Freek Wiedijk
Faculteit FNWI, iCIS
Radboud Universiteit Nijmegen
f.wiedijk@cs.ru.nl

Herman Geuvers
Faculteit FNWI, iCIS
Radboud Universiteit Nijmegen
h.geuvers@cs.ru.nl

Josef Urban
CIIRC
Czech Technical University, Prague
josef.urban@gmail.com

Een wiskundig bewijs correct bewezen: De meest efficiënte manier om bollen op te stapelen

Sommige bewijzen van wiskundige stellingen zijn zo bewerkelijk dat ze alleen met computerondersteuning geverifieerd kunnen worden. Een voorbeeld is het bewijs van de vierkleurenstelling, die zegt dat iedere landkaart met vier kleuren ingekleurd kan worden zonder dat aangrenzende landen dezelfde kleur krijgen. Een recent voorbeeld is het bewijs van het vermoeden van Kepler, dat zegt dat de meest voor de hand liggende stapeling van bollen in de ruimte (zoals de groenteman sinaasappelen stapelt) ook de meest efficiënte is. In dit artikel geven Freek Wiedijk, Herman Geuvers en Josef Urban een overzicht van het wiskundige deel van het bewijs en leggen uit op welke manier de computer bij de verificatie is gebruikt.

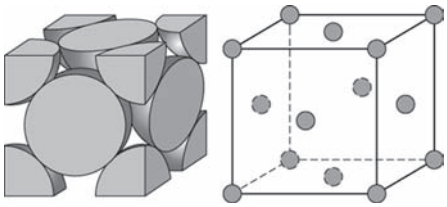
Johannes Kepler beschreef zijn vermoeden in 1611 en in 1998 kondigde de Amerikaan Tom Hales aan het bewezen te hebben. Zijn bewijs reduceert het probleem tot een kleine 20.000 mogelijke tegenvoorbeelden, die vervolgens verworpen worden. Daarvoor worden meer dan 23.000 niet-lineaire vergelijkingen opgelost en wordt aangetoond dat meer dan 43.000 lineaire programma's onoplosbaar zijn. Dat stuk van het bewijs is gedaan met computerprogramma's, en dit deel werd door de wiskundige reviewers niet geaccepteerd. Als reactie daarop is Hales het 'Flyspeck'-project begonnen, met als doel het gehele bewijs met een bewijsassistent te verifieren. Een bewijsassistent is een computerprogramma waarmee een gebruiker interactief een wiskundig bewijs construeert, dat vervolgens door het programma gecheckt wordt. Omdat bewijsassistenten een buitengewoon hoge betrouwbaarheid hebben zijn er daarna geen referenten meer nodig. In 2014 is het Flyspeck-project voltooid.

Het Kepler-vermoeden

Stel we hebben oneindig veel even grote bollen, en we willen die zo dicht mogelijk tegen elkaar in de driedimensionale ruimte plaatsen. Wat is de manier om dat met de grootst mogelijke dichtheid te doen?

Een voor de hand liggende manier is om de rangschikking te kiezen die een groenteboer voor sinaasappelen gebruikt, en die ook gebruikt wordt om kanonskogels naast een kanon op te stapelen. Dit is de zogenaamde *kubische vlakgecentreerde stapeling* (in het Engels: face centered cubic of FCC packing). In deze

Figuur 1 Efficiënt opgestapelde sneeuwballen.



Figuur 2 De FCC-stapeling.

stapeling is

$$\frac{\pi}{\sqrt{18}} = 74{,}0480\ldots\,\%$$

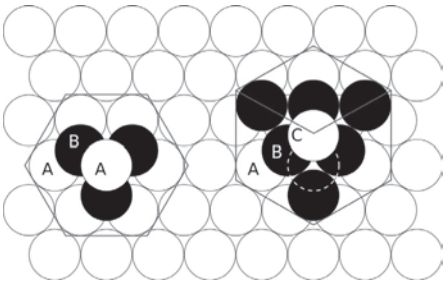
van de ruimte gevuld. Bij deze stapeling liggen de middelpunten van de bollen zowel op de hoekpunten als in het midden van de zijvlakken van de kubussen uit een driedimensionaal kubisch rooster. De roosterpuntafstand is $2r\sqrt{2}$ als r de straal van de bollen is. Zoals Figuur 2 laat zien passen er precies vier bollen in een kubus met ribbe $2r\sqrt{2}$, dus het deel van de kubus dat opgevuld wordt door de bollen is precies $\pi/\sqrt{18}$.

Een stapeling met deze dichtheid is overigens niet uniek. Ook de *hexagonale dichtste stapeling* (hexagonal close-packed of HCP packing) heeft deze dichtheid. Deze wordt bereikt door in het platte vlak een bol te omsluiten door zes andere bollen en zo verder het platte vlak vol te leggen. Zo ontstaat een hexagonaal rooster, als de cellen van een honingraat. Vervolgens wordt hier op dezelfde wijze een tweede laag bovenop gelegd. De derde laag kan nu weer op dezelfde wijze gelegd worden als de eerste, en de vierde weer op dezelfde wijze als de tweede enzovoort. Dit levert HCP, de hexagonale dichtste stapeling. Daarbij blijft het grondvlak altijd zichtbaar: we kunnen door de stapeling heen kijken. De derde laag kan ook gelegd worden over de openingen die er na de eerste twee lagen nog zijn. Als we vervolgens de bollen weer leggen volgens de posities in laag 1, en vervolgens weer in de posities van laag 2, laag 3 enzovoort, dan is er sprake van FCC, de kubische vlakgecentreerde stapeling. Als we in de FCC-stapeling een bol op het derde vlak beschouwen met de zes bollen daar direct onder in het tweede vlak, zien we één uitstekende punt van de kubus van het eerste figuur van de FCC-stapeling. Zie Figuur 3.

