Krachtige bewijzen

Rosalie Iemhoff

August 31, 2011

In 2009 werd mij door de Nederlandse Wetenschaps Organisatie een Vidi beurs toegekend voor het project "The power of constructive proofs". Het project is wiskundig van aard en valt binnen het NWO gebiedsbestuur Exacte Wetenschappen. Op uitnodiging van het ANTW heb ik een artikel geschreven dat gaat over die vakgebieden in de wiskundige logica, de Bewijstheorie en het Constructivisme, waarop het project betrekking heeft. Het is geen alomvattend overzicht van die gebieden, maar belicht die thema's die voor het project van belang zijn.

1 Bewijzen

Quod erat demonstradum, dat is waar Euclides, in de afgekorte vorm Q.E.D., zijn bewijzen die hij meer dan tweeduizend jaar geleden optekende, mee afsloot. En terecht: de wiskundige bewijzen van Euclides in zijn boek *Elementen* zijn helder en precies en de schrijver heeft getracht om zijn redeneringen te ontleden in aanschouwelijke axioma's en beweringen die daaruit volgen. Hierdoor voldoet het merendeel van de bewijzen in de *Elementen* aan dat wat van een bewijs gevraagd wordt: ze leiden tot de overtuiging dat dat wat bewezen wordt waar is.

Niet alle uitspraken lenen zich voor een dergelijke aanpak. Wanneer 's avonds in de tuin in Combray de tuinbel klinkt, dan is dat een bewijs dat de klepel tegen de klok geslagen heeft. Het bewijs heeft weliswaar een andere vorm dan de bewijzen in de Elementen, maar voldoet aan hetzelfde criterium: de overtuiging dat de bijbehorende bewering waar is.

De meeste concepten in de wiskunde zijn minder tastbaar dan een klepel en een klok, en die grote mate van abstractie en het daarmee gepaard gaande feit dat haar beweringen zelden door de natuur, dat wil zeggen door metingen of andere observaties, bevestigd of ontkracht kunnen worden, leidt tot de behoefte haar beweringen te rechtvaardigen op de wijze van Euclides. De concepten worden door middel van definities en axioma's zo nauwkeurig mogelijk beschreven en de bewijzen worden, voor zover mogelijk, ontleed in argumenten waarvan de correctheid hetzij reeds bewezen hetzij evident is.

De Bewijstheorie is het vakgebied in de wiskunde dat deze gestructureerde vorm van bewijzen bestudeert. In het hierna volgende zal ik beschrijven hoe deze tak

van de wiskunde is ontstaan, om vervolgens dat onderwerp te belichten dat betrekking heeft op het project, namelijk *constructieve bewijzen*.

2 De grondslagencrisis

Tot de 19e eeuw beschouwde men de wiskundige objecten die werden bestudeerd, objecten zoals getallen, oppervlakken en continue functies, over het algemeen als intuïtief duidelijk en onproblematisch. Maar met de opkomst van steeds abstractere noties, zoals verzamelingen en wonderlijke functies, nam het verlangen toe om de wiskunde van een stevig fundament te voorzien, door het crëeren van een systeem waarin alle wiskunde gerepresenteerd kan worden, en dat bovendien uit axioma's bestaat waarvan de waarheid boven twijfel verheven is. Zo een systeem zou weliswaar niet noodzakelijk de vraag naar de ontologische status van de wiskunde beantwoorden, maar het zou haar in ieder geval vrijwaren van onwaarheden.

Deze positie, waarin de wiskundige wereld zich aan het eind van de negentiende eeuw bevond, leidde tot verschillende pogingen dergelijke grondslagen voor de wiskunde te formuleren. Verassend was vervolgens wat Bertrand Russell aantoonde: dat ogenschijnlijk onschuldige aannames in die systemen tot tegenspraken leiden [15]. Russells paradox impliceert niet dat de wiskunde niet klopt, geenszins, maar illustreert wel de problematiek bij het in woorden vangen, dat wil zeggen het axiomatiseren, van zulke abstracte concepten als bijvoorbeeld verzamelingen.

Wanneer in een proces aangaande een inbraak het slachtoffer zegt door de aangeklaagde bestolen te zijn, terwijl de aangeklaagde dat ontkent, dan zijn die twee uitspraken in tegenspraak met elkaar, samen zij zijn inconsistent. Er zal gezocht worden naar bewijsmateriaal dat hetzij de uitspraak van de een, hetzij die van de ander ondersteunt. En als dat niet gevonden wordt gaat ieder zijns weegs. De tegenspraak doet ons niet twijfelen aan de wereld, omdat zij ontstond door twee uitspraken die zonder bewijs niet op voorhand voor waar werden gehouden. Maar als beweringen die voor waar gehouden worden tot een tegenspraak leiden is dat schokkend. En als die uitspraken betrekking hebben op de grondslagen van de wiskunde, op het fundament voor de wiskunde dat men aan het bouwen is, dan stort dat bouwwerk ineen. De dramatiek van die toestand spreekt uit de naam die zij heeft gekregen: de *grondslagencrisis*.

