Geschiedenis van de Logica
Samenvatting Hoofdstuk 8

Jesse Mulder en Niels van Miltenburg

14 juni 2007

8.1 Onvolledigheid en Complexiteit

Er wordt vaak beweerd dat de onvolledigheidsstelling van toepassing is op formele systemen die voldoende "complexiteit" hebben. Wij hebben echter gezien dat er bijzonder complexe systemen zijn waar de onvolledigheidsstelling niet op toepasbaar is en bijzonder eenvoudige systemen waarop hij wel toepasbaar is. Dus dit informele gebruik van "complexiteit" en de suggestie dat dit soort "complexiteit" iets van doen heeft met de onvolledigheidsstelling is misleidend. Complexiteit in de technische zin binnen de logica heeft wel een verband met onvolledigheid. Deze zogeheten Kolmogorov complexiteit kan namelijk worden gebruikt om de eerste onvolledigheidsstelling te bewijzen.

Chaitin's onvolledigheidsstelling

We zullen gebruik maken van de theorie van de berekenbare eigenschappen van rijtjes die we in Hoofdstuk 3 gezien hebben. De Kolmogorov complexiteit van een (binair) rijtje s, notatie $K(s)$, is niet de lengte van s zelf, maar de lengte van de kortst mogelijke combinatie van een rijtje i met een bepaald programma P, waarbij P, indien i als input gegeven wordt, s als output levert. P is dus een programma zoals we dat kennen uit Hoofdstuk 3. Een rijtje is *uiterst comprimeerbaar* als zijn Kolmogorov complexiteit klein is in vergelijking met zijn eigen lengte en *uiterst incomprimeerbaar* als zijn Kolmogorov complexiteit bijna even groot is als zijn eigen lengte. Voor elke n zeg, groter dan 1000 zijn de meeste rijtjes met lengte n uiterst incomprimeerbaar. In het bijzonder is er voor elke n ten minste één rijtje s met lengte n [1] die maximaal incomprimeerbaar is, dat wil zeggen $K(s) = n$. Incomprimeerbare rijtjes zijn erg *willekeurig*, in de zin dat er geen patroon in te ontdekken valt dat ervoor zou kunnen zorgen dat je een algoritme kan geven dat een stuk korter is dan het rijtje zelf.

Terug naar onvolledigheid: Laat T een consistent formeel systeem zijn dat de "bepaalde hoeveelheid rekenkunde" bevat. Chaitin's onvolledigheidsstelling

[1] Dit is in te zien omdat er $1 + 2 + 4, ...2^{n-1} = 2^n - 1$ mogelijke programma's kleiner dan n zijn, terwijl er 2^n rijtjes zijn van lengte n.

stelt nu dat er een constante c is, afhankelijk van T, zodanig dat T geen uitspraken bewijst van de vorm $K(s) > c$. Aangezien er wel degelijk zulke ware uitspraken bestaan, volgt dat, tenzij T onware uitspraken over complexiteit bewijst, er uitspraken zijn van de vorm $K(s) > c$ die onbeslisbaar zijn in T. Laten we deze stelling eerst bekijken via een informele schets en vervolgens via een wat formeler bewijs.

Een bewijsschets

Stel dat er arbitrair grote n zijn zodat de consistente theorie T bewijst dat $K(s) > n$ voor bepaalde s. Stel verder dat het rijtje t voldoende informatie bevat om alle stellingen van T te genereren (die zijn immers berekenbaar opsombaar). We kiezen n zodanig dat n min het aantal symbolen in de notatie van n een aantal malen groter is dan de lengte van t. Om nu een rijtje met een complexiteit hoger dan n te vinden doorlopen wij de stellingen van t totdat we een stelling vinden van de vorm $K(s) > n$. Dit betekent echter dat we s kunnen produceren met behulp van alleen t samen met de notatie van n, maar de complexiteit van deze gecombineerde informatie is veel kleiner dan n. Dat leidt uiteraard tot een tegenspraak met de bewezen uitspraak $K(s) > n$.

