiële functie $\mu R : \mathbb{N} \to \mathbb{N}$ d.m.v.

$$\mu R(n) \quad = \quad \min\{m_0 \in \mathbb{N} \mid (n, m_0) \in R\}; \tag{14.3}$$

$$\mu R(n) \quad \uparrow \quad \text{als zo'n } m_0 \text{ niet bestaat.} \tag{14.4}$$

Een relatie wordt ook vaak als *zoekprobleem* aangeduid, omdat je bij gegeven n een m zoekt die voldoet aan $(m, n) \in R$ (vaak genoteerd als $R(m, n)$). Priemfactorisatie is bijvoorbeeld een zoekprobleem, waarbij R bestaat uit alle paren (n, m) waarbij m een priemfactor van n is. Dan is $\mu R(n)$ dus de kleinste priemfactor van n. Terug naar het bewijs: als $n \in S$ desda $\exists_m(n, m) \in R$, dan is $S = D(\mu R)$. In Opgave 10.2 is aangetoond dat als R berekenbaar is, μR dat ook is, en dus geldt $4 \Rightarrow 3$.

Voor $2 \Rightarrow 4$ kiezen we een programma P dat $\tilde{\chi}_S$ berekent, dus $\tilde{\chi}_S = f^1_P$. We definiëren nu de relatie: $(n, m) \in R$ desda P in hooguit m stappen $\tilde{\chi}_S(n)$ uitrekent. Als $n \notin D(\tilde{\chi}_S)$ zal dus $(n, m) \notin R$ voor alle m en omgekeerd bestaat zo'n m bij gegeven n als $n \in D(\tilde{\chi}_S)$. Dus $\{n \mid \exists_m(n, m) \in R\} = D(\tilde{\chi}_S) = S$. Het punt is dat R berekenbaar is door na te gaan of P na m stappen op input n nog aan de slag is: technisch gesproken kan dit door te kijken of $\rho_0(m, n) = 0$, zie hoofdstuk 11.[3] Hiermee is $2 \Rightarrow 4$ duidelijk.

---

1. We nemen stilzwijgend aan dat $S \neq \emptyset$ en $S \neq \mathbb{N}$ (i.e., $S^c \neq \emptyset$).
2. Stel dat in (10.1) de functies g en h_i partieel gedefinieerd zijn. Dan bestaat $D(f)$ per definitie uit de $\vec{n} \in \mathbb{N}^p$ die in $D(h_i)$ zitten voor alle i en waarvoor bovendien geldt dat $(h_1(\vec{n}), \ldots, h_l(\vec{n})) \in D(g)$. In het bovenstaande geval is $g = E$ totaal en $l = 1$, zodat $D(f) = D(h)$ met $f = g \circ h$.
3. De vraag of P ooit stopt is niet noodzakelijk berekenbaar, dat is precies wat het *Halting Theorem* straks gaat zeggen.

Nu met een soortgelijke truc $3 \Rightarrow 1$: stel dat f wordt berekend door P en definieer $g : \mathbb{N}^2 \to \mathbb{N}$ als

$$g(n,m) = n \text{ als } P \text{ in hooguit } m \text{ stappen } f(n) \text{ uitrekent;} \tag{14.5}$$
$$g(n,m) = n_0 \text{ (een willekeurig element van } S\text{) als dit niet zo is.} \tag{14.6}$$

Dan is g berekenbaar (zie vorige stap) en is $D(f) = R(g)$, het bereik van g (opgave). Dan maken we uit g een functie $\varphi : \mathbb{N} \to \mathbb{N}$ door $\varphi(n) = g((n)_1, (n)_2)$, waarbij $(n)_j = f_j(n)$ met f_j gedefinieerd in Lemma 12.1. Je ziet met enig nadenken (opgave) dat $R(\varphi) = R(g)$, zodat $S = D(f) = R(\varphi)$, en $3 \Rightarrow 1$ is rond.

Ten slotte $1 \Rightarrow 4$: stel $S = \varphi(\mathbb{N}) = R(\varphi)$, en definieer een relatie R door $(n,m) \in R$ als $n = \varphi(m)$. Deze relatie is berekenbaar omdat φ dat is en $1 \Rightarrow 4$ volgt. Q.E.D.

Vanuit de lijst $(\phi_0, \phi_1, \ldots)$ van berekenbare functies $f : \mathbb{N} \to \mathbb{N}$ (zei Stelling 13.3) maken we nu

$$K = \{n \in \mathbb{N} \mid n \in D(\phi_n)\} \equiv \{n \in \mathbb{N} \mid \phi_n(n)\downarrow\}. \tag{14.7}$$

een beroemde deelverzameling van $\mathbb{N}$.

Stelling 14.1 *De verzameling K is recursief opsombaar maar niet berekenbaar.*

Om de eerste claim te bewijzen definiëren we de 'diagonaal' $\Delta : \mathbb{N} \to \mathbb{N}^2$ door $\Delta(n) = (n,n)$. Deze functie is berekenbaar.[4] Dan volgt $K = D(U_1 \circ \Delta)$. Omdat U_1 berekenbaar is (Stelling 13.3) en Δ ook, is $U_1 \circ \Delta$ berekenbaar, en daarmee is K volgens Lemma 14.1.3 recursief opsombaar.

De tweede bewering over K volgt uit het ongerijmde. Als K berekenbaar is, is K^c recursief opsombaar (Steling 13.1) en is dus $\tilde{\chi}_{K^c}$ berekenbaar (Lemma 14.1.2). Omdat de lijst (ϕ_i) compleet is bestaat er een $m \in \mathbb{N}$ zodat $\tilde{\chi}_{K^c} = \phi_m$. We vragen ons nu af of $m \in K$. Zo ja, dan is $\phi_m(m)\downarrow$ per definitie van K maar tevens $\tilde{\chi}_{K^c}(m)\downarrow$ oftewel $m \in K_c$. Maar als $m \in K_c$ dan $\phi_m(m)\uparrow$ per definitie van K en tevens $\tilde{\chi}_{K^c}(m) = 1$ en dus $\phi_m(m)\downarrow$, opnieuw een tegenspraak. Daarmee is K niet berekenbaar. Q.E.D.

Het algemene *Halting Problem* gaat om de vraag of een computerprogramma P bij gegeven input $n \in \mathbb{N}$ stopt dan wel eeuwig doorloopt—met andere woorden, of $n \in D(f_P^1)$. Een oplossing van het *Halting Problem* is dan (bijvoorbeeld) een functie $h : \mathbb{N}^2 \to \mathbb{N}$ zodanig dat:

$$h(m,n) = 1 \text{ als } \phi_m(n)\downarrow, \text{ oftewel als } n \in D(\phi_m)\ ; \tag{14.8}$$
$$h(m,n) = 0 \text{ als } \phi_m(n)\uparrow, \text{ oftewel als } n \notin D(\phi_m)\ . \tag{14.9}$$

Deze functie geeft dus aan of $P_{(m)}$ al dan niet stopt op input $n \equiv (n,0,0,\ldots)$. Een *berekenbare* oplossing van het *Halting Problem* zou direct tot een bewijs van het Goldbach vermoeden leiden![5] Je kunt namelijk makkelijk een programma maken dat vanaf $k = 1$ nagaat of er priemgetallen p_1, p_2 bestaan zodat $2k = p_1 + p_2$; zo ja, dan gaat de machine verder met $k+1$; zo nee, dan stopt het programma (dat dan een tegenvoorbeeld tegen het Goldbach vermoeden heeft gevonden). Als het programma eeuwig doorloopt is het Goldbach vermoeden waar, en anders niet. Helaas pindakaas: nu komt het *Halting Theorem*!

Stelling 14.2 *Er bestaat geen* berekenbare *functie $h : \mathbb{N}^2 \to \mathbb{N}$ die voldoet aan* (14.8) - (14.9).

Als h berekenbaar was, dan zou $h \circ \Delta = \chi_K$, en daarmee K, dat ook zijn. Zie echter Stelling 14.1. Q.E.D.

Een ander leuk voorbeeld, dat in feite nauwelijks verschilt van (14.7), is de verzameling

$$D = \{n \in \mathbb{N} \mid n \in \phi_n(\mathbb{N})\}. \tag{14.10}$$

Stelling 14.3 *De verzameling D is recursief opsombaar maar niet berekenbaar.*

Het bewijs is een opgave.

Een diepe stelling van Matiyasevich zegt dat bij iedere recursief opsombare verzameling $S \subset \mathbb{N}$ een polynoom $p(n_0, \vec{n})$ in $p+1$ variabelen met coëfficiënten in $\mathbb{Z}$ kan worden gevonden zodanig dat $n_0 \in S$ desda de Diophantine vergelijking $p = 0$ een oplossing $(n_0, \vec{n}) \in \mathbb{N}^{p+1}$ heeft (oftewel: er bij gegeven n_0 een oplossing $\vec{n} \in \mathbb{N}^p$ bestaat).

4. We gebruiken hier (10.1) met $p = 1$, $l = 2$, $h = \Delta$ oftewel $h_1 = h_2 = \mathrm{id} \equiv \pi_1^1$ (i.e. $\mathrm{id}(n) = n$), en $g = U_1$.
5. Het *Goldbach vermoeden* is een onbewezen uitspraak uit de getaltheorie: is ieder even getal de som van twee priemgetallen?

Opgave 14.1

Bewijs Stelling 14.3.

Opgave 14.2

In het bewijs van de implicatie $3 \Rightarrow 1$ in Lemma 14.1 wordt beweerd dat $D(f) = R(g)$ en $R(\varphi) = R(g)$. Bewijs deze beweringen.

Opgave 14.3

Bewijs Stelling 13.1 op een nieuwe en preciezere manier met behulp van Lemma 14.1. Gebruik met name deel 2 daarvan als karakterisatie van recursief opsombare verzamelingen in het bewijs S berekenbaar $\Rightarrow S$ en S^c recursief opsombaar, en deel 4 in de omgekeerde richting. Deze omkering is overigens de moeilijke kant!

15

De (eerste) onvolledigheidsstelling van Gödel

Berekenbare functies hebben een onverwachte en spectaculaire toepassing op de theorie van bewijsbaarheid. We hebben al gezien dat er een *conceptueel* verschil is tussen bewijsbaarheid en waarheid. Beide begrippen slaan in eerste instantie op puur formele uitspraken φ (in ons geval in de taal van **PA** of van **ZF**), waarin allerlei abstracte symbolen voorkomen (zoals $\neg$, $\rightarrow$, $\forall$, $x, y, \ldots$, en $\mathbf{0}$, $+$, $\times$ resp. $\emptyset$, $\in$, $\ldots$).

- Bij de vraag of φ *bewijsbaar* is (m.a.w., een *stelling* is, zie hoofdstuk 4), genoteerd $\vdash \varphi$, hebben de symbolen geen betekenis, en ga je uitsluitend af op de axioma's en deductieregels. Het bewijzen is daarmee een symbolische aangelegenheid, die i.h.b. *berekenbaar* is.
- Bij het nagaan of φ *waar* is (zie resp. Definities 5.1 en 8.1), notatie $\vDash \varphi$, interpreteer je alle symbolen in φ zoals je dat gewend bent (namelijk in termen van natuurlijke getallen resp. verzamelingen). Een puur *formele* uitspraak in **PA** of **ZF** wordt zo een *concrete* uitspraak over getallen of verzamelingen, waarvan wij aanemen dat *deze waar of onwaar is* (of we dat nu weten of niet).

Niettemin werden de begrippen bewijsbaarheid en waarheid in de wiskunde van Euclides tot het einde van de 19e eeuw geïdentificerd. Daar was een goede reden voor, want voor zover het conceptuele verschil tussen bewijsbaarheid en waarheid al werd opgemerkt, dacht iedereen dat een uitspraak waar is desda zij bewijsbaar is. Zelfs Hilbert dacht dat! Wel zag hij als eerste in dat het samenvallen van ware en bewijsbare uitspraken bewezen moest worden. We brengen in herinnering dat in **PA** (en ook in **ZF**) een bewijsbare uitspraak altijd waar is: de domeinspecifieke axioma's zijn immers waar en de zuiver logische axioma's zetten ware uitspraken altijd om in ware uitspraken. Officieel heet dit principe

- *Correctheid*: als $\vdash \varphi$, oftewel φ is bewijsbaar, dan geldt dus ook $\vDash \varphi$, oftewel φ is waar.

Hier volgt uit dat **PA** en **ZF** *consistent* zijn, in de volgende zin:

Definitie 15.1 *Een logisch systeem heet* consistent *als er geen uitspraak φ (in de taal van dat systeem) bestaat zodat $\vdash \varphi$ en $\vdash \neg\varphi$ beide (binnen dat systeem) gelden.*[1]

Een correct maar inconsistent logisch systeem is onmogelijk (als we aannemen dat een uitspraak niet tegelijk waar en onwaar kan zijn). Consistentie is dus een zwakkere aanname dan correctheid.

Definitie 15.2 *Een uitspraak χ in een logisch systeem (zoals **PA** of **ZF**) heet* onbeslisbaar *(binnen dat systeem) als noch $\vdash \chi$ noch $\vdash \neg\chi$. M.a.w., χ kan niet worden bewezen, maar haar negatie $\neg\chi$ evenmin. Een logisch systeem dat minstens één onbeslisbare uitspraak bevat heet* onvolledig.

Nu komt de fameuze (eerste) onvolledigheidsstelling van Gödel, in twee equivalente versies:

Stelling 15.1 *1. Als **PA** (resp. **ZF**) consistent is, is **PA** (resp. **ZF**) onvolledig.*
*2. Als **PA** (resp. **ZF**) correct is, bestaan er ware maar onbewijsbare uitspraken in **PA** (resp. **ZF**).*

De eerste versie van de stelling (die Gödel zelf ook min of meer zo gaf) is puur syntactisch, de tweede mengt syntax met semantiek en spreekt meer tot de verbeelding. Niettemin zie je, gegeven de correctheid van **PA** (resp. **ZF**), snel in dat beide formuleringen equivalent zijn (opgave).
We gaan nu de tweede versie bewijzen volgens een methode à la Turing die aansluit op het vorige hoofdstuk;[2] Het originele bewijs van Gödel komt daarna. Een volledig bewijs van de stellingen van Gödel is bijvoorbeeld te vinden in Peter Smith, *An Introduction to Gödel's Theorems* (CUP, 2007).

1. Het volgt uit de axioma's van de eerste orde logica dat in een inconsistent systeem iedere uitspraak bewijsbaar is.
2. Ontleend aan M. Davis, The Incompleteness Theorem, *Notices of the* AMS 53, 414–418 (2006).

Stel $S \subset \mathbb{N}$ is recursief opsombaar. Dan is er volgens Lemma 14.1 een berekenbare verzameling $R \subset \mathbb{N}^2$ zodat $n \in S$ desda $\exists_m(n,m) \in R$. Het cruciale punt (zie Lemma 15.2 beneden) is nu dat omdat R berekenbaar is, er een formule ψ_R in **PA** (en dus ook in **ZF**) bestaat met de eigenschap dat

$$(n_1,n_2) \in R \quad \text{desda} \quad \vdash \psi_R(\mathbf{n}_1,\mathbf{n}_2); \tag{15.1}$$
$$(n_1,n_2) \notin R \quad \text{desda} \quad \vdash \neg\psi_R(\mathbf{n}_1,\mathbf{n}_2). \tag{15.2}$$

Uit de correctheid van **PA** volgt dat je deze condities ook zo kunt schrijven (zie opgave):

$$(n_1,n_2) \in R \quad \text{desda} \quad \vDash \psi_R(\mathbf{n}_1,\mathbf{n}_2); \tag{15.3}$$
$$(n_1,n_2) \notin R \quad \text{desda} \quad \vDash \neg\psi_R(\mathbf{n}_1,\mathbf{n}_2). \tag{15.4}$$

Bekijk nu voor iedere n de uitspraak

$$\chi_n \equiv \neg\exists_y \psi_R(\mathbf{n},y). \tag{15.5}$$

De interpretatie $[[\chi_n]]_{\mathbb{N}}$ van χ_n (in $\mathbb{N}$) is dat er geen m is zodat $\psi_R(n,m)$ (als uitspraak over natuurlijke getallen). Volgens (15.4) is dat zo desda er geen m is zodat $(n,m) \in R$. Omdat $n \in S$ desda er wél een m is zodat $(n,m) \in R$ (zie boven), is er geen m zodat $(n,m) \in R$ desda $n \notin S$. M.a.w., $\vDash \chi_n$ desda $n \notin S$.[3]

Lemma 15.1 *Als $S \subset \mathbb{N}$ recursief opsombaar is maar niet berekenbaar, dan bestaat er een $n \in \mathbb{N}$ zodat χ_n in* (15.5) *onbeslisbaar is en waar (i.e., $n \notin S$).*

De crux is dat de verzameling

$$\mathcal{X} = \{n \in \mathbb{N} \mid \vdash \chi_n\} \tag{15.6}$$

van alle n waarvoor χ_n bewijsbaar is (merk op dat $\mathcal{X} \subseteq S$), recursief opsombaar is. Dit is zo omdat:

1. de verzameling
$$\mathcal{S} = \{n \in \mathbb{N} \mid n = G(\varphi),\ \varphi \text{ is een stelling}\} \tag{15.7}$$
van Gödel-codes van stellingen van **PA** of **ZF** recursief opsombaar is;
2. berekend kan worden of een gegeven stelling φ de vorm $\varphi \equiv \chi_n$ heeft (en zo ja, voor welke n).