Hoewel de grondslagencrisis zeker niet iedereen bezighield, veel wiskundigen hebben een uiterst Platonische opvatting van de wiskunde, leidde het tot een verhit en polemisch debat over de vraag wat dan wel de juiste opvatting van de wiskunde is en wat haar grondslagen (haar fundament, haar basis) zijn. De meningen verschilden, maar voor dit artikel is vooral van belang hoe de wiskundige David Hilbert uit Göttingen in de twintiger jaren van de vorige eeuw op de grondslagencrisis reageerde [10, 11]. Hij zette in op het vinden van een finitistisch systeem van axioma's en regels, waarvan wordt aangetoond dat de wiskunde uiteindelijk daartoe herleid kan worden. Het epistemologische

karakter van finitistisch redeneren zou dan een rechtvaardiging vormen voor de gehele wiskunde. Deze aanpak wordt sindsdien *Hilberts programma* genoemd. De wiskundige Kurt Gödel bewees echter in 1931 dat een dergelijke aanpak niet kan slagen. Hiermee werd *Hilberts programma*, in de enge zin van het woord, ontkracht. Maar de studie van bewijzen was ontstaan, en daarmee dat vakgebied in de wiskundige logica dat later *Bewijstheorie* is gaan heten.

3 Opvattingen van de wiskunde

Zoals vaak wanneer een concept gepreciseerd wordt ontstaan er verschillende opvattingen over de juiste interpretatie ervan. Dat is in het geval van bewijzen ook zo. De grondslagencrisis was gedeeltelijk een debat over de waarheid van de logische redeneringen die in bewijzen gebruikt worden. Men was het niet eens. Er ontstonden bekende opvattingen van de wiskunde, zoals het *Intuïtionisme*, *Predicativisme*, *Formalisme*, *Logicisme* en *Finitisme*, maar de stroming die voor dit artikel van belang is, is het *Constructivisme*. Deze opvatting van de wiskunde wordt gekenmerkt door het zich beperken tot *constructieve* bewijzen: slechts dat wat constructief bewezen kan worden is waar. In het begin van de twintigste eeuw ontstond geleidelijk het onderzoek naar de constructiviteit van begrippen en bewijzen. Wiskundigen waren zich ook voor die tijd al bewust van de mate van constructiviteit van een bewijs, maar het systematisch onderscheiden van constructieve en niet-constructieve argumenten kwam pas tot bloei in genoemde periode. Het Constructivisme is in zekere zin voortgekomen uit en heeft grote overeenkomsten met het Intuïtionisme, de opvatting van de wiskunde, of beter, van het menselijk denken, die ontwikkeld is door de nederlandse wiskundige Lutzen Egbertus Brouwer. Ik zal mij hier echter beperken tot het Constructivisme, en het Intuïtionisme buiten beschouwing laten.

Wat is een constructief bewijs? Als Hercule Poirot aantoont dat niemand anders dan monsieur X zijn hoed gestolen kan hebben, dan is dat een constructief bewijs van de bewering dat iemand zijn hoed gestolen heeft. Niet alleen wordt aangetoond dat er iemand bestaat die die eigenschap heeft, de persoon kan zelfs benoemd worden. Wat is een niet-constructief bewijs? Op een windstille avond klinkt in Combray de tuinbel. Dat is een niet-constructief bewijs van de bewering "Er is iemand die de tuinbel heeft doen klingelen." Weliswaar is bewezen dat er iemand bestaat die aan die eigenschap voldoet, maar de persoon kan niet benoemd worden. Als vervolgens Swann over het tuinpad aan komt lopen krijgt die bewering alsnog een constructief bewijs omdat diegene die de bel heeft doen klingelen nu benoemd kan worden. Of, om een meer wiskundig voorbeeld te geven: er zijn verschillende bewijzen van de Hoofdstelling van de Algebra die zegt dat elk polynoom een nulpunt heeft (in de complexe getallen). De constructieve bewijzen bevatten een algoritme om de nulpunten te creëren, de niet-constructieve bewijzen beargumenteren weliswaar dat de nulpunten bestaan, maar leveren geen methode om ze te vinden.