Er bestaan zelfs overaftelbaar veel stapelingen met de optimale dichtheid. Ze worden allemaal gevormd door oneindig veel vlakke lagen van bollen op elkaar te plaatsen. Binnen zo'n laag liggen de bollen op een hexagonaal rooster en voor iedere volgende laag zijn er dan twee manieren om die op de laag eronder te plaatsen. Als je hierbij alterneert tussen twee posities (loodrecht gezien) dan krijg je de hexagonale dichtste stapeling. Als je telkens dezelfde afstand opschuift krijg je de kubische vlakgecentreerde stapeling.

Een dichtheid van $\pi/\sqrt{18}$ kan dus op veel manieren bereikt worden. Maar kan het ook beter?

In 1611 schreef Johannes Kepler (1571–1630) in zijn boek *Strena Seu De Nive Sexangula* ('Over de zeshoekige sneeuwvlok') [9] dat dit niet het geval was:

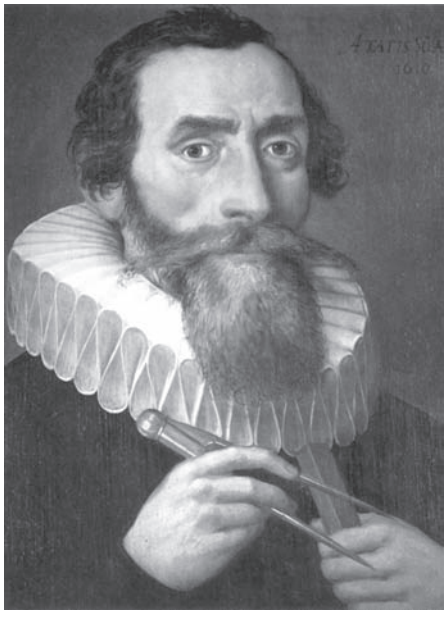


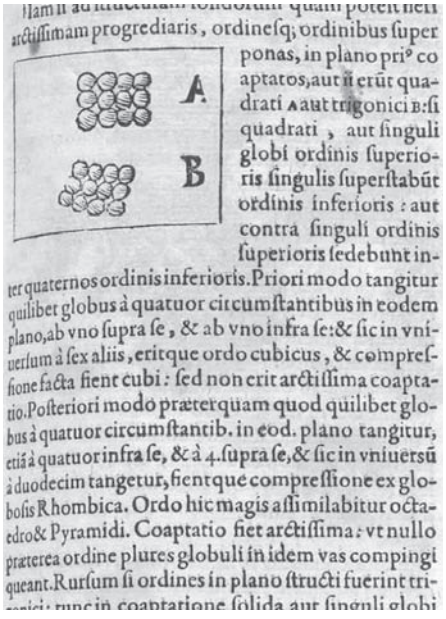
Figuur 3 Laagjes bollen in de HCP en FCC stapelingen.

> "Posteriori modo praeterquam quod quilibet globus a quatuor circumstantibus in eodem plano tangitur, etiam a quatuor infra se et a quatuor supra se, et sic in universum a duodecim tangetur, fientque compressione ex globosis rhombica. Ordo hic magis assimilabitur octaedro et pyramidi. Coaptatio fiet arctissima: ut nullo praeterea ordine plures globuli in idem vas compingi queant."

Dit kan vertaald worden als:

> "In deze rangschikking raakt elke bol niet alleen zijn vier buren in hetzelfde vlak, maar ook vier onder hem, en vier erboven, zodat alle bollen door twaalf andere worden aangeraakt, en de bollen worden samengeperst tot rombische dodecaëders. Deze rangschikking heeft meer de structuur van een octaëder en een piramide. Deze stapeling is de dichtst mogelijke: in geen enkele rangschikking kunnen meer bollen worden geplaatst in dezelfde ruimte."





Figuur 4 Links Johannes Kepler, in het midden een detail van de titelpagina van *Strena Seu De Nive Sexangula*, en rechts de claim van Kepler.

Hoewel Kepler claimt dat deze stapeling het dichtst is, geeft hij geen bewijs. De uitspraak dat de kubische vlakgecentreerde stapeling de grootst mogelijke dichtheid heeft van alle bolstapelingen is daarom bekend geworden als *het Kepler-vermoeden*.

Optimaliteit bewijzen in het geval dat de bollen gerangschikt zijn volgens een rooster was al gedaan door Carl Friedrich Gauss (1777–1855). Evenwel was het lange tijd een open probleem of de kubische vlakgecentreerde stapeling ook optimaal was zonder deze restrictie.

Een bewijs te ingewikkeld om te beoordelen

In 1953 liet László Fejes Tóth (1915–2005) zien dat het bewijzen van het Kepler-vermoeden kon worden gereduceerd tot een groot maar eindig aantal berekeningen [2].

Gebaseerd op deze ideeën gaf Tom (1958–) samen met zijn student Samuel Ferguson een bewijs voor het Kepler-vermoeden. Hij kondigde de voltooiing van dit bewijs in augustus 1998 aan.