We bewijzen deze claims niet in detail, maar het idee van 1. is dat uit Stelling 12.1 volgt dat de lijst

$$\mathcal{B} = \{n \in \mathbb{N} \mid n = G(B),\ B \text{ is het bewijs van een stelling}\} \tag{15.8}$$

van Gödel-getallen van bewijzen van stellingen berekenbaar is (i.t.t. de lijst van Gödel-getallen van stellingen), omdat algoritmisch kan worden vastgesteld of een bepaald getal n de Gödel-code van een bewijs B is, en zo ja, van welke uitspraak, die immers de laatste regel van het bewijs is. Definieer nu de relatie $\mathcal{R} \subset \mathbb{N}^2$ door $(n,m) \in \mathcal{R}$ desda $n = G(\varphi)$ voor een zekere uitspraak φ en $m = G(B)$ voor een bewijs B van φ (zodat volgt dat $\vdash \varphi$). Net als $\mathcal{B}$ is $\mathcal{R}$ berekenbaar, en omdat $\mathcal{S}$ en $\mathcal{R}$ zich precies tot elkaar verhouden als in Lemma 14.1.4, namelijk $n \in \mathcal{S}$ desda er een m is zodat $(n,m) \in \mathcal{R}$ (een uitspraak is een stelling als er een bewijs van bestaat), volgt uit dat lemma dat $\mathcal{S}$ recursief opsombaar (r.e.) is.

De tweede claim volgt ook uit de eigenschappen van de Gödel-codering van **PA**. Uit een (recursieve) opsomming $(\varphi_0,\varphi_1,\ldots)$ van alle stellingen van **PA** kan dus achtereenvolgens worden bekeken of een bepaalde entry φ_k in de opsomming van de vorm $\varphi_k \equiv \chi_n$ is, voor zekere n. Als dit zo is vervangen we φ_k door n, en zo niet, dan schrappen we φ_k uit de lijst. Dit geeft een recursieve opsomming van $\mathcal{X}$.

Gegeven dat $\mathcal{X}$ recursief opsombaar is, bewijzen we nu Lemma 15.1 uit het ongerijmde. Stel dat iedere uitspraak χ_n die waar is ook bewijsbaar is. Dan geldt (wegens de correctheid van **PA**) dat $n \in \mathcal{X}$ desda $\vDash \chi_n$. Maar we hebben boven al gezien dat $\vDash \chi_n$ desda $n \notin S$. Dus $S^c = \mathcal{X}$. Maar we hebben net gezien dat $\mathcal{X}$ recursief opsombaar is. Dat was S ook al, zodat S berekenbaar is (Stelling 13.1). Tegenspraak, zodat er minsten één $n \notin S$ moet zijn waarvoor χ_n niet bewijsbaar is. Q.E.D.

Stelling 15.1 volgt direct uit Lemma 15.1 en Stelling 14.1: de ware maar niet bewijsbare uitspraak is de χ_n uit de laatste regel van het bovenstaande bewijs. Deze uitspraak is tevens onbeslisbaar. Q.E.D.

3. Als je Lemma 15.2 te lastig vindt kun je ook op gezag aannemen dat er een formule χ_n in **ZF** bestaat met als interpretatie $n \notin S$ (over verzamelingen i.h.a.), al krijg je Stelling 15.1 dan alleen voor **ZF** (en niet voor **PA**).

In het bovenstaande bewijs is flink gebruik gemaakt van het volgende lemma (van Gödel *himself*).

Lemma 15.2 *Een deelverzameling $P \subset \mathbb{N}^p$ is berekenbaar desda er een formule $\psi_P(x_1, \ldots, x_p)$ met p vrije variabelen in* **PA** *bestaat zodat de beide volgende condities gelden:*

1. $(n_1, \ldots, n_p) \in P$ *deen esda* $\vdash \psi_P(\mathbf{n}_1, \ldots, \mathbf{n}_p)$*;*
2. $(n_1, \ldots, n_p) \notin P$ *desda* $\vdash \neg\psi_P(\mathbf{n}_1, \ldots, \mathbf{n}_p)$*.*

Als aan deze twee condities is voldaan heet P *representeerbaar* (door ψ_P). Je mag in deze condities $\vdash$ vervangen door $\vDash$ (opgave), met andere woorden: P is representeerbaar door $\psi_P(x_1, \ldots, x_p)$ als

1. $(n_1, \ldots, n_p) \in P$ desda $\vDash \psi_P(\mathbf{n}_1, \ldots, \mathbf{n}_p)$;
2. $(n_1, \ldots, n_p) \notin P$ desda $\vDash \neg\psi_P(\mathbf{n}_1, \ldots, \mathbf{n}_p)$.

Hier zijn wat eenvoudige voorbeelden, waarvan het bewijs een oefening in **PA** is:

- $p = 1$: de verzameling E van even getallen is representeerbaar door
$$\psi_E(x) \equiv \exists_y(x = y + y). \tag{15.9}$$
- $p = 2$: de 'diagonaal' $\Delta \subset \mathbb{N}^2$ is representeerbaar door de formule
$$\psi_\Delta(x_1, x_2) \equiv (x_1 = x_2). \tag{15.10}$$
- $p = 3$: $O = \{(n_1, n_2, n_3) \mid n_3 = n_1 + n_2\}$ is representeerbaar door
$$\psi_O(x_1, x_2, x_3) \equiv (x_1 + x_2 = x_3). \tag{15.11}$$

In het tweede en derde voorbeeld heb je een (totale) functie $f : \mathbb{N}^{p-1} \to \mathbb{N}$ en $P = G_f$ is de grafiek
$$G_f = \{\vec{n} \in \mathbb{N}^p \mid n_p = f(n_1, \ldots, n_{p-1})\}; \tag{15.12}$$
in (15.10) is de functie $f = \pi^1_1$ oftewel $f(n) = n$. Dergelijke grafieken zijn representeerbaar desda f berekenbaar is (waarbij het soms even zoeken is naar de juiste formule $\psi_f \equiv \psi_{G_f}$). Voorbeelden:
$$\begin{aligned} \psi_Z(x_1, x_2) &\equiv (x_2 = \mathbf{0}); & (15.13)\\ \psi_S(x_1, x_2) &\equiv (x_2 = x_1 + S(\mathbf{0})); & (15.14)\\ \psi_{\pi^3_2}(x_1, x_2, x_3, x_4) &\equiv (x_2 = x_4). & (15.15) \end{aligned}$$

Het bewijs van dit lemma is lang en technisch, maar het idee is als volgt.

- *P representeerbaar $\Rightarrow$ χ_P berekenbaar.*
We hebben al gezien dat er een (totale) berekenbare functie $f : \mathbb{N} \to \mathbb{N}$ bestaat met als beeld de lijst G van Gödel-getallen $G(\varphi_i)$ van alle stellingen (φ_i) van **PA**, opgesomd in willekeurige volgorde. Als P nu representeerbaar is door een formule $\psi_P(x_1, \ldots, x_p)$, dan bereken je voor gegeven $\vec{n} \equiv (n_1, \ldots, n_p)$ het Gödel-getal $n_1 = G(\psi_P(\mathbf{n}_1, \ldots, \mathbf{n}_p))$ en tevens dat van de bijbehorende negatie, i.e. $n_2 = G(\neg\psi_P(\mathbf{n}_1, \ldots, \mathbf{n}_p))$. Vervolgens kun je de lijst G van zojuist nalopen tot je ofwel n_1 ofwel n_2 tegenkomt. In het eerste geval is $\chi_P(\vec{n}) = 1$, terwijl in het tweede $\chi_P(\vec{n}) = 0$.
- *χ_P berekenbaar $\Rightarrow$ P representeerbaar.*
Volgens Stelling 11.1 is χ_P partieel recursief. De stappen die χ_P d.m.v. de drie basisfuncties en de drie elementaire operaties van recursietheorie definiëren, geven tevens een procedure om de formule ψ_P te construeren. Voor de basisfuncties zie (15.13) - (15.15) boven. Stel nu dat $f = g \circ h$, waarbij ψ_g en ψ_h bekend zijn. Dan kun je kiezen
$$\psi_f(x, y) \equiv \exists_z(\psi_h(x, z) \wedge \psi_g(z, y)). \tag{15.16}$$
Je wilt namelijk dat $\psi_f(x, y)$ waar is desda $y = f(x) = g(h(x))$, en dat is precies zo als $y = g(z)$ voor $z = h(x)$. Iets soortgelijks, maar ingewikkelders, geldt voor recursie en minimalisatie. Zo kom je uiteindelijke op een formule $\psi_{\chi_P}(x, y)$ die de grafiek G_{χ_P} representeert. De laatste stap is dan om de formule $\psi_P(x)$ te vinden die P representeert (in de zin dat $n \in P$ desda $\vDash \psi_P(\mathbf{n})$). Deze formule wordt gegeven door
$$\psi_P(x) \equiv \psi_{\chi_P}(x, S(\mathbf{0})). \tag{15.17}$$
Dan geldt namelijk $\vDash \psi_P(\mathbf{n})$ desda $\vDash \psi_{\chi_P}(\mathbf{n}, S(\mathbf{0}))$, oftewel $(n, 1) \in G_{\chi_P}$, oftewel $G_{\chi_P}(n) = 1$, oftewel $n \in P$. En dat moet per definitie zo zijn desda $\vDash \psi_P(\mathbf{n})$. Q.E.D.

Er zijn, naast K en D in (14.10), nog talloze andere voorbeelden van recursief opsombare maar niet berekenbare verzamelingen. Neem bijvoorbeeld een opsomming $(\alpha_n(x))_n$ van alle formules van **PA** met één vrije variabele, en definieer

$$E = \{n \in \mathbb{N} \mid \vdash \alpha_n(\mathbf{n})\}. \tag{15.18}$$

Dan is E recursief opsombaar (per constructie) maar niet berekenbaar. Stel namelijk dat E berekenbaar is. Dan is ook E^c berekenbaar en is er volgens Lemma 15.2 een formule $\psi_{E^c}(x)$ zodat $n \in E^c$ desda $\vdash \psi_{E^c}(\mathbf{n})$, etc. Deze formule moet van de vorm $\psi_{E^c} = \alpha_e$ zijn voor zekere $e \in \mathbb{N}$. Dat geeft echter een tegenspraak (zie opgave).

We geven nu een schets van het oorspronkelijke bewijs dat Gödel van Stelling 15.1 gaf. Het volgt uit de eigenschappen van de Gödel-codering van **PA** dat de volgende deelverzamelingen berekenbaar zijn:

1. $\mathcal{W} \subset \mathbb{N}^3$, met $(n_1, n_2, n_3) \in \mathcal{W}$ desda $n_1 = G(\varphi(x_1))$ de code is van een formule $\varphi(x_1)$ met één vrije variabele x_1 en $n_3 = G(B_{\varphi(\mathbf{n_2})})$ de code is van een bewijs van de uitspraak $\varphi(\mathbf{n}_2)$.
2. $\tilde{\mathcal{W}} \subset \mathbb{N}^2$, met $(n_1, n_2) \in \tilde{\mathcal{W}}$ desda $(n_1, n_1, n_2) \in \mathcal{W}$, oftewel: $(n_1, n_2) \in \tilde{\mathcal{W}}$ desda er zowel een formule $\varphi(x_1)$ bestaat als een bewijs $B_{\varphi(\mathbf{n}_1)}$ van $\varphi(\mathbf{n}_1)$, met $n_1 = G(\varphi(x_1))$ en $n_2 = G(B_{\varphi(\mathbf{n}_1)})$.

We kunnen dus een formule $\psi_{\mathcal{W}}(x_1, x_2, x_3)$ kiezen die $\mathcal{W} \subset \mathbb{N}^3$ representeert is (in **PA**). Dan is $\tilde{\mathcal{W}}$ is representeerbaar door $\psi_{\tilde{\mathcal{W}}}(x_1, x_2) = \psi_{\mathcal{W}}(x_1, x_1, x_2)$, zodat volgens Lemma 15.2 dus geldt:

$$(n_1, n_2) \in \tilde{\mathcal{W}} \quad \text{desda} \quad \vdash \psi_{\tilde{\mathcal{W}}}(\mathbf{n}_1, \mathbf{n}_2); \tag{15.19}$$

$$(n_1, n_2) \notin \tilde{\mathcal{W}} \quad \text{desda} \quad \vdash \neg\psi_{\tilde{\mathcal{W}}}(\mathbf{n}_1, \mathbf{n}_2). \tag{15.20}$$

We definieren nu de volgende open formule met vrije variabele x_1:

$$\varphi(x_1) = \neg\exists_{x_2}\psi_{\tilde{\mathcal{W}}}(x_1, x_2). \tag{15.21}$$

Deze formule heeft als Gödel-code een bepaald natuurlijke getal

$$n_1 = G(\varphi(x_1)). \tag{15.22}$$

Vervolgens substitueren we $\mathbf{n}_1$ voor de vrije variabele x_1 in $\neg\exists_{x_2}\psi_{\tilde{\mathcal{W}}}(x_1, x_2)$. Dit geeft de beroemde uitspraak van Gödel (*Gödel sentence*), die haar eigen onbewijsbaarheid vaststelt:[4]

$$\chi \equiv \varphi(\mathbf{n}_1) = \neg\exists_{x_2}\psi_{\tilde{\mathcal{W}}}(\mathbf{n}_1, x_2). \tag{15.23}$$

De interpretatie van $[[\chi]]_{\mathbb{N}}$ van χ in $\mathbb{N}$ is immers dat er geen bewijs bestaat van de uitspraak $\varphi(\mathbf{n}_1)$.

Lemma 15.3

*1. De uitspraak χ is niet bewijsbaar in **PA**.*
2. De uitspraak χ is waar (in de zin van Definitie 5.1).

We bewijzen deel 1 uit het ongerijmde. Stel namelijk dat $\vdash \chi$, oftewel $\vdash \neg\exists_{x_2}\psi_{\tilde{\mathcal{W}}}(\mathbf{n}_1, x_2)$:

- Er bestaat dan een bewijs $B_{\varphi(\mathbf{n}_1)}$ van $\varphi(\mathbf{n}_1)$, met code $n_2 = G(B_{\varphi(\mathbf{n}_1)})$.
- Neem tevens $n_1 = G(\varphi(x_1))$, met $\varphi(x_1)$ gegeven door (15.21).
- Dan is $(n_1, n_2) \in \tilde{\mathcal{W}}$ volgens de definitie van $\tilde{\mathcal{W}}$.
- Dan volgt uit (15.19) dat $\vdash \psi_{\tilde{\mathcal{W}}}(\mathbf{n}_1, \mathbf{n}_2)$.
- Daaruit volgt $\vdash \exists_{x_2}\psi_{\tilde{\mathcal{W}}}(\mathbf{n}_1, x_2)$.
- En dus, met (15.21), $\vdash \neg\varphi(\mathbf{n}_1)$.
- Maar met de definitie (15.23) van χ is dit precies $\vdash \neg\chi$.

Uit $\vdash \chi$ volgt dus $\vdash \neg\chi$, maar dit is in tegenspraak met de aanname dat **PA** correct en dus consistent is. De oorspronkelijke aanname dat χ bewijsbaar is, i.e., $\vdash \chi$, moet dus fout zijn. M.a.w., χ is niet bewijsbaar.