Wanneer in een *constructief* bewijs beweerd wordt dat er een object met zekere eigenschappen bestaat, dan bevat het bewijs, impliciet of expliciet, een methode

om dat object te construeren. Expliciet wanneer het object met name genoemd wordt: "Het is Swann die de tuinbel heeft doen klingelen". Impliciet wanneer dat niet het geval is maar het bewijs wel een algoritme bevat om het object te construeren. Een constructief bewijs van de Hoofdstelling van de Algebra somt natuurlijk niet voor elk mogelijk polynoom expliciet diens nulpunten op, maar aan de hand van het algoritme dat het bevat kan elk nulpunt berekend worden.

In een *niet-constructief* bewijs wordt er weliswaar van een zeker object aangetoond dat het bestaat, maar het bewijs bevat geen algoritme om het te construeren. Wanneer ik thuis kom, zie dat er een venster gebroken is en dat mijn diamanten ring verdwenen is, dan mag dat als voldoende bewijs beschouwd worden van de bewering: "Iemand heeft mijn ring gestolen", maar het is geen constructief bewijs zolang er geen methode is die met zekerheid naar de dader leidt. De kracht van constructieve bewijzen is dat zij wel een methode bevatten om de objecten die in het argument voorkomen te produceren.

In constructieve bewijzen wordt niet alleen constructiviteit geëist van existentiële uitspraken, maar van alle in het bewijs voorkomende redeneringen. De *Brouwer-Heyting-Kolmogorov* interpretatie verwoordt wat een constructief bewijs is door te beschrijven wat de constuctieve interpretatie van de logische operatoren is [19]:

- Een constructief bewijs van "A en B" bestaat uit een bewijs van A en een bewijs van B.
- Een constructief bewijs van "A of B" bestaat uit een bewijs van A of een bewijs van B.
- Een constructief bewijs van "A impliceert B" bestaat uit een constructie die elk bewijs van A in een bewijs van B transformeert.
- Een constructief bewijs van "Er bestaat een element met eigenschap A" bestaat uit de constructie van een object in het domein en een bewijs dat dat object aan A voldoet.
- Een constructief bewijs van "Voor alle elementen in het domein geldt A" bestaat uit een constructie die elk bewijs dat een zeker object tot het domein behoort transformeert in een bewijs van de bewering dat het object aan A voldoet.

Merk op dat, net als in het Intuïtionisme overigens, onder deze interpretatie *tertium non datur* ofwel het *principe van de uitgesloten derde*, "A geldt of de ontkenning van A geldt" niet geldt: niet voor elke bewering is er een constructie die A bewijst of een constructie die de ontkenning van A bewijst.

Interessant is dat ook Euclides al onderscheid lijkt te maken tussen constructieve en niet-constructieve argumenten: hij sluit de rechtvaardiging van een constructie niet af met Q.E.D. maar met Q.E.F., quod erat faciendum, dat wat gedaan moest worden.

Met de opkomst van de computer is de belangstelling voor en de studie van constructieve bewijzen sterk toegenomen, ook onder mensen die het Constructivisme niet aanhangen. Voor het maken van software die bijvoorbeeld wiskunde ondersteunt zijn constructieve bewijzen van belang. Wanneer van polynomen de nulpunten berekend moeten worden is een constructief bewijs van het feit dat polynomen nulpunten hebben een grote hulp, want daaruit kan een algoritme voor het berekenen van de nulpunten geëxtraheerd worden, dat vervolgens als basis kan dienen voor implementatie. Een bewijs waarin alleen maar aangetoond wordt dat de nulpunten bestaan maar niet hoe ze gevonden kunnen worden, is dan niet nuttig. Of, om een eenvoudiger voorbeeld te geven: een computer die, wanneer je vraagt wat $272 + 572$ is slechts antwoordt dat er een getal bestaat dat gelijk is aan $272 + 572$ is onnodig, maar een die "844" antwoordt biedt werkelijk uitkomst.

Zo wordt het Constructivisme zowel vanuit een praktisch als vanuit een filosofisch standpunt beoefend. Errett Bishop, die voor het Constructvisme deed wat Herman Weyl voor het Predicativisme deed, namelijk aantonen dat grote delen van de wiskunde op constructieve wijze verkregen kunnen worden, geeft in [2] als motivatie voor zijn werk:

The primary concern of mathematics is number, and this means the positive integers .... In the words of Kronecker, the positive integers were created by God. Kronecker would have expressed it even better if he had said that the positive integers were created by God for the benefit of man (and other finite beings). Mathematics belongs to man, not to God. We are not interested in properties of the positive integers that have no descriptive meaning for finite man. When a man proves a positive integer to exist, he should show how to find it. If God has mathematics of his own that needs to be done, let him do it himself.