Een bijzonderheid van dit bewijs is dat het is gebaseerd op de resultaten van een divers en groot aantal computerberekeningen. Om het bewijs te vertrouwen moet je er dus op kunnen vertrouwen dat de gebruikte software geen bugs heeft en dat de computer tijdens het rekenen nergens een storing heeft gehad. We zullen verderop de structuur van het bewijs schetsen.

Hales probeerde zijn bewijs gepubliceerd te krijgen in de *Annals of Mathematics*. Wat hij ter beoordeling instuurde was een document van 250 pagina's, vergezeld van 3 gigabytes aan computerbestanden. De *Annals* stelde vervolgens een leesgroep van twaalf referenten in met als opdracht de correctheid van het bewijs te controleren. In 2003, na vier jaar werk, gaf deze groep de opdracht terug, zonder de correctheid te hebben vastgesteld. De groep had geen fouten in het bewijs kunnen vinden. Maar aan de andere kant was het bewijs zo complex dat de groep niet in staat was geweest het te beoordelen. De groep meldde dat ze '99 procent zeker' waren van de correctheid van het bewijs, maar dat ze er niet volledig waren uitgekomen.

Er werd vervolgens besloten om het bewijs in tweeën te hakken. Het tekstuele deel werd geaccepteerd in de *Annals* in 2005 [4], terwijl het computergedeelte werd gepubliceerd in twee artikelen in *Discrete and Computational Geometry* in 2006 [7]. Het *Annals*-artikel bevatte een verwijzing naar de computerhelft van het bewijs, maar gaf daarbij de disclaimer van de editors van het tijdschrift dat het hun niet gelukt was de correctheid hiervan te beoordelen.

Tom Hales

Het Flyspeck-project

Computers zijn bezig het karakter van de wiskunde te veranderen. Als je een hulpmiddel hebt gebruik je het ook, en computers zijn voor wiskunde een buitengewoon krachtig hulpmiddel.

Er zijn allerlei manieren waarop je computers kunt gebruiken om wiskunde te doen:

- Ten eerste kun je computers gebruiken om te rekenen. Hierbij kan het gaan om getalsmatige berekeningen, maar ook om grote hoeveelheden gevallen langs te gaan. Dit is het soort computergebruik dat de basis is voor het bewijs van Hales en Ferguson.

  Computers rekenen gewoonlijk met eindige precisie (met *floating point numbers* of drijvendekommagetallen), en maken dus afrondfouten, maar dit hoeft geen reden te zijn dat berekeningen niet wiskundig hard bruikbaar zijn. Zo kun je kiezen naar welke kant je getallen laat afronden, en in plaats van alleen met benaderingen kun je met intervallen rekenen. Bij *interval-aritmetiek* zorg je ervoor dat het reële getal waarover je een uitspraak doet gegarandeerd binnen de intervalbenadering ligt. Interval-aritmetiek is een essentieel onderdeel van het Hales–Ferguson-bewijs.
- Wiskundige berekeningen hoeven niet numeriek te zijn, maar kunnen ook *symbolisch* zijn. Als ik het getal $\sqrt{2}$ beschouw, dan kan ik maar eindig veel cijfers achter de komma opschrijven. Evenwel, door dit getal symbolisch te beschouwen heb ik toch maar eindig veel inkt nodig om het in volledige precisie te kunnen manipuleren.

  Een dergelijk onderscheid bestaat ook in de computer. De *computer algebra* systemen als Mathematica en Maple werken niet met getallen maar met symbolische expressies. Ook deze systemen worden vaak gebruikt als handig hulpmiddel in wiskundig onderzoek.
- Bij de vorige twee manieren om computers te gebruiken gaat het over rekenen, en het *redeneren* over wat de berekeningen voorstellen wordt aan de mens overgelaten. Er zijn ook computersystemen die helpen bij het redeneren [3]. Hierbij kun je onderscheid maken tussen het vinden van redeneringen versus het verifiëren van redeneringen. In het eerste geval gaat het om ATP-systemen (automated theorem provers), en in het tweede geval om ITP-systemen (interactive theorem provers). Een andere term voor een ITP-systeem is een *bewijsassistent*. Hoewel bij ITP het bewijs door de mens wordt aangedragen bieden deze programma's toch een heleboel hulp bij het redeneren.

De eerste twee vormen van computergebruik hebben binnen de wiskunde een hoge vlucht genomen. De laatste is momenteel voornamelijk nog een onderzoeksonderwerp voor informatici, maar was precies wat Hales nodig had.

In januari 2003 besloot Hales zijn bewijs met een ITP-systeem te gaan controleren. Omdat deze systemen een buitengewoon hoge betrouwbaarheid hebben, zouden er daarna geen referenten meer nodig zijn. Hij had met ITP-specialisten gecorrespondeerd (waaronder met ons), en de schatting was dat het ongeveer twintig manjaar zou kosten om het bewijs van het Kepler-vermoeden in een ITP-systeem in te voeren en te verifiëren. Hales besloot dat dit een doenlijk project was. Als naam voor het project [6] koos hij *Flyspeck*, door met het patroon `f*p*k` (voor 'formal proof of Kepler') in een lijst woorden te zoeken. In het Engels

John Harrison, ontwikkelaar HOL Light-bewijsassistent

betekent "to flyspeck" ook zoiets als "in extreem detail op gebreken controleren", dus deze naam was zeer toepasselijk. Als systeem voor het project koos hij het HOL Light-systeem [8] van John Harrison. Harrison is op *interactive theorem proving* (ITP) gepromoveerd in Cambridge, en is als ITP-specialist werkzaam bij Intel in Portland in de Verenigde Staten. Hoewel hij in zijn baan correctheidsbewijzen voor Intel verifieert, die dus over informatica gaan, heeft hij in zijn vrije tijd een indrukwekkende hoeveelheid wiskundige bewijzen in zijn systeem geformaliseerd.