Ook deel 2 volgt uit het ongerijmde. Stel dat χ niet waar, zodat $\neg\chi$ waar is (een uitspraak is immers waar of niet waar). Dan geldt dus $\vDash \exists_{x_2}\psi_{\tilde{\mathcal{W}}}(\mathbf{n}_1, x_2)$, oftewel: er is een $n_2 \in \mathbb{N}$ zodat $\psi_{\tilde{\mathcal{W}}}(n_1, n_2)$ geldt (als uitspraak over getallen). Dit is equivalent met $(n_1, n_2) \in \tilde{\mathcal{W}}$, en we zijn in het vorige deel van het bewijs aangeland, leidend tot dezelfde tegenspraak. Q.E.D.

4. De implicaties van zelfreferentie van logische systemen als **PA** en de stellingen van Gödel voor zaken als het menselijk bewustzijn zijn door beroemde auteurs als Douglas Hofstadter en Roger Penrose buiten alle proporties opgeblazen, zie bijvoorbeeld *I Am a Strange Loop* (Basic Books, New York, 2007) van de eerste en *Shadows of the Mind* (Oxford University Press, 1994) van de tweede. Het uitstekende boek van wijlen Torkel Franzén, *Gödel's Theorem: An Incomplete Guide to its Use and Abuse* (A K Peters, 2005) geeft een ontnuchterende demystificatie van dergelijke populair-wetenschappelijke werken (die wel erg leuk zijn!).

Opgave 15.1

Laat zien dat de twee formuleringen van de eerste onvolledigheidsstelling aan het begin van dit hoofdstuk equivalent zijn.

Opgave 15.2

Maar het bewijs af dat (15.18) niet berekenbaar is.

Opgave 15.3

a) Bewijs dat als P representeerbaar is door $\psi_P(x_1, \ldots, x_p)$, dan geldt dat $(n_1, \ldots, n_p) \in P$ desda $\vDash \psi_P(\mathbf{n}_1, \ldots, \mathbf{n}_p)$. Leg tevens uit waarom de twee condities in Lemma 15.2 onafhankelijk zijn.

b) Bewijs dat Δ representeerbaar is door ψ_Δ. Met andere woorden: bewijs uit de axioma's van **PA** dat $n_1 = n_2$ desda $\vdash (\mathbf{n}_1 = \mathbf{n}_2)$ en $n_1 \neq n_2$ desda $\vdash \neg(\mathbf{n}_1 = \mathbf{n}_2)$.

Opgave 15.4

We hebben een printer die bepaalde combinaties van de volgende symbolen kan printen: $\neg$, P, G, en de haakjes (en). We kennen de regels van de printer niet.[5] Een willekeurige (eindige) combinatie van deze symbolen heet een *term*. Er zijn dus geen regels voor term-formatie, alles is toegestaan. Een *uitspraak* is een term van één van de volgende vormen: $P(t)$, $PG(t)$, $\neg P(t)$, $\neg PG(t)$, waarbij t een willekeurige term is. We definieren waarheid als volgt: $\vDash P(t)$ desda t geprint kan worden, $\vDash PG(t)$ desda $t(t)$ geprint kan worden, $\vDash \neg P(t)$ als t niet geprint kan worden, en $\vDash \neg PG(t)$ als $t(t)$ niet geprint kan worden. We nemen aan dat de printer *correct* funtioneert, in de zin dat iedere printbare uitspraak waar is. *Geef een uitspraak die waar is maar niet printbaar.*

5. Printbaarheid is hier een metafoor voor afleidbaarheid, en voor de stellingen van Gödel doen de precieze axioma's er feitelijk niet toe, zolang de machinerie van het bewijs maar doorgaat.

16

De tweede onvolledigheidsstelling

De *eerste* onvolledigheidsstelling (i.e. Stelling 15.1) geeft een ware uitspraak in **PA** die niet binnen **PA** bewijsbaar is. Deze uitspraak χ uit het bewijs is echter nogal introvert: zij zegt iets over zichzelf, maar niets noemenswaardigs over **PA**. De *tweede* onvolledigheidsstelling van Gödel (i.e. Stelling 16.1) geeft een veel informatiever voorbeeld van een ware maar niet bewijsbare uitspraak.[1]

Eerst formuleren we de consistentie *van* **PA** door middel van een uitspraak *in* **PA**. Om te beginnen wordt de deelverzameling $N \subset \mathbb{N}^2$ gegeven door $(n_1, n_2) \in N$ desda er een uitspraak φ bestaat met $n_1 = G(\varphi)$ en $n_2 = G(\neg\varphi)$. Vervolgens is de deelverzameling $C \subset \mathbb{N}^4$ gedefinieerd door $(n_1, n_2, n_3, n_4) \notin C$ desda

1. $(n_1, n_3) \in B$;
2. $(n_2, n_4) \in B$;
3. $(n_1, n_2) \in N$,

waarbij $B \subset \mathbb{N}^2$ no. 2 in de lijst na Lemma 15.2 is. Als $(n_1, n_2, n_3, n_4) \notin C$, is er dus een uitspraak φ zodat zowel φ als $\neg\varphi$ bewijsbaar zijn: **PA** is in dat geval inconsistent. De consistentie van **PA** is dus precies de eigenschap dat $(n_1, n_2, n_3, n_4) \in C$ voor alle $(n_1, n_2, n_3, n_4) \in \mathbb{N}^4$.
Nu zijn B en N beide berekenbaar (om de bekende reden dat een computer de Gödel-codering uit kan voeren en tevens kan bepalen of gecodeerde uitdrukkingen correcte uitspraken resp. bewijzen zijn), en daarmee is ook C berekenbaar en dus representeerbaar door een formule $\psi_C(x_1, x_2, x_3, x_4)$. Laat

$$\Gamma \equiv \forall_{x_1}\forall_{x_2}\forall_{x_3}\forall_{x_4}\, \psi_C(x_1, x_2, x_3, x_4). \tag{16.1}$$

Analoog aan Lemma 15.3 hebben we:

Lemma 16.1

*1. De uitspraak Γ is niet bewijsbaar in **PA**.*
2. De uitspraak Γ is waar (in de zin van Definitie 5.1).

Het bewijs van dit lemma is veel moeilijker dan dat van Lemma 15.3. Deel 1 volgt uit het feit dat de implicatie $\Gamma \to \chi$, met χ als in het vorige hoofdstuk, binnen **PA** bewezen kan worden, m.a.w., dat

$$\vdash (\Gamma \to \chi). \tag{16.2}$$

Dit is een verscherping van Lemma 15.3, dat kan worden geformaliseerd als $\vDash (\Gamma \to \chi)$. Maar nu volgt de onbewijsbaarheid van Γ direct uit het ongerijmde: stel $\vdash \Gamma$, dan volgt uit (16.2) en de *modus ponens* dat $\vdash \chi$. Dit is echter in tegenspraak met Lemma 15.3. Deel 2 is helaas nog veel moeilijker![2] Nu volgt:

Stelling 16.1 *De consistentie van **PA** kan binnen **PA** wel worden geformuleerd, maar niet bewezen.*

Hiermee is de consistentie van **PA** een nieuw voorbeeld van een ware maar onbewijsbare stelling in **PA**.

---

1. Deze tweede stelling moet ook aan von Neumann worden toegeschreven, die het resultaat en het bewijs direct zag—hij was een legendarisch snelle denker—terwijl hij de eerste voordracht van Gödel over diens eerste onvolledigheidsstelling in 1931 bijwoonde. Gödel had deze conclusie zelf toen ook al getrokken en publiceerde hem.
2. Dat bewijs werd in 1936 binnen **ZF** geleverd door Gerhard Gentzen (1909–1945), destijds een assistent van Hilbert. Gentzen was een vooraanstaand logicus. Voor zijn tragische leven, eindigend met de hongerdood in een gevangenis in Praag, zie Eckart Menzler-Trott, *Gentzens Problem: Mathematische Logik im nationalsozialistischen Deutschland* (Birkhäuser, 2001). Een volledig bewijs van Lemma 16.1 is bijvoorbeeld te vinden in Peter Smith, *An Introduction to Gödel's Theorems* (CUP, 2007).

We hebben nu gezien dat de consistentie van **PA** nog wel in **PA** te definiëren is, maar niet te bewijzen. Met de waarheid is het nog erger gesteld, volgens een stelling van Alfred Tarski (1901–1983) uit 1934 (tevens onafhankelijk gevonden door Gödel), die de *ondefinieerbaarheid van waarheid* uitdrukt:

Stelling 16.2 *De deelverzameling $T \subset \mathbb{N}$ met $n \in T$ desda er een uitspraak ψ bestaat met $n = G(\psi)$ en $\vDash \psi$, is niet representeerbaar in* **PA** *(met andere woorden, er is geen 'waarheidspredikaat' in* **PA***).*

Het bewijs berust op het feit dat als T representeerbaar is, dan ook de deelverzameling F representeerbaar is, gegeven door $n \in F$ desda $n = G(\psi(x))$ voor een formule ψ met één vrije variabele x en $\nvDash \psi(n)$. Gegeven dit feit kun je het bewijs nu zelf afmaken door de uitspraak: "ik ben niet waar" te formaliseren.

Let op: de uitspraak "ik ben niet waar" leidt tot een tegenspraak; dit is de klassieke leugenaarsparadox "ik lieg". Die uitspraak is waar desda zij onwaar is. De uitspraak χ in (15.23) uit het bewijs van de eerste onvolledigheidsstelling daarentegen zegt "ik ben onbewijsbaar". Deze uitspraak is gewoon waar.

Het is jammer dat **PA** onvolledig is, zijn eigen consistentie niet kan bewijzen, en zijn eigen waarheidsbegrip (oftewel semantiek) niet eens kan formuleren, maar kunnen we niet gewoon wat wiskunde toevoegen om een theorie te krijgen die al deze eigenschappen wél heeft? Het antwoord is *nee*. Ieder logisch systeem dat **PA** bevat (zoals **ZF**) bevat onbewijsbare uitspraken die waar zijn als het systeem consistent is, en daarmee is zo'n systeem ook onvolledig. Het is mogelijk om de consistentie van **PA** binnen de verzamelingenleer af te leiden, maar de verzamelingenleer, het meest algemene systeem van de wiskunde, kan niet haar eigen consistentie bewijzen.

Hoe weten we dan eigenlijk dat de wiskunde consistent is? Het antwoord is *dat we dit helemaal niet weten!* Alle pogingen hierin verandering te brengen (zoals Hilbert hoopte) worden door de tweede onvolledigheidsstelling van Gödel (in haar meest algemene vorm) onmogelijk gemaakt.

Ook afgezien van dit probleem is de wiskunde minder zeker dan men tot ongeveer 1900 altijd gedacht had. Het idee van (opnieuw) Hilbert was dat de zekerheid van de wiskunde zou volgen uit het feit dat bewijzen een puur mechanische bezigheid is die, zoals wij nu zouden zeggen, op 100% betrouwbare wijze door computers zou kunnen worden uitgevoerd. In het bijzonder wordt bij dat soort bewijzen geen gebruik gemaakt van een eventuele interpretatie van een theorie, en/of van intuïtie, enzovoort. Inderdaad kan daarmee een grote hoeveelheid wiskunde worden afgedekt, maar, volgens Gödel, niet alles. Er blijft (in de woorden van de logicus Jean-Yves Girard) altijd een *blind spot* oftewel 'blinde vlek'.

De pogingen om de calculus te funderen door de analyse, de analyse door een goede definitie van $\mathbb{R}$, en deze laatste weer door de verzamelingenleer, met andere woorden, de zoektocht naar zekerheid in de wiskunde, heeft haar doel dus niet bereikt. Is de wiskunde daarmee op drijfzand gebouwd? Wie weet, maar het is onwaarschijnlijk: in de verzamelingenleer (in ieder geval voor zover deze op **ZF** is gebaseerd) zijn nog nooit tegenspraken voorgekomen. Bovendien zijn er geen voorbeelden van belangrijke wiskundige vragen die onbeslisbaar zijn (al is het een kwestie van smaak wat hier 'belangrijk' is).[3] In het verleden behaalde beleggingsresultaten geven echter geen garantie voor de toekomst!

3. De continuümhypothese van Cantor (zie voetnoot 3) is weliswaar onbeslisbaar in **ZF** en **ZFC**, maar dat is voor zover bekend niet gerelateerd aan de stellingen van Gödel en bovendien heeft deze hypothese geen enkele invloed op de gangbare wiskunde.

17

Het P≠NP probleem

In hoofdstuk 9 is het begrip *berekenbaarheid* van functies van $\mathbb{N}^p$ naar $\mathbb{N}$ gedefinieerd. In het algemeen kunnen we een probleem *berekenbaar* noemen als er een manier is om het te (her)formuleren in termen van natuurlijke getallen en (totale) *berekenbare* functies van $\mathbb{N}^p$ naar $\mathbb{N}$. Dit betekent dat het probleem, na de numerieke (her)formulering (die soms enige creativiteit vergt), *in principe* door een computer kan worden opgelost. Een oud voorbeeld uit de navigatie is het vinden van de kortste route tussen twee plaatsen via een (bekend) netwerk van wegen. Een wiskundige is echter niet zozeer geïntereseerd in een speciaal geval, maar in het *algemene* probleem een methode te geven om voor een *willekeurig* netwerk van plaatsen en wegen de kortste route tussen twee gegeven plaatsen uit dat netwerk te vinden.[1]

De volgende twee berekenbare problemen zijn anders van aard maar niet minder praktisch bruikbaar:

- bepaal of een getal $n \in \mathbb{N}$ al dan een niet priemgetal is;
- bepaal de priemfactoren van een getal $n \in \mathbb{N}$.

Deze twee problemen lijken een nauw verband met elkaar te hebben. Om dit te formaliseren zeggen we:

Definitie 17.1

1. *Een* beslisprobleem *is een deelverzameling* $S \subset \mathbb{N}$ *(of de bijbehorende functie* $\chi_S : \mathbb{N} \to \mathbb{N}$*).*
2. *Een* zoekprobleem *is een deelverzameling* $R \subset \mathbb{N} \times \mathbb{N}$ *(of de bijbehorende functie* $\chi_R : \mathbb{N}^2 \to \mathbb{N}$*).*
3. *Een zoekprobleem* $R \subset \mathbb{N}^2$ *bepaalt een beslisprobleem* $S_R \subset \mathbb{N}$ *door middel van*

$$S_R := \{n \in \mathbb{N} \mid R(n) \neq \emptyset\}; \tag{17.1}$$

$$R(n) := \{m \in \mathbb{N} \mid (n, m) \in R\}. \tag{17.2}$$

De vraag of $n \in \mathbb{N}$ een priemgetal is, is bijvoorbeeld een beslisprobleem. Priemfactorisatie is daarentegen een zoekprobleem, waarbij R bestaat uit alle paren (n, m) waarbij m een priemfactor van n is. Het bijbehorende beslisprobleem heeft $n \in S_R$ desda n *geen* priemgetal is (co-primaliteit).

Het algemene idee van een zoekprobleem R is dat voor gegeven '*instance*' n iedere $m \in R(n)$ een oplossing is; als $R(n) = \emptyset$ bestaat zo'n oplossing niet. Het beslisprobleem S_R bestaat dus uit de $n \in \mathbb{N}$ waarvoor het zoekprobleem R minstens één oplossing m heeft. Zo'n oplossing m met $(n, m) \in R$, waarmee je dus aantoont dat $n \in S_R$, heet een *bewijs* of *getuige* van n (Engels: *certificate* of *witness*). Een priemfactor m van n is bijvoorbeeld een bewijs dat n geen priemgetal is.

We zien bij priemgetallen iets typisch: het *verifiëren* dat een getal niet priem is gaat 'snel' (door de delers te vermenigvuldigen), terwijl het *vinden* van delers (door alle mogelijkheden uit te proberen) 'langzaam' gaat.[2] Het gaat bij 'snelheid' om *het aantal stappen dat een berekening duurt als functie van de lengte van de input*.[3] Denk (bij een beslisprobleem) aan het aantal stappen $\tau(n)$ dat de berekening van $\chi_S(n)$ m.b.v. een bepaald programma P duurt als functie van de lengte $\ell(n)$ van n. Hier is $\ell(n)$ simpelweg gedefinieerd als het aantal decimalen van n (het maakt daarbij weinig uit of binaire of decimale notatie wordt gebruikt, zie opgave); bij een functie van p argumenten $\vec{n} = (n_1, \ldots, n_p)$ is $\ell(\vec{n})$ het aantal decimalen van de som $n_1 + \cdots + n_p$.