4 De structuur van bewijzen

Bewijzen kunnen allerlei vormen hebben. De bewijzen dat Swann over het tuinpad aan komt lopen, dat de appel van Newton naar de aarde valt, dat Napoleon in 1804 zichzelf kroonde en dat elk polynoom een nulpunt heeft, hebben allen een heel andere vorm. Wat wiskundige bewijzen gemeen hebben is dat zij vaak vrij direct te analyseren en te representeren zijn op de wijze van Euclides, bijvoorbeeld als afleidingen in de predikaatlogica. Deze *formele* bewijzen, de representaties van de "echte" bewijzen, hebben, hoewel even gevariëerd als de wiskunde zelf, een gemeenschappelijk skelet: hun logische structuur. Het onderzoek naar die structuur wordt *Structurele* of *Analytische Bewijstheorie* genoemd.

Hoewel de Brouwer-Heyting-Kolmogorov interpretatie weergeeft hoe de logische operatoren constructief opgevat moeten worden, is op voorhand niet duidelijk dat dat soort bewijzen op een dergelijke wijze gerepresenteerd kunnen worden als klassieke bewijzen in de predikaatlogica: als afleidingen in een elegant systeem met simpele axioma's. Arend Heyting introduceerde in [9] de intuïtionistische

predikaatlogica. Net als voor klassieke predikaatlogica geldt hier dat het systeem niet een definitie is van wat een geldige constructieve redenering is, maar dat andersom elk bewijs dat te representeren is als een afleiding in het systeem, constructief geldig is. Dit systeem maakt het mogelijk op structurele wijze constructieve bewijzen te onderzoeken.

De problemen die in de Analytische Bewijstheorie bestudeerd worden zijn meestal niet verbonden aan één specifiek bewijs, of aan bewijzen over één specifiek onderwerp, maar algemeen van aard. De kern van het Vidi project is het onderzoek naar de structuur van constructieve bewijzen en de vergelijking, op structureel niveau, van constructieve en klassieke bewijzen. Ter afsluiting zal ik daar drie voorbeelden van geven. De twee laatste voorbeelden worden expliciet in het project genoemd, het eerste is een voorbeeld van een van de eerste grote resultaten in de Bewijstheorie.

Bewijzen bevatten vaak lemma's, die in het resultaat van het bewijs niet terug te zien zijn. De stelling is bijvoorbeeld uitlsuitend een bewering over natuurlijke getallen, maar het bewijs maakt gebruik van een lemma over oppervlakken in een drie-dimensionale ruimte. Een stelling uit de Analytische Bewijstheorie [6] laat zien dat een dergelijk bewijs altijd te ontleden is in een bewijs waarin uitsluitend natuurlijke getallen voorkomen. Zo'n bewijs is echter over het algemeen veel langer dan het originele bewijs. Dit zou men als een verklaring voor het gebruik van lemma's kunnen zien, hoewel daarvoor ook veel andere redenen zijn: de omweg via oppervlakken kan aanschouwelijker zijn, of eleganter, of eerder verkregen zijn in een andere context.

De lengte van bewijzen speelt ook een rol in het tweede voorbeeld. Gegeven een ware bewering kan men zich afvragen hoe lang het kortste bewijs van die bewering is. De lengte van een bewijs hangt natuurlijk af van de axioma's die men aanneemt. Maar zelfs op het niveau van de propositielogica (dus zonder quantoren) en voor heel simpele beweringen raakt het oplossen van dergelijke vragen aan bekende open problemen, zoals het NP *versus* P probleem uit de Complexiteitstheorie.

Een principe dat dit probleem illustreert is het Pigeonhole Principe dat stelt dat er bij $n+1$ duiven en n hokjes, tenminste een hokje meer dan één duif bevat. Een eenvoudig bewijs van deze bewering beschouwt alle mogelijkheden waarop de duiven in de hokjes geplaatst kunnen worden en concludeert dat bij elk van die mogelijkheden er in tenminste één van de hokjes meer dan een duif zit. Een keurig bewijs, maar lang: bij $n+1$ duiven bevat het alle mogelijke verdelingen van de duiven over de hokken, dus zo lang moet het bewijs minstens zijn. In 1987 bewees Sam Buss [4] dat er een veel korter bewijs bestaat. Dat bewijs maakt op essentiële wijze gebruik van tertium non datur, en is niet-constructief. Een van de thema's van mijn project is het vergelijken van de lengtes van constructieve en niet-constructieve bewijzen. Mensen redeneren vaak niet-constructief ook waar een constructief argument gebruikt kan worden. Het zou mooi zijn als daar in termen van complexiteit een reden voor gegeven zou kunnen worden, namelijk, dat die bewijzen in sommige gevallen aanzienlijk korter zijn dan hun constructieve variant.