Het HOL Light-systeem is vooral voor wiskunde een van de sterkere systemen, maar wordt in de informatica minder gebruikt. Andere, in de informatica bekendere ITP-systemen zijn het Coq-systeem [1] uit Frankrijk en het Isabelle-systeem [11] uit Engeland/Duitsland. De gebruikers van deze systemen bleken ook zeer in Flyspeck geïnteresseerd ("eindelijk een echte wiskundige die onze systemen nodig heeft!") en hebben ook aan Flyspeck gewerkt. Een deel van het werk met Isabelle is ook in het uiteindelijke Flyspeck-bewijs terechtgekomen (zie verderop), maar het overgrote deel van het Flyspeck-bewijs is geformaliseerd in het HOL Light-systeem.

Hales besloot Flyspeck een extra impuls te geven door het coderen van het bewijzen te 'outsourcen, namelijk in Vietnam. Hij organiseerde daar een groep Vietnamese wiskundigen, leerde ze HOL Light, en zette ze aan het coderen van het bewijs van het Kepler-vermoeden. Tegelijk werkte hij aan een boek dat het bewijs minutieus gedetailleerd weergeeft, het zogeheten 'blueprint'-boek, want de subtitel is 'A blueprint for formal proofs'. Dit boek [5] telde uiteindelijk 334 bladzijden.

Op 10 augustus 2014 werd bekend gemaakt dat het Flyspeck-project was voltooid. Het bewijs was in de tussentijd aangepast en gestroomlijnd (ook om verificatie met de computer te vergemakkelijken), en dit aangepaste bewijs is dus 100 procent zeker correct. Het Kepler-vermoeden kan sinds deze datum als bewezen worden beschouwd.

Zekerheid dat een bewijs correct is

Een wiskundige gaat achter een computer met HOL Light zitten, en claimt: dankzij dit systeem weet ik 100 procent zeker dat deze stelling bewijsbaar is. Hoe kan hij zo zeker van zijn zaak zijn? Het oorspronkelijke Kepler-bewijs van Hales en Ferguson bevatte een groot aantal computerberekeningen, en het was daardoor moeilijk vast te stellen of het allemaal correct was. Het Flyspeck-bewijs heeft net zo goed een groot aantal computerberekeningen (door HOL Light) nodig om te verwerken. Waarom zou dit anders zijn?

Een ITP-systeem als HOL Light implementeert een redeneersysteem uit de mathematische logica dat extreem eenvoudig is. Alle complexiteit van de redenering in het zeer ingewikkelde Kepler-bewijs wordt teruggebracht tot een gigantisch aantal (miljarden) zeer elementaire redeneerstapjes. Stuk voor stuk zijn deze stapjes uiterst simpel. Het gebruikte redeneersysteem heet HOL (voor 'higher order logic', hogere-orde logica), en bestaat uit maar tien zeer eenvoudige redeneerregels. Ieder stapje past één van die regels toe.

Nu komt de controle van de correctheid van het bewijs uitsluitend neer op het controleren van deze redeneerstapjes. Maar omdat het redeneersysteem zo eenvoudig is, is het maar een heel klein deel van de gebruikte software dat dit doet. Deze *logische kern* is ongeveer vierhonderd programmaregels lang (geschreven in de functionele programmeertaal OCaml). Door het gebruik van de techniek van *abstracte datatypen* kan er geen wiskundige incorrectheid optreden als deze kern van het programma foutloos is. En bij een programma van vierhonderd regels is het goed te doen om alle fouten eruit te halen.

In andere woorden: in plaats van het belachelijk ingewikkelde Kepler-bewijs op correctheid te moeten beoordelen, hoeven de referenten nu alleen vierhonderd regels OCaml-code op correctheid te controleren, en de computer doet dan de rest.

Nu zijn er ook wel programmeerfouten in kernen van ITP-systemen gevonden, dus we zouden nog een stap verder willen gaan. In de informatica bestaat er technologie — ook gebaseerd op ITP — om van programma's (in het bijzonder als het geschreven is in een functionele programmeertaal) vast te stellen dat er *nul* fouten in zitten. Deze technologie hebben eerst John Harrison en vervolgens Ramana Kumar (een andere promovendus uit Cambridge) gebruikt om formeel te bewijzen dat de kern van HOL Light foutloos is [10]. Zelfs hier hoeven de referenten zich dus geen zorgen meer over te maken.

Er is hier natuurlijk wel sprake van een kip-en-ei-probleem, en tevens volgt uit de Gödelstelling (die zegt dat een consistent logisch systeem niet van zichzelf kan bewijzen dat het consistent is) dat een systeem niet de correctheid van zijn eigen broncode kan vaststellen. Maar al met al betekent al deze technologie dat de betrouwbaarheid van ITP-systemen, en daardoor van de gecontroleerde bewijzen, extreem hoog is. Onvoorstelbaar veel hoger dan die van bewijzen die alleen door mensen geverifieerd zijn.