Een formelere route

In paragraaf 3.3 zagen we de berekenbaar optelbare verzameling van programma's die een rijtje als input hebben en als output ook een rijtje hebben, of anders niet eindigen.

$$P_0, P_1, P_2, ...$$

Als we nu Kolmogorov complexiteit willen definieren kunnen we dat doen in termen van programma's en rijtjes: $K(s)$ is de lengte van het kortste paar (i, w) zodat P_i met input w, s als output levert. Merk op dat onze definitie afhankelijk is van welke opsomming je kiest voor jouw rijtje programma's. Het kan echter worden aangetoond dat voor elke twee opsommingen van programma's de resulterende complexiteitsmaatstaven K_1 en K_2 in essentie equivalent zijn. Dat wil zeggen dat er een constante c is, onafhankelijk van s, maar afhankelijk van K_1 en K_2, zodat $|K_1(s) - K_2(s)| < c$ voor alle s. Dit betekent dat de *kwantitatieve* resultaten afhankelijk zijn van de definitie van K, c is immers afhankelijk van de gekozen definitie van $K(s)$. Anderzijds betekent dit wel dat de *kwalitatieve* resultaten (zoals Chaitin's onvolledigheidsstelling) onafhankelijk zijn van de manier waarop je complexiteit definieert.

We hebben het gehad over "de lengte van een paar (i, w)", wat hiermee bedoelt wordt is dat we van twee rijtjes één rijtje maken zodanig dat beide rijtjes uit het nieuw verkregen rijtje kunnen worden afgelezen (zie voor een duidelijk voorbeeld pagina 140).
Verder is het belangrijk om op te merken dat een uitspraak van de vorm $K(s) > n$ een Goldbachachte uitpraak is, zoals blijkt uit de herformulering:

Voor elke m en voor elk paar (i, w) met een lengte kleiner dan n, is het niet het geval dat m stappen in de uitvoering van P_i met input w, tot s als output leiden.

Dit heeft als gevolg dat op het moment dat een consistente theorie $K(s) > n$ bewijst, de complexiteit van s inderdaad groter is dan n, we mogen immers Π_1-reflectie toepassen.
Tot slot hebben we nog een berekenbare opsomming nodig van de berekenbaar opsombare verzamelingen: $W_0, W_1, W_2, ...$ W_i is de verzameling rijtjes s, waarvoor P_i met input s eindigt. W_i is berekenbaar opsombaar, omdat de verzameling ware uitspraken van de vorm "P_i met input s eindigt na n stappen" beslisbaar is. We kunnen dus alle ware uitspraken van deze vorm genereren en s als output geven voor elke gevonden ware uitspraak om zo een berekenbare opsomming van W_i te krijgen.
Dan nu het bewijs:

Bewijs: Kies W_p zodanig, dat gegeven een theorie T, W_p de verzameling stellingen van T is.
Stel een programma P_e, dat bij een input van een paar van numerieke rijtjes (p, k), op zoek gaat naar een zin in W_p van de vorm "de complexiteit van w is groter dan de lengte van het paar $(k, (p, k))$." Als zo'n zin gevonden wordt dan geeft P_e als output rijtje w.

Stel dat P_e eindigt voor input (p, e) met resultaat w.
Vanwege onze definitie van complexiteit is $K(w)$ nu hooguit de lengte van $(e, (p, e))$ (hooguit, omdat er misschien nog kortere paren te vinden zijn de w als output leveren). Dit betekent echter dat P_e een uitspraak heeft gevonden in W_p, dat wil in dit geval zeggen in de stellingen T die zegt: "de complexiteit van w is groter dan de lengte van het paar $(e, (p, e))$." Aangezien deze uitspraak Goldbachachtig is betekent dat, dat als T consistent is er een tegenspraak ontstaat en dan is T dus niet consistent. Dit betekent dat als T consistent is, T geen uitspraken van de vorm "$K(w) > c$" waarbij c de lengte van een paar $(e, (p, e))$ is.