---

1. Dit probleem is opgelost door de Nederlandse informaticus E.W. Dijkstra.
2. Het gebied van de informatica dat zich hiermee bezighoudt heet *complexiteitstheorie* (*Computational complexity*). Een goede (en ook leuke) inleiding is bijvoorbeeld C. Moore & S. Mertens, *The Nature of Computation* (Oxford University Press, 2011).
3. Dit aantal stappen bepaalt namelijk de rekentijd. Geheugencapaciteit van computers vormt al lang geen obstakel meer, en de (steeds hoger wordende) kloksnelheid van de computer speelt verrassend genoeg ook een ondergeschikte rol (zie opgave).

Het aantal stappen hang uiteraard (naast de input) af van het programma P (specifiek op een Registermachine) dat een bepaalde functie f berekent: een eenvoudig voorbeeld is optelling m.b.v. ons programmaatje uit hoofdstuk 10. Dat gebruikt voor de berekening van $n_1 + n_2$ precies $2n_2$ stappen, zodat $\tau(n_1, n_2) = 2n_2$ en dus $\tau(\vec{n}) \leq 2 \cdot 10^{\ell(\vec{n})}$. Je weet echter al sinds de basisschool dat je grote getallen het snelst per decimaal optelt, waarvoor geldt dat $\tau(\vec{n}) \leq C \cdot \ell(\vec{n})$. Dit is een enorme verbetering! Het is dus belangrijk om P slim te kiezen, maar daarin zit een marge: we willen namelijk we niet zozeer *precies* weten hoe $\tau(n)$ van $\ell(n)$ afhangt, maar slechts in een ruwe *schatting*, zoals uitgedrukt door de volgende definitie van de fameuze *complexiteitsklassen* P en NP uit de (theoretische) informatica.

Definitie 17.2 *1. Een (totale) berekenbare functie $f : \mathbb{N}^p \to \mathbb{N}$ ligt in P als er een programma P is met $f = f_P^p$, en constanten $C \in \mathbb{N}$, $k \in \mathbb{N}$ bestaan zodat $\tau(\vec{n}) \leq C \cdot \ell(\vec{n})^k$ voor alle $\vec{n} \in \mathbb{N}^p$.*

2. Een beslisprobleem $S \subset \mathbb{N}$ ligt in:

- *P als de karakteristieke functie $\chi_S : \mathbb{N} \to \mathbb{N}$ in P ligt.*[4]
- *NP als er een polynomiaal*[5] *zoekprobleem $V \subset \mathbb{N}^2$ bestaat (genaamd een* verificatiemethode *voor S) met $S_V = S$ en met karakteristieke functie $\chi_V : \mathbb{N}^2 \to \mathbb{N}$ in P.*

Ruw gezegd is de karakterisatie van de complexiteitsklassen P en NP dus als volgt:

- P omvat problemen waarvan het *vinden* van een oplossing 'snel' mogelijk is.[6]
- NP omvat problemen waarvan het *verifiëren* van een oplossing 'snel' lukt.

Voor beslisproblemen geldt P⊆NP (zie opgave), maar er bestaan nog veel meer complexiteitsklassen en een berekenbaar probleem hoeft dus niet in P of NP te liggen. Het is i.h.a. ook moeilijk om te zeggen in welke klasse een gegeven probleem ligt; dit hang vaak gevoelig af van de details. Het *Traveling Salesman Problem*) ligt eveneens in NP (en naar verwachting niet in P), maar het analoge kortste-pad probleem ligt (zoals opgelost door Dijkstra) weer in P (zoals iedere navigator aantoont). Het bepalen van priemfactoren ligt in NP (en waarschijnlijk niet in P),[7] en dat werd tot voor kort ook gedacht van het beslisprobleem van primaliteit. In 2002 werd echter door drie Indiase informaticastudenten (Agrawal, Kayal en Saxena) onverwacht bewezen dat primaliteit in P ligt! Het kan verkeren ...

Je gaat in een opgave bewijzen dat formeel P⊆NP voor beslisproblemen, wat (hopelijk) ook overeenkomt met je intuïtie dat het vinden van een oplossing moeilijker is dan het verifiëren ervan. Deze intuïtie leidt tot het beroemdste vermoeden van de theoretische informatica:[8] geldt P≠NP? Dit vermoeden drukt uit dat er berekenbare problemen in NP bestaan die niet in P liggen, zodat er 'echt' moeilijke algoritmisch oplosbare problemen bestaan. Hoezeer het ook voor de hand ligt, dit vermoeden blijkt heel moeilijk te bewijzen. Je kunt namelijk wel constructief aantonen dat een gegeven NP-probleem in P ligt door er een expliciet algoritme voor te geven dat in P ligt (soms onverwacht, zoals bij primaliteit), maar om te bewijzen dat het probleem níet in P ligt moet je aantonen dat een dergelijk algoritme niet bestaat.

Het belangrijkste inzicht tot zover om het probleem op te lossen is het bestaan van NP-*volledige problemen*, in de vroege jaren '70 ontdekt door de beroemde informatici Cook, Karp, en Levin. Dat zijn problemen die (zichzelf niet meegerekend) ieder ander probleem in NP in polynomiale tijd oplossen:

Definitie 17.3 *1. Een beslisprobleem $S \subset \mathbb{N}$ wordt* gereduceerd *tot $S' \subset \mathbb{N}$, notatie $S \leq S'$, als er een berekenbare functie $f : \mathbb{N} \to \mathbb{N}$ in P is met de eigenschap dat $n \in S$ desda $f(n) \in S'$.*

*2. Een beslisprobleem $S' \subset \mathbb{N}$ in NP heet NP-*volledig *als $S \leq S'$ voor ieder beslisprobleem S in NP.*

---

4. Hierbij staat P voor 'polynomiaal (begrensd)'. De oorspronkelijke definitie van NP (= Nondeterministic Polynomial) draaide om zgn. niet-deterministische Turing machines. De afkorting NP staat dus *niet* voor Non-Polynomial!

5. Een zoekprobleem $R \subset \mathbb{N} \times \mathbb{N}$ heet *polynomiaal* als er $\tilde{C}$ en $\tilde{k}$ in $\mathbb{N}$ bestaan zodat $(n, m) \in R$ impliceert $\ell(m) \leq \tilde{C} \cdot \ell(n)^{\tilde{k}}$. Deze eis wordt opgelegd om te vermijden dat dat alleen al het uitschrijven van m in termen van n meer dan polynomiale tijd kost.

6. Problemen in P hebben typisch $k = 1, 2, 3$; grote constanten als $k = 100$ o.i.d. komen in de praktijk niet voor.

7. We hebben de definitie van P en NP voor zoekproblemen echter nog niet gegeven, dus bij deze: een zoekprobleem R ligt in NP als het bijbehorende beslisprobleem S_R in NP ligt, met R als verificatiemethode. De definitie van P is ingewikkelder. Een *oplossing* van een zoekprobleem R is een functie $f : \mathbb{N} \to \mathbb{N}_*$ is met de eigenschap $f(n) \in R(n)$ desda $R(n) \neq \emptyset$, terwijl $f(n) = *$ desda $R(n) = \emptyset$. Hier staat $\mathbb{N}_*$ voor $\mathbb{N} \cup \{*\}$, de verzameling $\mathbb{N}$ uitgebreid met een extra element $*$. Een oplossing f van het zoekprobleem F bijvoorbeeld kent aan $n \in \Pi^c$ een bepaalde priemfactor $f(n)$ toe, en geeft $f(n) = *$ als $n \in \Pi$. Het begrip *berekenbare functie* $f : \mathbb{N}^p \to \mathbb{N}$ kan worden uitgebreid tot functies $f : \mathbb{N}^p \to \mathbb{N}_*$ (bedenk zelf hoe), en een zoekprobleem $R \subset \mathbb{N}^2$ ligt dan in P als R polynomiaal is en er een berekenbare oplossing f van R bestaat in P.

8. Het P≠NP probleem komt zelfs voor op de lijst van de 7 belangrijkste *wiskundige* problemen van onze tijd, zoals opgesteld door het *Clay Mathematics Institute*.Zie `http://www.claymath.org/millennium/`. Het Poincaré Vermoeden is inmiddels bewezen door de Rus Perelman. Die weigerde echter de geldprijs, omdat hij naar eigen zeggen al tevreden was met wat hij had (een kleine flat vol kakkerlakken). Wie een probleem uit deze lijst oplost krijgt 1 miljoen dollar. Zet hem op!

In de praktijk betekent dit dat een NP-volledig probleem als subroutine kan worden ingezet bij het oplossen van een willekeurig ander NP-probleem. Als deze subroutine als één rekenstap wordt geteld, kan zo ieder NP-probleem in polynomiale tijd worden opgelost. Als van ook maar één NP-volledig probleem zou worden aangetoond dat het in P ligt, is het P≠NP probleem dus in één klap opgelost (en wel negatief: dan zou namelijk P=NP). Vrijwel niemand gelooft dit echter.

Het bestaan van NP-volledige problemen is op zich niet raadselachtig, zoals uit het volgende voorbeeld blijkt.[9] De berekenbare functies $f : \mathbb{N}^2 \to \mathbb{N}$ zijn opsombaar, en dat geldt ook voor de speciale berekenbare functies χ_R die in P liggen, met $R \subset \mathbb{N}^2$. Dit geeft een opsomming $(R_1, R_2, \ldots)$, waarbij we zonder bewijs toevoegen dat van een gegeven zoekprobleem $R \subset \mathbb{N}^2$ in polynomiale tijd kan worden uitgerekend welke R_k het is (met andere woorden, er bestaat een programma dat R (bijv. via de Gödel-code van een programma dat χ_R berekent) in polynomiale tijd het getal $k \in \mathbb{N}$ kan bepalen waarvoor $R = R_k$.

Bekijk nu het beslisprobleem WIT (voor 'witness') dat voor een gegeven paar $(k, n) \in \mathbb{N}^2$ bepaalt of er een $m \in \mathbb{N}$ bestaat met $(n, m) \in R_k$: zo ja, dan geldt $(k, n) \in$ WIT (om dit letterlijk in de vorm van Definitie 17.2 moet je (k, n) nog coderen door een enkel getal $\tilde{n} \in \mathbb{N}$). Dit beslisprobleem ligt in NP: het bijbehorende zoekprobleem $W \subset \mathbb{N}^3$ is uiteraard $(k, n, m) \in W$ desda $(n, m) \in R_k$, en dit ligt (per definitie van de R_k) in P. Tevens is dit probleem NP-volledig: voor een gegeven beslisprobleem S in NP, met bijbehorend zoekprobleem V, is de functie f uit Definitie 17.3 (die zonder de codering van (k, n) door $\tilde{n}$ feitelijk een functie $f : \mathbb{N} \to \mathbb{N}^2$ is) simpelweg $f(n) = (k, n)$, waarbij k is bepaald door $V = R_k$. Deze functie ligt vanwege de opmerkingen in de vorige paragraaf in P. Aan de eis dat $n \in S$ (hetgeen het geval is desda $\exists_m (n, m) \in V$) desda $f(n) \in$ WIT (oftewel $(k, n) \in$ WIT) is voldaan omdat $V = R_k$.

Opgave 17.1

a) Stel $\tau(n) = C_1 \cdot \ell(n)$ voor een berekening van een functie $f(n)$ op een gegeven computer. Stel dat de berekening met de gegeven kloksnelheid van de computer binnen 1 uur kan worden gedaan zolang $\ell(n) \leq k_1$ (voor een bepaalde $k_1 \in \mathbb{N}$), en binnen 1000 uur (oftewel: met een 1000 keer snellere computer binnen 1 uur) zolang $\ell(n) \leq k_{1000}$. Als $\tau(n) \leq C \cdot \ell(n)$, dan geldt $k_{1000} = 1000 \cdot k_1$.
Geef het verband tussen k_{1000} en $k_1$voor $\tau(n) = C_2 \cdot \ell(n)^3$ en $\tau(n) = C_3 \cdot 2^{\ell(n)}$.

b) In de informatica gebruikt men het het binaire stelsel om gehele getallen te noteren. De lengte $\ell_2(n)$ van een natuurlijk getal is dan het totaal aantal nullen en enen in de binaire expansie van n. Laat zien dat $\log_2(n) \leq \ell_2(n) \leq \log_2(n)+1$ en analoog dat $\log_{10}(n) \leq \ell(n) \leq \log_{10}(n)+1$ voor de decimale versie $\ell \equiv \ell_{10}$. Toon nu aan dat

$$\ell_2(n) - 2 \leq K \cdot \ell(n) \leq \ell_2(n) + \log_2(10) + 1.$$

Leg uit dat het daarom voor de definitie van P en NP niet uitmaakt of je decimale of binaire notatie (voor n) gebruikt.

Opgave 17.2

Ligt vermenigvuldiging in P? Beantwoord deze vraag d.m.v. een schatting voor $\tau(n_1, n_2)$ als functie van $\ell(n_1, n_2)$ voor $f(n_1, n_2) = n_1 \times n_2$ als je deze operatie uitvoert door:

a) herhaald optellen (m.a.w. 123×456 uitrekent door 123 keer 456 bij zichzelf op te tellen);

b) de methode van de lagere school (dus 123 en 456 onder elkaar opschrijven, enz.).

Opgave 17.3

Toon (vanuit Definitie 17.2) aan dat P⊆NP voor beslisproblemen.

9. Er zijn echter *duizenden* NP-volledige problemen (boeken vol!); naast het al genoemde probleem van Hamilton en het nauw gerelateerde *Traveling Salesman Problem* (TSP) is ook het logische probleem SAT zeer bekend.

18

Kansrekening

We passen het idee van axiomatisering nu toe op een deelgebied van de wiskunde, i.t.t. de wiskunde als geheel. In het eerste geval worden de axioma's niet in een logische taal geformuleerd, maar binnen de verzamelingenleer.[1] We kiezen voor dit deelgebied de kansrekening, omdat dit gebied zeer eenvoudige axioma's heeft en bovendien vele toepassingen kent. Daarvan zullen we de forensische statistiek en de kwantumfysica behandelen.[2]

Er zijn twee equivalentie manieren om de kansrekening te axiomatiseren.Beide gaan uit van een *kansruimte* X. Wiskundig is dat gewoon een verzameling, die in dit college dus *eindig* wordt genomen, zodat $X = \{x_1, \ldots, x_n\}$. De elementen x_i van deze ruimte worden geïnterpreteerd als mogelijke uitkomsten van een *toevalsproces* (of *kansexperiment*). Denk aan het eenmalig werpen van een dobbelsteen, waarbij $X = \underline{6} \equiv \{1, 2, 3, 4, 5, 6\}$. Een deelverzameling van X heet een *event* of *gebeurtenis* (slechte naam). Denk bijvoorbeeld aan $A = \{1, 3, 5\}$ bij het dobbelen, maar ook aan $A = \{6\}$: een individuele uitkomst is een speciaal geval van een gebeurtenis.[4]

Na deze toelichting komt nu de axiomatisering.

Definitie 18.1 *Zij gegeven een eindige verzameling X (en de reële getallen $\mathbb{R}$).*

1. *Een* kansfunctie *op X is een functie $P : \mathcal{P}(X) \to \mathbb{R}$ die voldoet aan:*

$$0 \leq P(A) \leq 1 \text{ voor alle } A \subset X; \tag{18.1}$$
$$P(X) = 1; \tag{18.2}$$
$$P(A \cup B) = P(A) + P(B) \text{ als } A \cap B = \emptyset. \tag{18.3}$$

2. *Een* kansverdeling *op X is een functie $p : X \to \mathbb{R}$ met de eigenschappen:*

$$p(x) \geq 0; \tag{18.4}$$
$$\sum_{x \in X} p(x) = 1. \tag{18.5}$$

---

1. Voor de liefhebbers: **PA** en **ZF** hebben een *syntactische* axiomatisatie door middel van eerst orde logica, waarin eerst een logische taal wordt opgesteld en pas als tweede stap naar interpretaties wordt gezocht. Zoals de meeste deelgebieden van de wiskunde heeft de kansrekening daarentegen een zogenaamde *semantische* axiomatisatie. Hierin wordt een theorie direct gedefinieerd door een axiomatisatie van haar klasse van modellen, in dit geval binnen de gebruikelijke verzamelingenleer. Deze opzet gaat onder meer terug op John von Neumann.