Als de implementatie van het ITP-systeem volledig vertrouwd wordt kan er uiteraard in een ander onderdeel van de computer een softwarefout of hardwarefout zitten, waardoor een incorrect bewijs geaccepteerd wordt door de computer. Het is uiterst onwaarschijnlijk dat, bijvoorbeeld, een fout in het besturingssysteem ervoor zou zorgen dat een incorrect bewijs juist wel door de ITP-kern geaccepteerd zou worden. Dit punt wordt ondervangen door de bewijsverificatie op verschillende computers met verschillende software opnieuw te draaien.

Het Hales–Ferguson-bewijs

Het bewijs van het Kepler-vermoeden bestaat uit ruwweg acht stappen, waarbij we hier het bewijs vertellen van het resultaat terugwerkend naar eerdere lemma's. De spil van het bewijs is stap (d), de "lokale annulus-ongelijkheid".

(a) De precieze formulering van het Kepler-vermoeden. Het Kepler-vermoeden gaat over oneindigheid: wat er mogelijk is als

we een oneindige ruimte vullen met oneindig veel bollen met vaste straal r_0. Dit betekent dat we het over een limietproces hebben, want de dichtheid van de bollen is de limiet van de dichtheid van deze bollen binnen een groeiende bol met straal r, waarbij r naar oneindig gaat. Nu hoeft deze limiet niet te bestaan, maar de $\limsup$ bestaat natuurlijk altijd wel. Wat we dus moeten bewijzen is dat dit voor iedere mogelijke configuratie van de bollen nooit groter zal zijn dan $\pi/\sqrt{18}$.

Het is duidelijk dat de $\limsup$ niet afhangt van de keuze van r_0, dus vanaf nu zullen we $r_0 = 1$ nemen. We kijken dus naar een stapeling van eenheidsbollen.

(b) De uitspraak die bewezen wordt in het Flyspeck-project. Flyspeck kijkt niet naar het volume van de doorsnede van de bollen met de grote bol met straal r, maar telt de middelpunten van de kleine bollen die zich binnen de grote bol bevinden. Omdat het volume van de grote bol evenredig is met r^3 en wat we zo verwaarlozen correspondeert met een volume ten hoogste evenredig met r^2, maakt dit voor de $\limsup$ van de dichtheid niet uit.

Voorts heeft Flyspeck het niet over de $\limsup$, maar bewijst het de volgende uitspraak:

Voor iedere stapeling S bestaat een c zodat voor iedere $r \geq 1$ geldt dat:

$$\operatorname{card}(V_S \cap B(0,r)) \leq \frac{\pi}{\sqrt{18}} r^3 + cr^2.$$

Hierin is V_S de verzameling met de middelpunten van de kleine bollen behorend bij stapeling S, en $B(0,r)$ is een groeiende (open) bol met straal r. De eis $r \geq 1$ is duidelijk nodig voor het geval dat de oorsprong in V_S zit. De constante c hangt in deze formulering af van de stapeling, maar Hales claimt dat deze ongelijkheid ook voor een vaste c kan worden bewezen. Deze verfijning zit evenwel niet in Flyspeck.

In de computercode die de input voor het HOL Light-systeem is, is deze uitspraak gecodeerd als:

```
!V. packing V ==>
  (?c. !r. &1 <= r ==>
    &(CARD(V INTER ball(vec 0,r))) <=
    pi * r pow 3 / sqrt(&18) + c * r pow 2))
```

Hierin is '**!**' de universele kwantor $\forall$, '**?**' de existentiële kwantor $\exists$, en '**&**' de functie die een natuurlijk getal afbeeldt op het corresponderende reële getal.

(c) Verwaarloosbare FCC-compatibele functies. We hebben het ook in deze herformulering nog steeds over een oneindig probleem, en we willen dit graag reduceren naar een eindig probleem, en zo een aanpak mogelijk maken die analyseert wat er rond een enkele bol kan gebeuren.

Hiertoe nemen we een stapeling S en we verdelen de ruimte in de *Voronoi-cellen* van de verzameling van bolmiddelpunten van S, V_S. Voor ieder punt $v \in V_S$ is de Voronoi-cel $\Omega(V_S, v)$ de verzameling punten die dichter bij v ligt dan bij ieder ander punt in V_S.

Een reëelwaardige functie $G(v)$ op de punten van V_S heet *verwaarloosbaar* als er een c_1 bestaat zodat voor alle $r \geq 1$:

$$\sum_{v \in V_S(0,r)} G(v) \leq c_1 r^2.$$

De functie $G(v)$ heet *FCC-compatibel* als voor iedere $v \in V_S$,

$$4\sqrt{2} - \operatorname{vol}(\Omega(V_S, v)) \leq G(v).$$

Het getal

$$4\sqrt{2} = 5{,}55685\ldots$$

is het volume van de Voronoi-cellen van FCC, de kubische vlakgecentreerde stapeling.

Als de stapeling S echt beter is dan FCC, dan zijn de Voronoi-cellen van S kleiner dan die van FCC. De definitie van een verwaarloosbare FCC-compatibele functie $G(v)$ betekent dat de Voronoi-cellen van S niet significant kleiner zijn dan die van FCC: het verschil is maximaal van orde r^2, terwijl het aantal punten in $V_S(0,r)$ van orde r^3 is. Dus in de limiet is de afwijking verwaarloosbaar. Hieruit volgt duidelijk het Kepler-vermoeden.

Het bestaan van zo'n verwaarloosbare FCC-compatibele functie $G(v)$ is stap (f) van deze bewijsschets.

(d) De lokale annulus-ongelijkheid. Dit is het centrale lemma van het bewijs, dat ook voor andere stellingen toepasbaar is gebleken.