Het derde voorbeeld heeft ook een belangrijke plaats in het project. Redeneringen waarin existentiële en universele uitspraken voorkomen, bevatten impliciet functies, zoals de Zweedse wiskundige Thoralf Skolem [16] reeds in de twintiger jaren van de vorige eeuw aantoonde. En Jacques Herbrand, een Franse wiskundige die op jonge leeftijd in de Alpen verongelukte, liet enige jaren later zien hoe de objecten waar existentiële uitspraken naar verwijzen uit het bewijs kunnen worden geëxtraheerd. Dat geldt voor constructieve zowel als niet-constructieve bewijzen. Wanneer ik zeg dat er in Genesis iemand voorkomt die in het paradijs de verboden appel eet, dan is daarin de term *Eva* niet meer zichtbaar, maar in het bewijs van die bewering wel. Het expliciteren van die functies en termen wordt wel de constructieve inhoud van een klassiek bewijs genoemd. Hoe die zich echter tot de constructieve inhoud van constructieve bewijzen verhoudt is onduidelijk.

References

[1] E. Bishop en D. Bridges, *Constructive Analysis*, Springer, 1985.

[2] E. Bishop, *Foundations of Constructive Analysis*, Academic Press, 1967.

[3] L.E.J. Brouwer, *Collected Works 1 - Philosophy and Foundations of Mathematics*, A. Heyting (ed.), North-Holland, 1975.

[4] S.R. Buss, *Polynomial size proofs of the propositional pigeonhole principle*, Journal of Symbolic Logic 52, 1987, pp.916-927.

[5] *Handbook of Proof Theory*, Studies in Logic and the Foundations of Mathematics 137, S.R. Buss (ed.), Elsevier, Amsterdam, 1998.

[6] G. Gentzen, Untersuchungen über das logische Schliessen, *Mathematisches Zeitschrift* 39(1), 1969, pp.176-210.

[7] J.-Y. Girard, *Proof Theory and Logical Complexity - Volume I*, Studies in Proof Theory, Bibliopolis, Napoli, 1987.

[8] J. Herbrand, *Recherches sur la théorie de la demonstration*, PhD thesis University of Paris, 1930.

[9] A. Heyting, *Die formalen Regeln der intuitionistischen Logik*, Sitzungsberichte der Preussischen Akademie von Wissenschaften, Physikalisch-mathematische Klasse, 1930, pp.42-56.

[10] D. Hilbert en P. Bernays, *Grundlagen der Mathematik, vol. 1*, Springer, Berlin, 1934.

[11] D. Hilbert en P. Bernays, *Grundlagen der Mathematik, vol. 2*, Springer, Berlin, 1939.

[12] U. Kohlenbach, *Applied Proof Theory: Proof Interpretations and their Use in Mathematics*, Springer Monographs in Mathematics, Springer, 2008.

[13] S. Negri en J. von Plato, *Structural Proof Theory*, Cambridge University Press, 2001.

[14] W. Pohlers, *Proof theory: the first step into impredicativity*, Springer, 2009.

[15] B. Russell, *Letter to Frege*, in J. van Heijenoort, *From Frege to Gödel: A Source Book in Mathematical Logic (1879-1931)*, Cambridge, MA: Harvard University Press, 1967, pp.124-125.

[16] T. Skolem, Logisch-kombinatorische Untersuchungen über die Erfüllbarkeit oder Beweisbarkeit mathematischer Sätze nebst einem Theorem über dichte Mengen, *Skrifter utgitt av Videnskapsselskapet i Kristiania, I, Mat. Naturv. Kl.* 4, 1920, pp.1993-2002.

[17] G. Takeuti, *Proof Theory*, Studies in Logic and the Foundations of Mathematics, North-Holland/American Elsevier, 1975.
[18] A.S. Troelstra en H. Schwichtenberg, *Basic Proof Theory*, Cambridge Tracts in Theoretical Computer Science, Cambridge University Press, 1996.
[19] A.S. Troelstra en D. van Dalen, *Constructivism in Mathematics. Volume I*, North-Holland, Amsterdam, 1988.
[20] A.S. Troelstra en D. van Dalen, *Constructivism in Mathematics. Volume II*, North-Holland, Amsterdam, 1988.
[21] H. Weyl, *Das Kontinuum; Kritische Untersuchungen über die Grundlagen der Analysis*, Veit, Leipzig, 1918.