2. De toepassing waaruit de mathematische kansrekening oorspronkelijk is ontstaan is echter gokken. Gokspelen zoals dobbelen bestaan al sinds de oudheid. De wiskundige structuur van de onderliggende toevalsprocessen werd voor het eerst (serieus) bestudeerd in een briefwisseling tussen Fermat en Pascal in 1654.[3] Christiaan Huygens, die van deze correspondentie op de hoogte was, schreef in 1656 *Van Rekeningh in Spelen van Geluck*. Dit was het eerste boekje over kansrekening. Ondanks bijdragen van grote wiskundigen als Daniel Bernoulli (1700–1782) en Pierre-Simon (Markies van) Laplace (1749–1827) behield het onderwerp eeuwenlang haar associatie met vulgaire zaken als gokken, die eerder in de kroeg dan op de universiteit thuishoren. Het geboortejaar van de kansrekening als serieus onderdeel van de wiskunde is 1933, toen de Russische wiskundige Andrej Kolmogorov (1903–1987) het boek *Grundbegriffe der Wahrscheinlichkeitsrechnung* publiceerde. Daarin stelt hij axioma's voor de kansrekening op en verbindt hij het onderwerp met de eerder die eeuw ontwikkelde *maattheorie*. We geven een vereenvoudigde versie van deze axioma's, namelijk voor het geval dat een gegeven toevalsproces eindig veel mogelijke uitkomsten heeft. De axioma's zijn dan heel simpel, en zijn in feite al te vinden bij de Engelse dominee Thomas Bayes (1702–1761).

4. Als je een kansexperiment met kansruimte X een N keer herhaalt, is de kansruimte $= X^N = X \times \cdots \times X$ (N factoren X). Als je de kans op "twee keer 6 in 5 worpen" wilt weten, moet je dit beschouwen als de gebeurtenis die bestaat uit alle elementen van $\underline{6}^5$ waarin precies twee zessen voorkomen. In dat geval zie je misschien beter waarom het zin heeft kansen aan gebeurtenissen (en niet alleen aan uitkomsten) toe te kennen.

We beschouwen (18.1) t/m (18.3) als axioma's voor kans*functies*, en (18.4) en (18.5) als axioma's voor kans*verdelingen*. Deze axiomastelsels zijn equivalent in de volgende zin (bewijs: opgave!).

Stelling 18.1 *1. Gegeven een functie $p : X \to \mathbb{R}$, definiëren we een functie $P : \mathcal{P}(X) \to \mathbb{R}$ d.m.v.*

$$P(A) = \sum_{x \in A} p(x). \tag{18.6}$$

Als p voldoet aan (18.4) *en* (18.5)*, dan voldoet P aan* (18.1) - (18.3).

2. Gegeven een functie $P : \mathcal{P}(X) \to \mathbb{R}$, definiëren we een functie $p : X \to \mathbb{R}$ d.m.v.

$$p(x) = P(\{x\}). \tag{18.7}$$

Als P voldoet aan (18.1) - (18.3)*, dan voldoet p aan* (18.4) *en* (18.5).

3. Dit geeft een bijectie tussen de verzameling van functies $P : \mathcal{P}(X) \to \mathbb{R}$ die voldoen aan (18.1) - (18.3) *en de verzameling van functies $p : X \to \mathbb{R}$ die voldoen aan* (18.4) *en* (18.5).

De Bayesiaanse kansrekening, die centraal staat in talloze toepassingen en die we later dan ook zullen behandelen, is gebaseerd op een *voorwaardelijke kansfunctie* $\mathcal{P}(X) \times \mathcal{P}(X) \to \mathbb{R}$, die we voor het gemak ook P noemen (maar dan met twee argumenten) en dus noteren als $(A, B) \mapsto P(A|B)$. Preciezer gezegd: dit is een partiële functie, waarvan het domein D in $\mathcal{P}(X) \times \mathcal{P}(X)$ wordt bepaald door een gegeven kansfunctie $P : \mathcal{P}(A) \to \mathbb{R}$, en wel als $(A, B) \in D$ desda $P(B) \neq 0$. De uitdrukking $P(A|B)$ is dus niet gedefinieerd als $P(B) = 0$, en als $P(B) > 0$ geeft $P(A|B)$ de kans dat een uitkomst x in A ligt, gegeven dat x in B ligt, oftewel "de kans op A gegeven B." Met andere woorden: *$P(A|B)$ is de kans op A wanneer we de kansruimte X en de gegeven kansfunctie P beperken tot $B \subset X$*. De definitie is

$$P(A|B) = \frac{P(A \cap B)}{P(B)} \equiv \frac{P(A, B)}{P(B)} \tag{18.8}$$

Deze keuze kan als het *vierde axioma* van de kansrekening worden gezien, i.e. na (18.1) - (18.3). Dit vierde axioma kan dan worden vergeleken met de definitie van *onafhankelijkheid* in de kansrekening:

Definitie 18.2 *Twee deelverzamelingen $A \subset X$ en $B \subset X$ heten* onafhankelijk *ten opzichte van een gegeven kansfunctie P op X als*

$$P(A \cap B) = P(A)P(B). \tag{18.9}$$

Als $P(B) > 0$ is deze definitie equivalent met: A en B zijn onafhankelijk t.o.v. P desda $P(A|B) = P(A)$.

In dat geval heeft kennis van het feit dat de uitkomst in B ligt dus geen invloed op de kans dat deze in A ligt. Let op dat onafhankelijkheid is gedefinieerd *ten opzichte van een gegeven kansfunctie!*

Relatieve frequenties

Op het vwo werden kansen vroeger gedefinieerd als *relatieve frequenties*.[5] We herhalen een kansexperiment dan N keer, schrijven de uitkomsten $(x_1, \ldots, x_N)$ op, kiezen een deelverzameling $A \subset X$, tellen het aantal keren dat $x_k \in A$, noemen dit aantal $n(A)$, en interpreteren de kansfunctie ten slotte als

$$P(A) = \frac{n(A)}{N}. \tag{18.10}$$

Evenzo interpreteren we de voorwaardelijke kans, aangenomen dat $n(B) > 0$, d.m.v.

$$P(A|B) = \frac{n(A, B)}{n(B)}, \tag{18.11}$$

waarbij $n(A, B)$ het aantal keren is dat de uitkomst x_k in $A \cap B$ ligt. Deze interpretatie voldoet aan de axioma's (18.1) - (18.8) uit het vorige hoofdstuk (opgave), maar niettemin is zij problematisch.

5. Deze definitie gaat er stilzwijgend vanuit dat een kansexperiment willekeurig vaak herhaald kan worden. We hebben al gezien dat dit soms kan (bijv. bij dobbelen en bij de meeste natuurkundige experimenten), maar lang niet altijd (bijv. bij rechtszaken).

Ten eerste is deze procedure voor kleine N evident onzinnig. Voor $N = 1$ krijg je bijvoorbeeld, als je 6 gooit, $P(A) = 0$ als $6 \notin A$ en $P(A) = 1$ als $6 \in A$ (oftewel $p(6) = 1$ and $p(k) = 0$ voor $k \neq 6$). Je wilt N dus 'groot' kiezen en hoopt (om het begrip 'groot' precies te maken) dat er voor $N \to \infty$ een limiet bereikt wordt, zodat

$$P(A) = \lim_{N\to\infty} \frac{n(A)}{N}; \tag{18.12}$$

$$P(A|B) = \lim_{N\to\infty} \frac{n(A,B)}{n(B)}. \tag{18.13}$$

Als deze limieten inderdaad bestaan, is net als voor eindige N voldaan aan de axioma's van de kansrekening. Uitvoerig onderzoek heeft echter geleerd dat de *definitie* van kansen door limieten van relatieve frequenties *niet* werkt. Voor het bestaan van de bewuste limieten moeten kunstmatige voorwaarden worden opgesteld, de limiet hangt - als hij al bestaat - mogelijk af van de gegeven reeks uitkomsten, en bovendien is het praktisch onmogelijk om een kansexperiment oneindig vaak uit te voeren.

Wat *wel* door middel van formules als (18.12) en (18.13) kan, is de empirische *verificatie* van theoretisch *bepaalde* kansen op herhaaldelijke gebeurtenissen. Je kunt namelijk bewijzen dat *als* bijvoorbeeld $p(6) = 1/6$ (zoals kan blijken uit de symmetrische vorm van de dobbelsteen, de wisselende manier van gooien, enz.), dan de reeksen $(x_1, \ldots, x_N)$ waarvoor de limiet in (18.12) bestaat overweldigend veel waarschijnlijker zijn dan de reeksen waarvoor de limiet niet bestaat, en dat deze limiet dan gelijk is aan $1/6$. Een soortgelijk verhaal geldt voor kansen op microscopische processen zoals die in de kwantummechanica worden berekend; zie latere hoofdstukken. In al deze gevallen levert de theorie in principe kansen op uitkomsten van één enkel kansexperiment, waarna deze voorspellingen worden getoetst door het bewuste experiment vaak te herhalen. De kansen worden dan door de theorie *gedefinieerd* en door de relatieve frequenties van een herhaald kansexperiment *geverifieerd*. Het *definiëren* van kansen als relatieve frequenties lijkt echter zelfs voor herhaalbare kansexperimenten een dood spoor.[6]

Hier komt dan nog bij dat vele toevalsprocessen niet herhaald kunnen worden: denk aan de kans dat een verdachte in een bepaalde rechtszaak schuldig is, bijvoorbeeld op grond van een DNA-spoor. De zogenaamde 'Bayesiaanse' trend in de huidige kansrekening is daarom dat *alle* kansen primair als eenmalige kansen gedefinieerd moeten worden, ook die op herhaaldelijke gebeurtenissen.[7] De Bayesiaanse kansrekening komt in het volgende hoofdstuk aan bod.

Opgave 18.1

Bewijs Stelling 18.1.

Opgave 18.2

a) Laat zien dat (18.10) voldoet aan de axioma's (18.1) - (18.3).
b) Laat vervolgens zien dat (18.11) voldoet aan axioma (18.8).

6. En dan hebben we het niet over *weetkansen* versus *zweetkansen*, een belachelijk onderscheid dat in sommige wiskundeboeken voor het vwo wordt gemaakt en dat je, als je er helaas mee geconfronteerd bent, zo snel mogelijk weer moet vergeten.
7. Wat in de Bayesiaanse filosofie overblijft van (18.10) is dat het linkerlid eigenlijk moet worden gezien als de voorwaardelijke kans $P(A|(x_1, \ldots, x_N))$, i.e., een schatting van de kans op A gegeven de empirische input $(x_1, \ldots, x_N)$.

19

Bayesiaanse kansrekening

De Bayesiaanse aanpak begint niet met een kansruimte X, maar met het opstellen van een aantal $(K+1)$ hypotheses, die we nummeren als H_0 t/m H_K, dus H_k met $k = 0, 1, \ldots, K$ (later zal H_0 vaak een speciale rol spelen). Deze sluiten elkaar per definitie uit, en precies één is waar (je weet alleen nog niet welke). Je kunt hierbij denken aan de verdachten van een misdaad, waarbij H_k de hypothese is dat verdachte no. k schuldig is (in een situatie waarin justitie er zeker van is dat er precies één dader is, die zich onder de verdachten bevindt). Formeel kunnen we dan een kansruimte X invoeren door middel van

$$X = \bigcup_{k=0}^{K} H_k \equiv H_0 \cup \cdots \cup H_K. \tag{19.1}$$

waarbij dus $H_k \subset X$ en $H_i \cap H_j = \emptyset$ als $i \neq j$.

Op deze kansruimte is een kansfunctie P gedefinieerd, die we echter niet kennen. We weten wél dat

$$\sum_{k=0}^{K} P(H_k) = 1. \tag{19.2}$$

Uit iteratie van axioma (18.3) van de kansrekening volgt namelijk

$$P(A_1 \cup \cdots \cup A_n) = \sum_{i=1}^{n} P(A_i) \tag{19.3}$$

als alle $A_i \subset X$ disjunct zijn, en met (18.2) volgt dan onmiddellijk (19.2). Vervolgens is er bewijsmateriaal E, dat als deelverzameling van X wordt beschouwd (hoe precies wordt in het midden gelaten), formeel met $P(E) > 0$, zodat de voorwaardelijke kansen $P(H_k|E)$ gedefinieerd zijn. Dan geldt:

$$P(H_i|E) = \left(1 + \sum_{k \neq i} \frac{P(H_k)}{P(H_i)} \cdot \frac{P(E|H_k)}{P(E|H_i)}\right)^{-1}. \tag{19.4}$$

In het speciale geval dat $P(H_i) = P(H_j)$ voor alle i, j, wat meestal wordt aangenomen, geeft dit dus

$$P(H_i|E) = \left(1 + \sum_{k \neq i} \frac{P(E|H_k)}{P(E|H_i)}\right)^{-1}, \tag{19.5}$$

de basis van de Bayesiaanse kansrekening. Vgl. (19.5) volgt direct uit de zgn. *regel van Bayes*

$$P(H_i|E) = P(E|H_i) \cdot \frac{P(H_i)}{P(E)}, \tag{19.6}$$

die zelf weer direct volgt uit (18.8), gecombineerd met opnieuw (18.8) en de formule

$$P(E) = \sum_{k=0}^{K} P(H_k \cap E). \tag{19.7}$$

Om deze laatste formule te bewijzen gebruiken we de distributieve eigenschap

$$\cup_k (A_k \cap B) = (\cup_k A_k) \cap B, \tag{19.8}$$

die voor alle deelverzamelingen A_k en B van een willekeurige verzameling X geldt. Met (19.1) volgt

$$\cup_k(H_k \cap E) = (\cup_k H_k) \cap E = X \cap E = E,$$

wat met (19.3) en de opmerking dat alle $H_k \cap E$ disjunct zijn (nl. omdat alle H_k dat zijn), (19.7) geeft.

We zullen zien dat de zgn. *likelihood ratios* $P(E|H_i)/P(E|H_k)$, waarin het bewijsmateriaal in aanmerking wordt genomen, vaak te berekenen zijn. Let op: als $P(E|H_i) = 0$ en/of $P(H_i) = 0$, dan verdwijnt H_i gewoon uit de lijst met hypotheses (het bewijsmateriaal E sluit H_i in dat geval namelijk uit).

We illustreren (19.5) in het *driedeurenprobleem* (*Monty Hall Problem*, *Ziegenproblem*). Bij dit probleem krijgt een deelnemer aan een quiz drie gesloten deuren te zien. Achter één daarvan bevindt zich een splinternieuwe sportauto, achter twee staat een geit (de veronderstelling is dat de deelnemer liever de auto wint dan een geit). De deelnemer kiest een deur, waarna de quizmaster (die weet waar de auto zich bevindt) een andere deur opent. Daar staat een geit. De deelnemer krijgt vervolgens de kans om van zijn oorspronkelijke keus af te wijken. Het *driedeurenprobleem* is de vraag of dat zijn kans om de auto te winnen verhoogt (N.B. het gaat dus om de kansen *zoals de deelnemer die ervaart*). In eerste instantie denken de meeste mensen dat het niet uitmaakt. De Bayesiaanse aanpak geeft het correcte antwoord:

Stel dat H_k (voor $k = 1, 2, 3$) de hypothese is dat de auto achter deur k staat, en dat het bewijsmateriaal E bestaat uit de keuze van bijv. deur 1 door de deelnemer en het openen van deur 2 door de quizmaster. Dan hebben we voor de voorwaardelijke kansen die in (19.5) nodig zullen zijn:

$$P(E|H_1) = 1/2; \tag{19.9}$$
$$P(E|H_2) = 0; \tag{19.10}$$
$$P(E|H_3) = 1. \tag{19.11}$$

Als de auto achter deur 1 staat, zoals H_1 zegt, dan heeft de quizmaster nl. twee deuren om te openen zonder de auto te laten zien. Ieder daarvan heeft dus kans $1/2$. Dit geeft (19.9). Ten tweede geldt (19.10) omdat achter de geopende deur een geit staat (terwijl daar volgens H_2 de auto zou moeten staan). Ten derde geldt (19.11) omdat de quizmaster geen andere keuze heeft dan het openen van deur 2 als de deelnemer deur 1 kiest en de auto achter deur 3 staat (zoals uitgedrukt door H_3). Invullen in (19.5) geeft

$$P(H_1|E) = 1/3; \tag{19.12}$$
$$P(H_3|E) = 2/3. \tag{19.13}$$

De deelnemer verdubbelt dus zijn kans om de auto te winnen als hij switcht.