Definieer het magische getal h_0 exact als

$$h_0 = 1{,}26$$

Bekijk nu de 'schil' van punten v om een eenheidsbol met middelpunt in de oorsprong met de eigenschap

$$1 \leq h(v) \leq h_0$$

waarbij $h(v)$ de helft van de afstand van punt v tot de oorsprong is. Deze 'schil' heet de *annulus* van de centrale bol. We gaan kijken wat er gebeurt als we bollen om deze centrale bol plaatsen, zodanig dat de middelpunten zich allemaal in deze annulus bevinden.

Voorts tellen we deze bollen gewogen: als ze verder naar buiten zijn tellen ze minder mee. (In dat geval is er meer ruimte tussen de bollen, en we willen een ongelijkheid die het aantal begrenst.) Precies gezegd definiëren we een functie $L(h)$ door

$$L(h) := \begin{cases} \frac{h_0 - h}{h_0 - 1} & \text{if } 1 \leq h \leq h_0, \\ 0 & \text{if } h_0 \leq h. \end{cases}$$

Deze functie vervalt lineair van 1 op het binnenoppervlak van de annulus naar 0 op het buitenoppervlak.

De lokale annulus-ongelijkheid is nu:

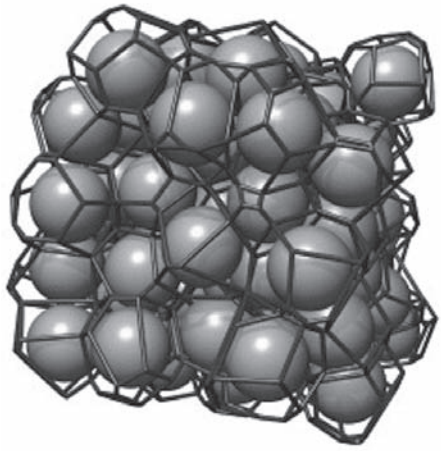
$$\sum_{v \in V_S} L(h(v)) \leq 12.$$

Het centrale lemma zegt dat deze ongelijkheid geldt voor iedere stapeling S.

De geldigheid van deze ongelijkheid zal volgen uit het resultaat in stap (g), en is een van de ingrediënten voor het bestaan van een verwaarloosbare FCC-compatibele functie in stap (f).

Dat er maximaal twaalf bollen aan een centrale bol kunnen raken was Kepler al duidelijk. Door de bollen verder naar buiten te bewegen passen er mogelijk meer, maar als je ze minder meetelt, blijft het 'aantal' dus toch hoogstens twaalf.

(e) Marchal-cellen en de cel-cluster ongelijkheid. Nu wordt het bewijs nog technischer, en we worden hier nog schetsmati-



Afbeelding: G.E. Schröder-Turk e.a., Europhysics Letters 90(3) (2010)

Figuur 5 Voronoi-cellen van een bolstapeling.

ger in onze beschrijving van het bewijs dan we toch al waren.

De Voronoi-cellen worden verdeeld in *Rogers-simplices* en deze worden weer onderverdeeld in fragmentjes die *Marchal-cellen* worden genoemd. Dit alles wordt gedaan om te komen tot de zogenaamde *cel-cluster-ongelijkheid*. Die heeft te maken met configuraties waarin twee bollen een afstand in een specifiek interval hebben (zo'n configuratie wordt een 'cel-cluster' genoemd). De cel-cluster-ongelijkheid blijkt de cruciale stap om te laten zien dat de functie $G(v)$, die we in de volgende sectie definiëren, verwaarloosbaar is.

(f) Met wat we nu hebben kunnen we, gegeven een stapeling S, een verwaarloosbare FCC-comptibele functie definiëren:

$$G(v) = -\operatorname{vol}(\Omega(V_S, v)) + 8m_1 - \sum 8m_2 L(h(v)).$$

Hierin:

$$\begin{aligned}
&\mathrm{sol}_0 = 3\arccos(1/3) - \pi = 0{,}551285\ldots,\\
&\tau_0 = 4\pi - 20\mathrm{sol}_0 = 1{,}54065\ldots,\\
&m_1 = \mathrm{sol}_0 2\sqrt{2}\,/\tau_0 = 1{,}01208\ldots,\\
&m_2 = (6\mathrm{sol}_0 - \pi)\sqrt{2}\,/\,(6\tau_0) = 0{,}0254145\ldots.
\end{aligned}$$

De som in de definitie van $G(v)$ loopt over alle bolmiddelpunten in V_S uitgezonderd de oorsprong. Als v te ver van de oorsprong ligt geldt $L(h(v)) = 0$, dus dit is een eindige som.

Uit de lokale annulus-ongelijkheid volgt nu dat deze functie FCC-compatibel is:

$$\begin{aligned}
&4\sqrt{2} - \operatorname{vol}(\Omega(V_S, v))\\
&\quad \leq -\operatorname{vol}(\Omega(V_S, v)) + 8m_1 - 12 \cdot 8m_2\\
&\quad \leq -\operatorname{vol}(\Omega(V_S, v)) + 8m_1 - \sum 8m_2 L(h(v))\\
&\quad = G(v).
\end{aligned}$$

Dat deze functie ook verwaarloosbaar is volgt dus uit de cel-cluster-ongelijkheid.