Het driedeurenprobleem werd voor het eerst gesteld in de Amerikaanse quiz *Let's make a deal* van presentator Monty Hall, maar kreeg pas grote bekendheid toen het in 1990 werd besproken in het Amerikaanse tijdschrift *Parade Magazine*. Marilyn Savant Vos schreef erover in haar column 'Ask Marilyn', waarin ze wekelijks wiskundevragen van lezers beantwoordde. Alhoewel Marilyn volgens het *Guinness Book of Records* de intelligentste vrouw ter wereld was, twijfelden velen aan haar bewering dat je je kans op de hoofdprijs verhoogt van $\frac{1}{3}$ naar $\frac{2}{3}$ door van deur te wisselen. Zelfs na haar uitleg bleven de brieven van mensen, onder wie voorname wetenschappers en wiskundigen, die het tegendeel beweerden, binnenstromen. Enkele reacties op haar (correcte!) oplossing waren:

> "Ik maak me grote zorgen over het gebrek aan wiskundig inzicht bij het grote publiek. Help alstublieft door uw fout toe te geven."
> "Ongelooflijk dat u uw fout nog steeds niet inziet nadat u door zeker drie wiskundigen bent verbeterd."
> "U hebt het volledig mis ... Hoeveel woedende wiskundigen zijn er nog voor nodig om u te overtuigen?"

Zowel in populair wetenschappelijke als serieuze wiskundige tijdschriften verschenen regelmatig artikelen over het Monty Hall probleem. Ook in Nederland zorgde het probleem voor veel opwinding toen er in 1995 een artikel over verscheen in het NRC-Handelsblad. Ook deze krant kreeg talloze brieven binnen en beëindigde uiteindelijk de discussie met de woorden:

> "Stop, stop, stop met brieven sturen. Het onbegrip tussen het gezond verstand en de wiskundigen is kennelijk onoverbrugbaar."

Opgave 19.1

Je hebt een vaas met K ballen in twee kleuren, zeg rood en wit (de kleuren van Ajax). Je wilt door middel van een steekproef schatten wat het aantal w witte ballen in de vaas is. Je hypothesen zijn H_0 t/m H_K, waarbij H_k stelt dat $w = k$. Je trekt (met terugleggen) n_W witte ballen en n_R rode, totaal $N = n_W + n_R$. Dat is de bewijslast E. In het vervolg is i één van de waarden $0, 1, \ldots, K$.

a) Wat is $P(H_i|E)$ volgens (19.5)?
b) Geef een schatting van $P(H_i|E)$ voor grote K.
c) Voor welke waarde van i is de uitdrukking in **b)** maximaal?

Hint: Gebruik in **a)** de volgende formule uit het vwo, met $p_i = i/K$:

$$P(E|H_i) = \frac{(n_W + n_R)!}{n_W! n_R!} p_i^{n_W} (1 - p_i)^{n_R}. \tag{19.14}$$

Gebruik in **b)** de volgende benadering voor grote K (volgt uit de theorie van de Riemann-integraal):

$$\frac{1}{K+1} \cdot \sum_{k=0}^{K} p_k^{n_W} (1 - p_k)^{n_R} \approx \int_0^1 dx\, x^{n_W} (1 - x)^{n_R}. \tag{19.15}$$

Herhaald partieel integreren of opzoeken (in een boek over integralen) geeft vervolgens

$$\int_0^1 dx\, x^{n_W} (1 - x)^{n_R} = \frac{n_W! n_R!}{(n_W + n_R + 1)!}. \tag{19.16}$$

Beschouw in **c)** de combinatie $x = i/K$ als een continue variabele in $[0, 1]$ en maximaliseer $P(H_i|E)$ als functie van x.

20

DNA-identificatie

Een van de belangrijkste toepassingen van de Bayesiaanse kansrekening uit het vorige hoofdstuk is DNA-*identificatie*. Deze techniek werd eind jaren '80 ingevoerd, met bijv. de volgende toepassingen:

- *Daderidentificatie*. Hier wordt een DNA-spoor T (wat dit precies inhoudt zullen we zo zien) op een lijk (soms een levende) aangetroffen, zijnde het slachtoffer is van een misdrijf. We gaan er vanuit dat T afkomstig is van de dader.[1] Vervolgens komt justitie met een lijst verdachten $(v_0, \ldots, v_K)$, met bijbehorende hypothesen H_k dat v_k de dader is. Een speciale verdachte v_0 heeft eveneens DNA-profiel T: deze *match* vormt het bewijsmateriaal E.[2] We willen de kans $P(H_0|E)$ bepalen dat v_0 de dader is, gegeven het bewijsmateriaal E, oftewel de DNA-*match* met v_0.
- *Slachtofferidentificatie*. Er is opnieuw een lijk met DNA-profiel T, maar deze keer is dat afkomstig van het lijk L zelf (dat typisch het slachtoffer was van een ongeval i.p.v. een misdrijf). De lijst $(v_0, \ldots, v_K)$ is in dit geval een lijst van vermisten. Nu is H_k de hypothese dat het lijk dat van v_k is, en is het bewijsmateriaal E de DNA-*match* tussen het lijk en vermiste v_0. De te bepalen grootheid $P(H_0|E)$ is nu de kans dat het gegeven lijk dat van vermiste v_0 is, gegeven de *match* met v_0.
- *Vaderidentificatie* De moeder van een baby beweert dat v_0 de vader van de baby is, terwijl deze man dat ontkent.[3] In deze situatie is $(v_0, \ldots, v_K)$ een (delicate) lijst van mogelijke vaders, met bijbehorende hypothesen H_k dat v_k de biologische vader van de baby is. Het bewijsmateriaal E is nu de DNA-*match* tussen de baby en de kandidaat-vader v_0. Het is duidelijk dat in deze situatie $P(H_0|E)$ de kans is dat v_0 de vader van de baby is.

We bepalen de gezochte kans $P(H_0|E)$ met behulp van (19.5) voor $i = 0$, dus

$$P(H_0|E) = \left(1 + \sum_{k=1}^{K} \frac{P(E|H_k)}{P(E|H_0)}\right)^{-1}. \tag{20.1}$$

Bij slachtofferidentificatie geldt dan vanwege de betekenis van E, H_0, en E_0 direct

$$P(E|H_0) = 1. \tag{20.2}$$

Bij daderidentificatie volgt dit als zeker is dat het spoor T van de dader afkomstig is. Bij vaderidentificatie is $P(E|H_0)$ gelijk aan 1 of aan $1/2$, zie einde hoofdstuk. We gaan verder uit van (20.2), zodat

$$P(H_0|E) = \left(1 + \sum_{k=1}^{K} P(E|H_k)\right)^{-1}. \tag{20.3}$$

Hierin moeten we dus nog de kansen $P(E|H_k)$ bepalen voor $k \neq 0$. Er zijn twee eenvoudige gevallen:

1. Bij de moord op Marianne Vaatstra werd aangenomen dat de dader uit de buurt kwam. Van alle mannen uit de buurt werd een DNA-profiel bepaald en er was alleen een *match* bij Jasper S..

---

1. In de praktijk wordt de kans $P(E|H_0)$ dat T inderdaad van de dader komt nader onderzocht. In de Puttense moordzaak (zie wikipedia) werd door het Openbaar Ministerie bijvoorbeeld plotseling, toen er geen DNA-match met de hoofdverdachte(n) bleek te zijn, ontkend dat het sperma op het lijk van Christel Ambrosius van de verkrachter en moordenaar afkomstig zou zijn. Hiertoe werd de zgn. 'sleeptheorie' bedacht, die echter onzin bleek te zijn: de hoofdverdachten waren gewoon onschuldig.
2. Strikt gesproken bestaat E dus uit twee delen: het spoor op het lijk is T en het profiel van v_0 is eveneens T.
3. Bijvoorbeeld omdat het buitenechtelijke affaire was, omdat hij vreest alimentatie te moeten betalen, of na een verkrachting.

Met hem als v_0 gold dus $P(E|H_k) = 0$ voor alle $k \neq 0$, en daarmee $P(H_0|E) = 1$. Daarmee viel het doek voor Japser S.[4]

2. De omgekeerde situatie is die waarin niets bekend is over de overige verdachten v_k. Dan neemt men een 'bevolkingsgemiddelde' $P(T)$ voor alle k, en dus onafhankelijk van k:

$$P(E|H_k) = P(T). \tag{20.4}$$

Onder deze aanname wordt (20.3) eenvoudigweg

$$P(H_0|E) = (1 + K \cdot P(T))^{-1}. \tag{20.5}$$

De allereenvoudigste toepassing van deze laatste formule is als volgt. Op een eiland is een moord begaan. Op het lijk wordt een DNA-spoor T aangetroffen. Verdachte no. nul blijkt deze eigenschap T te hebben. Op het eiland wonen (afgezien van het lijk en de dader) K mensen. De verdachte is geen familie van de andere eilandbewoners. De kans dat de verdachte schuldig is, is dan gelijk aan (20.5). Stel dat $K = 100$ en $P(T) = 0.01$; dan is $P(H_0|E) = 1/2$, wat kleiner is dan je zou verwachten gezien de DNA-match. Als daarentegen $K = 100$ en $P(T) = 10^{-10}$, dan is $P(H_0|E) = 0,99999999$.

Het wordt ingewikkelder als er familierelaties tussen v_k en v_0 zijn: daarmee stijgt de kans $P(E|H_k)$ in het algemeen (en daalt dus $P(H_0|E)$, omdat het waarschijnlijker wordt dat het spoor T niet van v_0 maar van v_k afkomstig is. Om uit te leggen hoe men dan te werk gaat eerst een korte uiteenzetting over T.

In de praktijk gebruikt men *Short Tandem Repeats* (STR) voor het DNA-profiel T; dit zijn korte stukjes (meestal niet-functioneel) DNA (in het eenvoudigste geval CA) op een bepaalde *locus* a, die zich een willekeurig aantal keer $\nu^{(a)}$ herhalen. Met N brokjes STR is het DNA-profiel T

$$T = (T^{(1)}, \ldots, T^{(N)}); \quad T^{(a)} = (\nu_1^{(a)}, \nu_2^{(a)}),\ a = 1, \ldots, N, \tag{20.6}$$

waarin voor iedere a de twee getallen $(\nu_1^{(a)}, \nu_2^{(a)})$ de *multipliciteiten* van de bewuste STR op *locus* a geven; de ene repetitie is afkomstig van de vader, de andere van de moeder (maar je weet i.h.a. niet welke). Het uit een dergelijk profiel verkregen bewijsmateriaal $E = (E^{(1)}, \ldots, E^{(N)})$ is dus *samengesteld*. Als de loci a van verschillende chromosomen komen mag je aannemen dat

$$P(E|H_k) = \prod_{a=1}^{N} P(E^{(a)}|H_k) = \prod_{a=1}^{N} P(\nu_1^{(a)}, \nu_2^{(a)}|H_k). \tag{20.7}$$

Onder de gebruikelijke aanname van *Hardy–Weinberg Evenwicht*, i.e. *random mating* in een grote populatie, geeft genetische theorie de volgende formules:

- Als $\nu_1^{(a)} \neq \nu_2^{(a)}$, dan geldt

$$P(\nu_1^{(a)}, \nu_2^{(a)}|H_k) = 2\kappa_0 P(\nu_1^{(a)})P(\nu_2^{(a)}) + \tfrac{1}{2}\kappa_1(P(\nu_1^{(a)}) + P(\nu_2^{(a)})) + \kappa_2; \tag{20.8}$$

- Als $\nu_1^{(a)} = \nu_2^{(a)}$, dan geldt

$$P(\nu_1^{(a)}, \nu_2^{(a)}|H_k) = \kappa_0 P(\nu^{(a)})^2 + \kappa_1 P(\nu^{(a)}) + \kappa_2, \tag{20.9}$$

waarbij $P(\nu^{(a)})$ de relatieve frequentie van $\nu^{(a)}$ in de totale (relevante) bevolking is, en κ_j de kans is dat v_k en v_0 *vanwege hun mogelijke verwantschap* (i.p.v. louter statistisch) j allelen delen. Deze kansen volgen uit elementaire genetica en staan in de volgende tabel:[5]

4. Jasper S. bekende nadat de DNA-*match* aan hem bekend werd gemaakt. Hoewel ruim 8000 mannen werden benaderd om mee te doen aan het DNA-onderzoek, waren slechts 900 daartoe bereid, onder wie vreemd genoeg Jasper S.! Als hij niet had bekend, had zijn advocaat kunnen betogen dat alle mannen uit Friesland hadden moeten worden getest. Daarmee waren we in het volgende scenario terechtgekomen en zou de kans op schuld van Jasper S. aanzienlijk zijn gedaald.

5. Deze tabel komt uit David J. Balding, *Weight-of-evidence for forensic* DNA*-profiles* (Wiley, Chichester, 2005), p. 91. De getallen voor halfbroer, halfzus, en grootouder zijn hetzelfde als voor tante en oom.

Familiegraad v_0-v_k	κ_0	κ_1	κ_2
eeneiïge tweeling	0	0	1
broer-zus etc.	1/4	1/2	1/4
ouder-kind	0	1	0
tante of oom-neef of nicht	1/2	1/2	0
neef-nicht etc.	3/4	1/4	0
achterneef-achternicht etc.	9/16	6/16	1/16
∞	1	0	0

In het extreme geval dat k en 0 een eeneiïge tweeling zijn geldt dus bijvoorbeeld

$$P(\nu_1^{(a)}, \nu_2^{(a)}|H_k) = 1. \tag{20.10}$$

Voor $\kappa_0 = \kappa_1 = \kappa_2 = \infty$ geven (20.8) en (20.9) daarentegen

$$\begin{aligned} P(\nu_1^{(a)}, \nu_2^{(a)}|H_k) &= 2P(\nu_1^{(a)})P(\nu_2^{(a)}) \quad \text{als } \nu_1^{(a)} \neq \nu_2^{(a)}; \\ P(\nu_1^{(a)}, \nu_2^{(a)}|H_k) &= P(\nu^{(a)})^2 \qquad\quad \text{als } \nu_1^{(a)} = \nu_2^{(a)} = \nu^{(a)}. \end{aligned} \tag{20.11}$$

Opgave 20.1

Bij de vliegramp in Tripoli op 12 mei 2010 zaten vele Nederlandse families in het vliegtuig. De DNA-identificatie van de slachtoffers is uitgevoerd door het Nederlands Forensisch Instituut met behulp van door de RU ontwikkelde software. Een sterk vereenvoudigd probleem is:
Onder de 103 omgekomen inzittenden bevindt zich slachtoffer v_0 met bekend DNA-profiel T_0. Een bepaald lijk met DNA-profiel T op de plaats van de crash geeft een match $T = T_0$. Verder blijkt uit de passagierslijst dat v_0 een broer, een tante, en een oom aan boord had. Stel nu dat het DNA-spoor T uit twee onafhankelijke delen bestaat, $T = (T^{(1)}, T^{(2)})$, met

$$T^{(1)} = (10, 10); \tag{20.12}$$
$$T^{(2)} = (6, 7). \tag{20.13}$$

De relatieve frequenties van deze STR's onder een karakteristieke bevolking zijn:

$$P(\nu^{(1)} = 10) = 0.3; \tag{20.14}$$
$$P(\nu^{(2)} = 6) = 0.2; \tag{20.15}$$
$$P(\nu^{(2)} = 7) = 0.1 \tag{20.16}$$

Wat is, op grond van deze informatie, de kans dat het lijk dat van slachtoffer v_0 is?

Appendix (Geen tentamenstof)
De formule (20.2) geldt voor daderidentificatie en slachtofferidentificatie. Bij vaderidentificatie komt er soms een correctiefactor 2, op grond van het volgende argument. Het DNA-profiel van de moeder wordt gebruikt om allelen te zoeken die zeker van de vader afkomstig zijn. Stel dat de baby op locus a een heterozygoot $E^{(a)} = (\nu_1^{(a)}, \nu_2^{(a)})$ is, dus met $\nu_1^{(a)} \neq \nu_2^{(a)}$, terwijl de moeder $(\nu_2^{(a)}, \nu_3^{(a)})$ heeft met $\nu_3^{(a)} \neq \nu_1^{(a)}$. Dan komt $\nu_2^{(a)}$ van de moeder, en $\nu_1^{(a)}$ dus van de vader. Ook bij een homozygoot $E^{(a)} = (\nu_1^{(a)}, \nu_1^{(a)})$ is het zeker dat $\nu_1^{(a)}$ van de vader komt. Met de notatie $T_0^{(a)} = (\mu_1^{(a)}, \mu_2^{(a)})$ voor het profiel van v_0 zijn er dan drie mogelijkheden:

$$\mu_1^{(a)} \neq \nu_1^{(a)}, \mu_2^{(a)} \neq \nu_1^{(a)} \quad \Rightarrow \quad P(E^{(a)}|H_0) = 0; \tag{20.17}$$
$$\mu_1^{(a)} \neq \mu_2^{(a)} = \nu_1^{(a)} \text{ of } \mu_2^{(a)} \neq \mu_1^{(a)} = \nu_1^{(a)} \quad \Rightarrow \quad P(E^{(a)}|H_0) = 1/2; \tag{20.18}$$
$$\mu_1^{(a)} = \mu_2^{(a)} = \nu_1^{(a)} \quad \Rightarrow \quad P(E^{(a)}|H_0) = 1. \tag{20.19}$$

Let op! In het licht van het bovenstaande verhaal betekent $P(E^{(a)}|H_0)$ in deze formules dus eigenlijk $P(E^{(a)}|H_0, E_m)$, waarbij E_m het DNA-profiel van de moeder is. Dat laatste wordt dus, net als het profiel E van de vermoedelijke vader v_0, als gegeven beschouwd. In het eerste geval (20.17) kan de verdachte niet de vader zijn.

21

Stochasten

We gaan in dot korte hoofdstuk wat verder met onze ontwikkeling van de kansrekening.

Definitie 21.1 *Stel dat X een eindige kansruimte is.*

- *Een* stochast *is een functie $f : X \to \mathbb{R}$.*
- *Het* spectrum *$\sigma(f)$ van een stochast f is het beeld van f (als deelverzameling van $\mathbb{R}$), i.e.,*

$$\sigma(f) := \{f(x) \mid x \in X\}. \tag{21.1}$$

- *Een kansfunctie $P : \mathcal{P}(X) \to [0,1]$ op X en een stochast $f : X \to \mathbb{R}$ geven samen een kansfunctie*

$$P_f : \mathcal{P}(\sigma(f)) \to [0,1] \tag{21.2}$$

op $\sigma(f)$ door middel van

$$P_f(A) := P(f^{-1}(A)). \tag{21.3}$$

Hier is $A \subset \sigma(f)$, en zoals gebruikelijk is $f^{-1}(A) := \{x \in X \mid f(x) \in A\}$.

De bijbehorende kans*verdeling* p_f op $\sigma(f)$, uitgedrukt in de kansverdeling (18.7) op X, is dan

$$p_f(\lambda) = \sum_{x \in X \mid f(x) = \lambda} p(x). \tag{21.4}$$

Als $\lambda \in \sigma(f)$ niet ontaard is, in de zin dat er precies één $x \in X$ is met $f(x) = \lambda$, luidt (21.4) simpelweg

$$p_f(\lambda) = p(x), \;\; x = f^{-1}(\{\lambda\}). \tag{21.5}$$

Een speciale kansverdeling op X is de *puntmaat* p^y, voor vaste $y \in X$, gedefinieerd door

$$p^y(x) = 1 \text{ als } x = y; \tag{21.6}$$
$$p^y(x) = 0 \text{ als } x \neq y. \tag{21.7}$$

De bijbehorende kansfunctie $P^y : \mathcal{P}(X) \to [0,1]$ wordt dan gegeven op $C \subset X$ door

$$P^y(C) = 1 \text{ als } y \in C; \tag{21.8}$$
$$P^y(C) = 0 \text{ als } y \notin C. \tag{21.9}$$

Hierbij is er dus geen onzekerheid over de uitkomst van het kansexperiment: die is altijd y.

De kansverdeling $p^y_f : \sigma(f) \to [0,1]$ van een willekeurige stochast f t.o.v. p^y is dan (ga na):

$$p^y_f(\lambda) = 1 \text{ als } f(y) = \lambda; \tag{21.10}$$
$$p^y_f(\lambda) = 0 \text{ als } f(y) \neq \lambda. \tag{21.11}$$

Een speciale *stochast* is een *karakteristieke functie* χ_B, gedefinieerd voor vaste $B \subset X$, waarbij

$$\chi_B(x) = 1 \text{ als } x \in B; \tag{21.12}$$
$$\chi_B(x) = 0 \text{ als } x \notin B. \tag{21.13}$$

Het spectrum van χ_B is uiteraard

$$\sigma(\chi_B) = \{0, 1\}. \tag{21.14}$$

Voor iedere kansverdeling p op X is er dus een kansverdeling $p_{\chi_B} \equiv p_B$ op $\{0, 1\}$, nl.

$$p_B(0) = P(B^c); \tag{21.15}$$
$$p_B(1) = P(B), \tag{21.16}$$

waarbij P de kansfunctie is die bij de kansverdeling p hoort volgens (18.6) en (18.7).

Definitie 21.2 *De* verwachtingswaarde *en de* dispersie *van een stochast f t.o.v. een kansverdeling p zijn*

$$E_p(f) := \sum_{x \in X} f(x)p(x); \tag{21.17}$$
$$\Delta_p(f) := E_p(f^2) - E_p(f)^2. \tag{21.18}$$

Hier is $f^2 : X \to \mathbb{R}$ de functie $x \mapsto f(x)^2$. Uit (21.17) volgt de alternatieve uitdrukking

$$E_p(f) = \sum_{\lambda \in \sigma(f)} \lambda \cdot p_f(\lambda). \tag{21.19}$$

We zien dat $\Delta_p(f)$ niet-negatief is, omdat, met de notatie 1_X voor de functie $x \mapsto 1$ voor alle $x \in X$,

$$\Delta_p(f) = E_p((f - E_p(f) \cdot 1_X)^2), \tag{21.20}$$

zodat de *standaardafwijking* $\sqrt{\Delta_p(f)}$ is gedefinieerd, Voor een puntmaat $p = p^y$ volgt uit (21.19) dat

$$E_{p^y}(f) = f(y); \tag{21.21}$$
$$\Delta_{p^y}(f) = 0. \tag{21.22}$$

Ook het omgekeerde geldt, en bevestigt je intuïtie over de dispersie c.q. de standaardafwijking:

Stelling 21.1 *Een kansverdeling p op X is van de vorm $p = p^y$ voor een zekere $y \in X$ desda $\Delta_p(f) = 0$ voor alle stochasten f op X.*

Het bewijs in de richting "$\Rightarrow$" is uiteraard bevat in (21.22). Voor "$\Leftarrow$": kies $f = p^y$, zodat $f^2 = f$. Dan is $\Delta_p(f) = p(y) - p(y)^2$. Uit de aanname $\Delta_p(f) = 0$ voor alle f volgt, door voor f te kiezen $f = \delta_z$ met $\delta_z(x) = \delta_{xz}$, dat $p(y) = 0$ of $p(y) = 1$ voor alle $y \in X$. Uit axioma (18.5) volgt nu dat $p(y) = 1$ voor precies één y, zodat $p = p^y$. Q.E.D.

Opgave 21.1

Leid de volgende uitdrukkingen af: (21.4), (21.8) - (21.9), (21.15) - (21.16), (21.19).

22

Kansrekening en klassieke natuurkunde

De klassieke natuurkunde is wiskundig gesproken niets anders dan een interpretatie van de kansrekening: preciezer gezegd, de zuiver wiskundige structuren van de kansrekening worden 'waargemaakt' door wiskundige modellen en begrippen uit de natuurkunde. Dit verhaal staat op zich, maar een belangrijk doel hierbij is het contrast met de kwantummechanica straks. Het gaat als volgt.[1]

C1 De *faseruimte* van een fysisch systeem is een kansruimte X (hier eindig verondersteld).

C2 Een *fysische grootheid* of *observabele* van dit systeem is een stochast (i.e. een functie $f : X \to \mathbb{R}$).

C3 Een *toestand* van het systeem is een kansverdeling p (of een kansfunctie P) op X.

C4 Een *zuivere* toestand is een puntmaat p^y op X (of, equivalent, een punt $y \in X$).[2]

C5 De *toestandsruimte* van het systeem is de verzameling $K(X)$ van alle kansverdelingen op X.

C6 De *waarde* van een observabele f in een zuivere toestand p^y is $f(y)$.

C7 De *gemiddelde waarde* van een observabele f in een willekeurige toestand p is $E_p(f)$.

C8 Wanneer het systeem zich in een toestand p bevindt, dan is de kans dat een meting van f een waarde $\lambda \in \sigma(f)$ geeft, genoteerd $P(f = \lambda)$, gelijk aan $p_f(\lambda)$.[3]

Het idee achter deze kanstheoretische opzet is dat het systeem zich in werkelijkheid altijd in een zuivere toestand bevindt, maar dat wij deze door gebrek aan kennis en rekencapaciteit meestal niet kennen (denk bijv. aan de precieze plaatsen en impulsen in een systeem met 10^{23} deeltjes). De precieze toestand wordt dan vervangen door een bepaalde kansverdeling over mogelijke toestanden (zie onder).[4]

Het eenvoudigste voorbeeld is $X = \underline{2}$, de verzameling met twee elementen. Informatici beschouwen $\underline{2}$ als een *bit* en schrijven daarom graag $\underline{2} = \{0, 1\}$. Fysici denken eerder aan een deeltje met twee toestanden, zeg 'spin up' en 'spin down', en schrijven daarom $\underline{2} = \{\uparrow, \downarrow\}$ of $\{-1, 1\}$. Hoe dan ook geldt

$$K(\underline{2}) \cong [0, 1], \tag{22.1}$$

waarmee we voorlopig bedoelen dat er een bijectie $\varphi : K(\underline{2}) \to [0, 1]$ bestaat, bijvoorbeeld $\varphi(p) = p(0)$ (immers $p(1) = 1 - p(0)$, zodat de kansverdeling $p \in K(\underline{2})$ geheel is bepaald door haar waarde in 0).

De afbeelding φ is echter meer dan alleen een bijectie: het is een functie die de *convexe structuur* behoudt. Merk eerst op dat de verzameling $V(X)$ van alle functies van X naar $\mathbb{R}$ een reële vector-ruimte is: optelling en scalaire vermenigvuldiging gaan puntsgewijs, i.e.,[5]

$$(f + g)(x) := f(x) + g(x); \tag{22.2}$$

$$(\lambda f)(x) = \lambda f(x),\ \lambda \in \mathbb{R}. \tag{22.3}$$

Definitie 22.1 *Een deelverzameling K van een reële vector-ruimte V heet* convex *als voor alle $v, w \in K$ en $\lambda \in (0, 1)$ geldt dat $\lambda v + (1 - \lambda)w \in K$, en* compact *als K gesloten en begrensd is.*

---

1. We laten eventuele axioma's over de tijdsevolutie van toestanden of observabelen hier weg.
2. Een punt $y \in X$ is natuurlijk niet hetzelfde als de kansverdeling p^y, maar voor het gemak halen we deze door elkaar. Officieel is het beter om een afbeelding $\iota : X \to K(X)$ te definiëren door $\iota(y) = p^y$, waar $K(X)$ in het volgende item wordt ingevoerd.
3. **C8** is equivalent met de uitspraak: Wanneer het systeem zich in een toestand p bevindt (met bijbehorende kansfunctie P), dan is de kans dat een meting van f een waarde $\lambda \in A$ geeft (met $A \subset \sigma(f)$) gelijk aan $P_f(A)$.
4. Toestanden die niet de werkelijke stand van zaken weergeven maar slechts onze kennis daarvan heten *epistemisch*.
5. Je kunt makkelijk nagaan dat $V(X)$ zo aan de axioma's van een reële vector-ruimte voldoet: het nulelement is bijvoorbeeld de functie $0(x) = 0$ voor alle x, en de inverse van f onder optelling is $-f$. Voor $X = \underline{2}$ geldt $V(\underline{N}) \cong \mathbb{R}^N$, ga na!

Je kunt de definitie van een convexe deelruimte K van een reële vector-ruimte V vergelijken met de definitie van een *lineaire* deelruimte L van V: dan moet voor alle vectoren $v, w \in L$ en $\lambda \in \mathbb{R}$ gelden dat $\lambda v + w \in L$. Een lineaire deelruimte is dus zeker convex, maar nooit compact: 'mooie' convexe verzamelingen zijn bovendien compact. Neem bijvoorbeeld $K = [0, 1]$ of $D = \{(x, y) \in \mathbb{R}^2 \mid x^2 + y^2 \leq 1\}$.

Stelling 22.1 *Voor een eindige kansruimte X is de toestandsruimte $K(X)$ een compacte convexe verzameling in de reële vector-ruimte $V(X)$.*

Het bewijs is een opgave. We bekijken nu wat ingewikkeldere voorbeelden, waarin N bits worden gecombineerd. Met de notatie $\underline{N} = \{0, 1, \ldots, N-1\}$, de verzameling met N elementen dus, nemen we

$$X_N = \underline{2}^{\underline{N}} := \{s : \underline{N} \to \underline{2}\}, \tag{22.4}$$

de verzameling van alle functies van $\underline{N}$ naar $\underline{2}$. Voor een informaticus is een element $x \in X_N$ van de vorm zeg $x = 011 \cdots 10$, waarmee wordt bedoeld $s(0)s(1)s(2) \cdots s(N-2)s(N-1)$. Dit is in feite een manier om de grafiek van s te schrijven. Een fysicus zou hetzelfde element schrijven als $x = \downarrow\uparrow\uparrow \cdots \uparrow\downarrow$.

De vraag is nu: in welke toestand is het systeem eigenlijk? In de fysica wordt deze vraag grotendeels beantwoord door een speciale observabele, de *hamiltoniaan* $h : X \to \mathbb{R}$, en door de *temperatuur* $T \geq 0$.

- Bij $T = 0$ bevindt het systeem zich in een *grondtoestand*: dit is een punt $x_0 \in X$ dat h minimaliseert (met andere woorden, $h(x_0) \leq h(x)$ voor alle $x \in X$).
- Bij $T > 0$ bevindt het systeem zich in een *evenwichtstoestand*:[6] dit is de kansverdeling

  $$p_T(x) = \frac{1}{Z_T} e^{-h(x)/T}, \tag{22.5}$$

  waarbij de *partitiefunctie* (nodig om te garanderen dat $\sum_x p_T(x) = 1$) is gegeven door

  $$Z_T = \sum_{x \in X} e^{-h(x)/T}. \tag{22.6}$$

De hamiltoniaan zegt vrijwel alles over een gegeven systeem. Voor X_N is een typisch voorbeeld

$$h(s) = -J \sum_{i=0}^{N-1} s(i)s(i+1) + B \sum_{i=0}^{N-1} s(i), \tag{22.7}$$

waarbij J en B constanten zijn, $s(N) \equiv s(0)$ (periodieke randvoorwaarden), en we $\underline{2}$ realiseren als $\{-1, 1\}$. Voor $B = 0$ en $J > 0$ volgt dat er twee grondtoestanden zijn: $s_0^{\pm}$, gegeven door $s_0^{\pm}(i) = \pm 1$ voor alle i. Voor $J = 0$ en $B > 0$ is er een unieke grondtoestand s_0, namelijk $s_0(i) = -1$ voor alle i.

Opgave 22.1

Bewijs Stelling 22.1 (bewijs compactheid is als bonus).

Opgave 22.2

In de twee zojuist besproken situaties, i.e., $B = 0, J > 0$ en $B > 0, J = 0$, wat is per geval de limiet voor $T \to 0$ van de kansverdeling p_T voor de Hamiltoniaan (22.7)?

Opgave 22.3

De *rand* ∂K van een convexe verzameling K bestaat uit alle punten $u \in K$ waarvoor geldt: als $u = \lambda v + (1 - \lambda)w$ voor zekere $v, w \in K$ en $\lambda \in (0, 1)$, dan volgt $v = w = u$.

a) Wat is de rand van $K = [0, 1]$? Bewijs je antwoord.

b) Wat is de rand van een gelijkzijdige driehoek inclusief interieur (gezien als convexe deelverzameling van $\mathbb{R}^2$)?

c) Bewijs voor iedere eindige kansruimte X dat $\partial K(X) = X$, waarbij we X identificeren met de verzameling van alle kansverdelingen van de vorm $p = p^y$, $y \in X$.

---

6. We nemen de constante van Boltzmann $k_B = 1$; anders komt er $\exp(-h(x)/k_B T)$.

23

Kansrekening en kwantummechanica

Met de wiskundige opzet uit het vorige hoofdsuk kon alle tot 1900 bekende fysica (in principe) worden beschreven. Rond 1900 werden echter verschijnselen als radioactiviteit en de precieze eigenschappen van warmtestraling bekend, die niet zo één twee drie door de klassieke natuurkunde verklaard konden worden. Dit leidde tot een periode van grote verwarring, die duurde van 1900 tot 1925.