(g) Het niet-bestaan van een tegenvoorbeeldstapeling. We hebben nog niet beschreven hoe de lokale annulus-ongelijkheid en de cel-cluster-ongelijkheid bewezen worden. We gaan nu eerst kijken hoe het bewijs van de eerste gaat. Over het bewijs van de tweede hebben we het in de volgende paragraaf.

Een verzameling bollen S rond een centrale bol waarvoor de lokale annulus-ongelijkheid niet geldt noemen we een *tegenvoorbeeldstapeling*. In feite eisen we voor een tegenvoorbeeldstapeling nog wat meer, zoals dat het aantal bollen ten hoogste veertien is, en dat de waarde van $\sum_{v \in V_S} L(h(v))$ maximaal is.

We willen laten zien dat er geen tegenvoorbeeldstapeling bestaat, want dan geldt de lokale annulus-ongelijkheid voor alle stapelingen.

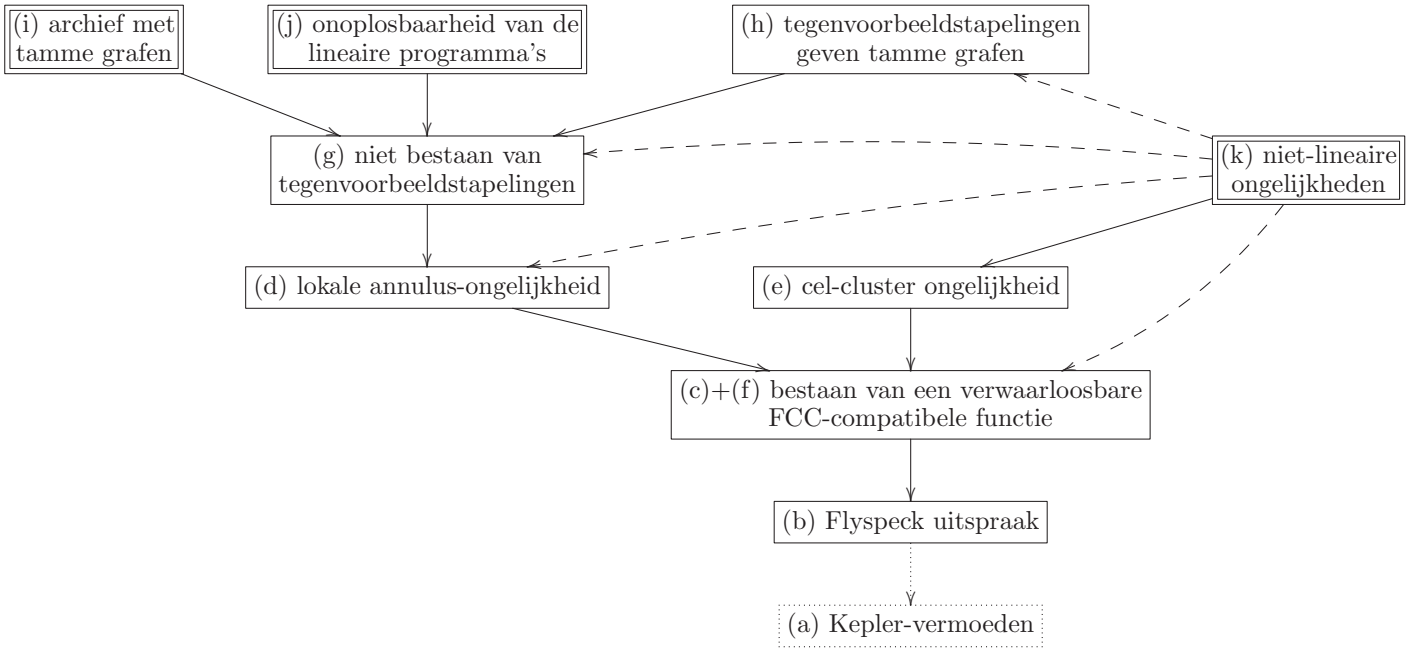
(h) Tamme grafen zijn de grafen van tegenvoorbeeldstapelingen. We definiëren nu bij een tegenvoorbeeldstapeling een graaf door twee middelpunten van bollen te verbinden als de afstand kleiner is dan $2h_0$. Deze grafen voldoen aan een reeks eigenschappen, en alle grafen die aan die eigenschappen voldoen noemen we *tamme* grafen. Deze worden gedefinieerd met een lijst van elf eigenschappen, waarvan de ingewikkeldste is dat er een functie van de vlakken in de graaf naar de reële getallen moet bestaan die aan drie verdere eigenschappen moet voldoen.

Het bewijs wordt nu afgemaakt door eerst te bewijzen dat de graaf van een tegenvoorbeeldstapeling altijd tam is. Dan wordt bewezen dat iedere tamme graaf in een lange lijst van 19.715 grafen voorkomt. En ten slotte wordt voor iedere graaf uit die lijst gekeken of het mogelijk is om de bollen zo te plaatsen dat de lokale annulus-ongelijkheid niet geldt. Dit correspondeert met het zoeken van een oplossing in een hele reeks lineaire programma's. Doordat dat voor geen enkele tamme graaf lukt, volgt hieruit de lokale annulus-ongelijkheid.

De computer helpt

Zoals gezegd rust het Hales–Ferguson-bewijs op een aantal computerberekeningen:

(i) Een programma dat de lijst van 19.715 grafen genereert waar alle tamme grafen



Figuur 6 Het bewijs van het Kepler-vermoeden.

bij zitten. Dit programma was oorspronkelijk in Java geschreven. De versie van dit programma in Flyspeck is geschreven in de taal van de bewijsassistent Isabelle en vervolgens geëxporteerd naar een programma in de programmeertaal ML. De verificatie van dit programma is het enige onderdeel van Flyspeck dat niet in HOL Light is gedaan maar in Isabelle. In de HOL Light-verificatie is het resultaat hiervan, inclusief de lijst grafen, als axioma aangenomen.