In januari 1926 waren er twee nieuwe theorieën op de markt, genaamd *matrixmechanica* en *golfmechanica*. De eerste, opgesteld door Werner Heisenberg (1901–1976), draaide zoals de naam al suggereert om het gebruik van matrices, waar fysici in die tijd allerminst mee vertrouwd waren en dan ook enorm van schrokken. De tweede theorie, afkomstig van Erwin Schrödinger (1887–1961), was eveneens op geavanceerde wiskunde gebaseerd, maar deze wiskunde was de theorie van partiële differentiaalvergelijkingen, die in die tijd alle fysici en wiskundigen beheersten (dat is nu helaas niet meer het geval). Schrödinger ging uit van de voorstelling dat alle vormen van materie (en dus ook deeltjes zoals elektronen) golven zijn. Schrödinger was niet alleen in zijn wiskunde veel conservatiever dan Heisenberg. Hij benadrukte zowel het aanschouwelijke karakter van zijn theorie als zijn visie dat deze deterministisch zou zijn. Hij bleek echter niet in staat deze visie waar te maken.

Toen vond een beslissende wending plaats. Max Born (1882–1970) stelde nog in datzelfde jaar (1926) voor om de 'materiegolven' van Schrödinger niet als fysische golven (zoals licht of geluid) te interpreteren, maar als wiskundige uitdrukkingen voor *kansen*. Een typisch citaat uit het artikel van Born is:

> "De kwantummechanica geeft geen antwoord op de vraag: 'wat is de toestand na de botsing?', maar uitsluitend op: 'wat is de kans op een bepaalde uitkomst van de botsing?'"

Born liet daarbij in het midden of de begintoestand (vóór de botsing) in principe nog wel perfect bepaald kon worden (zodat het toeval uitsluitend een gevolg zou zijn van een indeterministische tijdsevolutie). Maar het jaar daarop (1927) nam Heisenberg ook die illusie weg: in zijn artikel wordt aangetoond dat

> "canoniek geconjugeerde dynamische variabelen slechts gelijktijdig kunnen worden bepaald met een karakteristieke onzekerheid. Deze onzekerheid vormt de fundamentele oorzaak van het statistische karakter van de kwantummechanica."

De ideeën van Born en Heisenberg vormden een keerpunt in de geschiedenis van de natuurwetenschap: het was de eerste keer dat kansen een fundamentele plaats kregen in de natuur (en niet slechts gebruikt werden om een gebrek aan kennis op te vangen). Dit idee werd direct overgenomen door Niels Bohr (1885–1962), de toonaangevende fysicus van die tijd, en vond spoedig daarna (en ook nu nog) vrijwel algehele instemming. In 1927 lieten de natuurkundige Paul Dirac (1902–1984) en de wiskundige John von Neumann (1903–1957) zien hoe de theorieën van Heisenberg en Schrödinger samenhingen. Ze stelden een algemene theorie op die nu als *kwantummechanica* bekend staat. De materiegolven van Schrödinger werden nu geïnterpreteerd als *toestanden* van een kwantummechanisch systeem (te vergelijken met het geheel van alle plaatsen en snelheden van deeltjes dat de toestand van een klassieke systeem bepaalt), terwijl álle toestanden in de kwantumtheorie (en niet alleen materiegolven, zoals bij Born) sindsdien een zuiver kanstheoretische rol spelen. De kwantumtheorie voorspelt daarmee geen individuele gebeurtenissen, maar slechts de kans daarop.

Niettemin gelden de axioma's uit het vorige hoofdstuk ook voor de kwantummechanica, *mits alle wiskundige termen in de axioma's geherinterpreteerd worden*. Dit werd voor het eerst in 1925 ingezien door Heisenberg, maar de wiskundig correcte herinterpretatie werd in 1932 gegeven door von Neumann (en geldt nog steeds). Deze is volgt (lees desgewenst eerst Chapter 6 van Friedberg et al, *Linear Algebra*, Fourth Ed., met name Theorem 6.25; we gebruiken de notatie uit dat boek).

- De kansruimte wordt vervangen door een zogenaamde *Hilbert-ruimte* H. Dit is een bepaald soort complexe vector-ruimte met inproduct; de complicaties in de definitie (die we hier weglaten) zijn alleen van belang als H oneindig-dimensionaal is (zie het derdejaars vak Inleiding Functionaalanalyse). Het analogon van de aanname dat de klassieke kansruimte eindig is, is nu dat de Hilbert-ruimte eindig-dimensionaal is, en daarmee van de vorm $H = \mathbb{C}^n$, met inproduct

$$\langle v, w\rangle = \sum_{i=1}^{n} \overline{v}_i w_i. \tag{23.1}$$

- De toestand (klassiek een kansverdeling) wordt in de kwantumtheorie een *kansoperator*: i.e. een hermitische operator $\mathsf{P} : \mathbb{C}^n \to \mathbb{C}^n$ met positieve eigenwaarden $(p_1, \ldots, p_n)$ die voldoen aan

$$\sum_{i=1}^{n} p_i = 1. \tag{23.2}$$

  De eigenwaarden van P gedragen zich dus als klassieke kansen, preciezer: ze vormen een kansverdeling op de kansruimte $\{1, 2, \ldots, n\}$, met $p_i \equiv p(i)$. Een voorbeeld van een kansoperator is $\mathsf{P} = I/n$, waarbij I de eenheid $I(v) = v$ is. Deze P heeft één positieve eigenwaarde $p = 1/n$ met multipliciteit n, oftewel $p_1 = \cdots = p_n = 1/n$, zodat (23.2) geldt.
  We kunnen de definitie van een kansoperator ook abstracter opschrijven met behulp van de *trace* (oftewel het 'spoor', zie onder): een *kansoperator* P is per definitie positief[1] en voldoet aan

$$\mathrm{Tr}\,(\mathsf{P}) = 1. \tag{23.3}$$

  Hierbij is $\mathrm{Tr}\,(\mathsf{T})$ voor een willekeurige operator T gedefinieerd als de som van de eigenwaarden van T, waarbij een gegeven eigenwaarde zo vaak wordt meegeteld als haar multipliciteit (dus $\mathrm{Tr}\,(I) = n$). Het is voor berekeningen handig om een equivalente definitie van de trace te geven: kies een willekeurige *orthonormale* basis $\beta = (u_1, \ldots, u_n)$ van $\mathbb{C}^n$ (i.e., $\langle u_i, u_j\rangle = \delta_{ij}$), en definieer

$$\mathrm{Tr}\,(\mathsf{T}) = \sum_{i=1}^{n} \langle u_i, \mathsf{T}(u_i)\rangle. \tag{23.4}$$

  Een opgave uit Lineaire Algebra toont aan dat het rechterlid *onafhankelijk is van de basiskeuze*, zolang deze basis maar orthonormaal is. Je kunt dus voor een gegeven T de handigste basis kiezen. Als T hermitisch is neem je bijvoorbeeld de basis (v_i) van eigenvectoren van T, zodat we onze oorspronkelijke definitie van het spoor als de som van de eigenwaarden terugvinden:

$$\mathrm{Tr}\,(\mathsf{T}) = \sum_{i=1}^{n} \langle v_i, \lambda_i v_i\rangle = \sum_{i=1}^{n} \lambda_i \langle v_i, v_i\rangle = \sum_{i=1}^{n} \lambda_i \delta_{ii} = \sum_{i=1}^{n} \lambda_i. \tag{23.5}$$

- Een stochast of observabele is in de kwantummechanica een *hermitische* $n \times n$ operator T. Het spectrum $\sigma(\mathsf{T})$ van T is nu de verzameling eigenwaarden van T; deze zijn reëel, dus $\sigma(\mathsf{T}) \subset \mathbb{R}$. We schrijven $\sigma(\mathsf{T}) = \{\lambda_1, \ldots, \lambda_k\}$, waarin iedere eigenwaarde λ_i precies één keer voorkomt (ook als deze ontaard is, i.e., een hoger-dimensionale eigenruimte heeft). We noteren de eigenruimte bij λ_i als W_i, met bijbehorende orthogonale projectie T_i, zodat $\mathsf{T}_i^* = \mathsf{T}_i^2 = \mathsf{T}_i$, $\mathsf{T}_i\mathsf{T}_j = \delta_{ij}\mathsf{T}_i$, en

$$W_1 \oplus \cdots \oplus W_k = \mathbb{C}^n; \tag{23.6}$$
$$\mathsf{T}_1 + \ldots + \mathsf{T}_k = I; \tag{23.7}$$
$$\lambda_1 \cdot \mathsf{T}_1 + \ldots + \lambda_k \mathsf{T}_k = \mathsf{T}. \tag{23.8}$$

- Een kansoperator P en een hermitische operator T geven samen een kansverdeling p_T (niet te verwarren met het karakteristiek polynoom van T!) op het spectrum $\sigma(\mathsf{T})$ d.m.v.

$$\mathsf{p}_\mathsf{T}(\lambda_i) = \mathrm{Tr}\,(\mathsf{P}\mathsf{T}_i), \tag{23.9}$$

  waarin opnieuw de trace Tr voorkomt. Dit is de *Born-regel* (in deze vorm echter afkomstig van von Neumann), waar vrijwel alle voorspellingen van de kwantummechanica op gebaseerd zijn.

1. Een operator T heet *positief* als $\langle v, \mathsf{T}(v)\rangle \geq 0$ voor alle $v \in \mathbb{C}^n$. Dit blijkt het geval desda T hermitisch is en al zijn eigenwaarden positief zijn, dus $\lambda_i \geq 0$ voor alle $\lambda_i \in \sigma(\mathsf{T})$.

Stelling 23.1 *De bovenstaande uitdrukking definieert een kansverdeling op $\sigma(\mathsf{T})$, i.e., er geldt*

$$\mathsf{p}_\mathsf{T}(\lambda_i) \geq 0; \tag{23.10}$$

$$\sum_{i=1}^{k} \mathsf{p}_\mathsf{T}(\lambda_i) = 1. \tag{23.11}$$

Het bewijs van (23.11) is het eenvoudigst: uit (23.4) volgt dat de trace linear is, zodat

$$\sum_{i=1}^{k} \mathsf{p}_\mathsf{T}(\lambda_i) = \sum_{i=1}^{k} \mathrm{Tr}\,(\mathsf{P}\mathsf{T}_i) = \mathrm{Tr}\,(\mathsf{P}\sum_{i=1}^{k} \mathsf{T}_i) = \mathrm{Tr}\,(\mathsf{P}) = 1,$$

waarbij we onderdeel (23.7) van de spectraalstelling hebben gebruikt.

Om (23.10) te bewijzen gebruiken we in de definitie (23.4) van de trace de basis van eigenvectoren (u_i) van P (deze operator is hermitisch en heeft dus een orthonormale basis van eigenvectoren):

$$\begin{aligned}
\mathsf{p}_\mathsf{T}(\lambda_i) &= \mathrm{Tr}\,(\mathsf{P}\mathsf{T}_i) = \sum_{j=1}^{n} \langle u_j, (\mathsf{P}\mathsf{T}_i)(u_j)\rangle = \sum_{j=1}^{n} \langle \mathsf{P}^*(u_j), \mathsf{T}_i(u_j)\rangle \\
&= \sum_{j=1}^{n} \langle \mathsf{P}(u_j), \mathsf{T}_i(u_j)\rangle = \sum_{j=1}^{n} \langle p_j u_j, \mathsf{T}_i(u_j)\rangle = \sum_{j=1}^{n} p_j \langle u_j, \mathsf{T}_i(u_j)\rangle \\
&= \sum_{j=1}^{n} p_j \langle u_j, \mathsf{T}_i^*\mathsf{T}_i(u_j)\rangle = \sum_{j=1}^{n} p_j \langle \mathsf{T}_i(u_j), \mathsf{T}_i(u_j)\rangle = \sum_{j=1}^{n} p_j \|\mathsf{T}_i(u_j)\|^2 \geq 0,
\end{aligned}$$

waar we achtereenvolgens hebben gebruikt $\mathsf{P}^* = \mathsf{P}$ (want P is per definitie hermitisch) en $\mathsf{T}_i = \mathsf{T}_i^*\mathsf{T}_i$ (hetgeen geldt omdatT_i een orthogonale projectie is, ga na). Q.E.D.

Op deze manier ontstaan op een volkomen onverwachte wijze kansverdelingen op spectra van fysische grootheden. Net als in het klassieke geval zijn de kansverdelingen op alle observabelen T (voor een gegeven fysisch systeem met Hilbert-ruimte H) uiteindelijk afkomstig van één enkele toestand, namelijk de kansoperator P; het grote verschil is dat deze kwantumtoestand niet zelf een kansverdeling is.

Er zijn twee mooie speciale gevallen van de Born-regel (23.9), die ook gecombineerd kunnen worden:

- Als $\lambda_i \in \sigma(a)$ enkelvoudig is (dus niet ontaard), met andere woorden, als de bijbehorende eigenruimte W_i ééndimensionaal is, opgespannen door één enkele eenheidsvector v_i, dan geldt

  $$\mathsf{p}_\mathsf{T}(\lambda_i) = \langle v_i, \mathsf{P}(v_i)\rangle. \tag{23.12}$$

  Bereken het spoor in (23.9) namelijk m.b.v. (23.4) en kies daarvoor nu een basis van eigenvectoren van T. Één van die basisvectoren, zeg v_1, is v_i, en de andere, v_2 t/m v_n, staan daar loodrecht op. Dan geven (23.9) en (23.4), de laatste uiteraard met $\mathsf{P}\mathsf{T}_i$ i.p.v. T en v_i i.p.v. u_i, direct (23.10).
- Een speciale klasse kansmatrices wordt als volgt verkregen: kies een eenheidsvector $\psi \in \mathbb{C}^n$, zodat $\langle \psi, \psi\rangle = 1$, en definieer de operator P^ψ door

  $$\mathsf{P}^\psi(v) := \langle \psi, v\rangle \psi. \tag{23.13}$$

  Dit is precies de projectie op de ééndimenionale lineaire deelruimte $L = \mathbb{C}\cdot\psi$. Dit is een kansoperator (opgave), en de bijbehorende versie van de Born-regel (23.9) is

  $$\mathsf{p}_\mathsf{T}^\psi(\lambda_i) = \langle \psi, \mathsf{T}_i(\psi)\rangle = \|\mathsf{T}_i(\psi)\|^2. \tag{23.14}$$

- Gecombineerd geeft dit: als $\lambda_i \in \sigma(a)$ enkelvoudig is, met eigenvector v_i (en $\|v_i\| = 1$), dan geldt

  $$\mathsf{p}_\mathsf{T}^\psi(\lambda_i) = |\langle v_i, \psi\rangle|^2. \tag{23.15}$$

Opgave 23.1

Neem $n = 2$, dus $H = \mathbb{C}^2$ (dit is de Hilbert-ruimte van een *qubit*), neem als toestand P^ψ met

$$\psi = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ 1 \end{pmatrix}, \tag{23.16}$$

en kies als observabele

$$\mathsf{T} = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}. \tag{23.17}$$

Geef $\sigma(\mathsf{T})$ en bereken de kansen (23.15) voor de (beide) elementen $\lambda_i \in \sigma(\mathsf{T})$.

Opgave 23.2

De *verwachtingswaarde* en de *dispersie* van een hermitische matrix T t.o.v. een kansoperator P worden analoog aan (21.17) gegeven door

$$E_{\mathsf{P}}(\mathsf{T}) := \mathrm{Tr}\,(\mathsf{PT}); \tag{23.18}$$
$$\Delta_{\mathsf{P}}(\mathsf{T}) := E_{\mathsf{P}}(\mathsf{T}^2) - E_{\mathsf{P}}(\mathsf{T})^2. \tag{23.19}$$

a) Laat zien dat $E_{\mathsf{P}}(\mathsf{T}) = \sum_{i=1}^{k} \lambda_i \cdot \mathsf{p}_{\mathsf{T}}(\lambda_i)$, waarbij $\sigma(\mathsf{T}) = \{\lambda_1, \ldots, \lambda_k\}$.
b) Laat zien dat $\Delta_{\mathsf{P}}(\mathsf{T}) \geq 0$.

Opgave 23.3

Laat zien dat P^ψ in (23.13) inderdaad een kansoperator is en leid (23.14) af.

Opgave 23.4

a) Bewijs dat voor een eindig-dimensionale Hilbert-ruimte $H = \mathbb{C}^n$ de verzameling $P(H)$ van alle kansoperatoren op H een convexe deelverzameling is van de reële vector-ruimte van alle hermitische operatoren op H. (N.B. $P(H)$ is tevens compact, maar dat krijg je cadeau!).
b) Laat zien dat de rand $\partial P(H)$ (zie Opgave 22.3) precies bestaat uit alle kansoperatoren van de vorm P^ψ in (23.13), waarbij ψ de eenheidsvectoren in H doorloopt (*bonusopgave*).