(j) Een computerberekening die verifieert dat 43.078 lineaire programma's onoplosbaar zijn. Ieder lineair programma in deze lijst heeft rond de duizend variabelen en een vergelijkbaar aantal vergelijkingen. Deze lineaire programma's waren de hoofdmoot van de 3 gigabyte data uit het oorspronkelijke bewijs. In het HOL Light-bewijs worden ze *on the fly* gegenereerd en de onoplosbaarheid ervan wordt vervolgens bewezen.

(k) Een computerverificatie dat 23.242 niet-lineaire ongelijkheden met hoogstens zes variabelen gelden. Dit is de verificatie waarbij in het oorspronkelijke bewijs interval-aritmetiek wordt gebruikt. Deze ongelijkheden worden op allerlei plaatsen in het bewijs gebruikt. Om een idee te geven: het gaat hierbij om te verifiëren dat ongelijkheden van de volgende vorm gelden binnen een bepaald interval:

$$\frac{\begin{array}{c}-x_1x_3-x_2x_4+x_1x_5+x_3x_6-x_5x_6\\ +x_2(-x_2+x_1+x_3-x_4+x_5+x_6)\end{array}}{\sqrt{4x_2\begin{pmatrix}x_2x_4(-x_2+x_1+x_3-x_4+x_5+x_6)+\\ x_1x_5(x_2-x_1+x_3+x_4-x_5+x_6)+\\ x_3x_6(x_2+x_1-x_3+x_4+x_5-x_6)\\ -x_1x_3x_4-x_2x_3x_5-x_2x_1x_6-x_4x_5x_6\end{pmatrix}}} < \tan\left(\frac{\pi}{2}-0.74\right).$$

Hoe dit allemaal aan elkaar hangt is in het diagram in Figuur 6 weergegeven. De rechthoeken met dubbele randen zijn de rekenintensieve taken waarvoor speciale programma's zijn geschreven. De pijlen geven de afhankelijkheden tussen de verschillende onderdelen.

Het moeilijkste in de HOL Light-verificatie was het doenlijk krijgen van de verificatie van de computerberekeningen, omdat deze ook allemaal in hele kleine redeneerstapjes moesten worden afgebroken en door de HOL Light-kern geverifieerd. Om dit efficiënt genoeg te doen was een heleboel slimheid nodig. Dit was het onderwerp van het proefschrift van Alexey Solovyev [12], een promovendus van Hales.

Alexey Solovyev

En zelfs hierna kon het project pas worden afgerond toen Microsoft genereus rekentijd in de cloud beschikbaar stelde. Evenwel werd vrij kort daarna de hele verificatie nog eens overgedaan op een van de clusters van de Radboud Universiteit in Nijmegen.

Referenties

1 Coq development Team, The Coq proof assistant, https://coq.inria.fr.

2 L. Fejes Tóth, *Lagerungen in der Ebene auf der Kugel und im Raum*, first edition, Springer, 1953.

3 Georges Gonthier, Thomas C. Hales, John Harrison en Freek Wiedijk, Formal proof, *Notices of the American Mathematical Society* 55(11) (2008), 1370–1414.

4 Thomas C. Hales, A proof of the Kepler conjecture, *Annals of Mathematics* 162 (2005), 1063–1183.

5 Thomas C. Hales, *Dense Sphere Packings: A blueprint for formal proofs*, London Math. Soc. Lecture Note Series, Vol. 400, Cambridge University Press, 2012.

6 Thomas C. Hales, Mark Adams, Gertrud Bauer, Dat Tat Dang, John Harrison, Truong Le Hoang, Cezary Kaliszyk, Victor Magron, Sean McLaughlin, Thang Tat Nguyen, Truong Quang Nguyen, Tobias Nipkow, Steven Obua, Joseph Pleso, Jason Rute, Alexey Solovyev, An Hoai Thi Ta, Trung Nam Tran, Diep Thi Trieu, Josef Urban, Ky Khac Vu en Roland Zumkeller, A formal proof of the Kepler conjecture, *CoRR*, abs/1501.02155, 2015.

7 Thomas C. Hales en Samuel P. Ferguson, Historical overview of the Kepler conjecture; A formulation of the Kepler conjecture; Sphere packing III, Extremal cases; Sphere packing IV, Setailed bounds; Sphere packings VI, Tame graphs and linear programs, *Discrete & Computational Geometry* 36(1) (2006), 5–20; 21–69; 71–110; 111–166; 205–265.

8 J. Harrison, The HOL Light theorem prover, http://www.cl.cam.ac.uk/~jrh13/hol-light.

9 J. Kepler, *The Six-Cornered Snowflake*, Clarendon Press, 1966.

10 Ramana Kumar, Rob Arthan, Magnus O. Myreen en Scott Owens, Self-formalisation of higher-order logic, *Journal of Automated Reasoning* 56(3) (2016), 221–259.

11 L. Paulson, T. Nipkow en M. Wenzel, The Isabelle proof assistant, https://isabelle.in.tum.de.

12 A. Solovyev, *Formal Computations and Methods*, PhD thesis, University of Pittsburgh, 2013.