Een paar gevolgentrekkingen uit Chaitin's onvolledigheidsstelling

Het complement van de verzameling van maximaal incomprimeerbare rijtjes (de verzameling rijtjes s met $K(s) < |s|$), is een simpele verzameling; d.w.z. een verzameling die (1) berekenbaar optelbaar is en (2) waarvan het complement, hoewel oneindig, geen oneindige berekenbare deelverzameling heeft. Dit omdat een consistente theorie alleen een eindig aantal uitspraken van de vorm "s is een maximaal incomprimeerbare rijtje" bewijzen. Merk op dat er in het bewijs dat er onbewijsbare ware uitspraken van de vorm "s is een maximaal incomprimeerbare rijtje"zijn in een consistente theorie, geen expliciet voorbeeld van zo'n uitspraak wordt gegeven. Stel dat we een mechanisme zouden hebben voor het produceren van ware zinnen van deze vorm die, gegeven een consistente theorie T, niet bewijsbaar zijn in T, dan zouden we oneindig veel zinnen van deze

vorm kunnen produceren, wat niet kan. Aangezien "s is incomprimeerbaar" een Goldbachachtige uitspraak is, kunnen we niet een dergelijke uitspraak formuleren waarvan we weten dat hij onbeslisbaar is in T. Zoals Gödels bewijs voor zijn eerste onvolledigheidsstelling sterk deed denken aan de leugenaarsparadox, zo doen bovenstaande observaties erg denken aan Berry's paradox: "het kleinste getal dat ondefinieerbaar is met behulp van minder dan honderd woorden".

Complexiteit als schijnbare verklaring voor onvolledigheid

De suggestie is mede door Chaitin zelf gewekt dat deze vorm van de onvolledigheidsstelling ons informatie geeft over het fenomeen onvolledigheid. Zo is gesuggereerd dat een stelling niet meer informatie kan bevatten (hiermee bedoelt Chaitin, een grotere Kolmogorov complexiteit heeft) dan de set axioma's waaruit de betreffende stelling is afgeleid. Hierdoor zou onvolledigheid een veel natuurlijker en wijdverbreid fenomeen zijn dan tot dan toe gedacht werd. Chaitin's onvolledigheids stelling verteld echter helemaal niets over de complexiteit van stellingen maar gaat over stellingen over complexiteit. Natuurlijk is het zo dat de uitspraak $K(s) > n$ zelf ook een complexiteit heeft die groter is dan n (we kunnen s immers uit de uitspraak destilleren). Dit betekent echter niet dat de complexiteit van deze uitspraak verantwoordelijk is voor zijn onbewijsbaarheid. Ook is het niet het geval dat een een stelling geen grotere complexiteit kan hebben dan de axioma's waarvan hij is afgeleid.[2] We moeten concluderen dat Chaitin's onvolledigheidsstelling ons slechts een speciaal geval van onvolledigheid geeft, welke we kunnen begrijpen op basis van informele argumenten zoals degene die we eerder hebben gezien. Een punt wat we wel uit Chaitin's onvolledigheidsstelling kunnen afleiden is dat de onbeslisbare rekenkundige uitspraken niet per sé formaliseri ngen van vreemde aan zichzelf refererende uitspraken hoeven te zijn. Dit punt hebben we echter ook al eerder gezien in paragraaf 3.3 bij de onbeslisbaarheid van uitspraken over Diofantische vergelijkingen.

8.2 Onvolledigheid en willekeurigheid

Incomprimeerbare rijtjes worden ook wel *willekeurige rijtjes* genoemd. Willekeurigheid in deze zin is, zoals we zagen, een graduele eigenschap - rijtjes kunnen meer of minder incomprimeerbaar zijn en dus meer of minder willekeurig. Daarnaast bestaat er een ander concept van willekeurigheid dat *geen* graduele eigenschap aanduidt maar een absolute eigenschap van oneindige rijtjes. Een voorbeeld van zo'n willekeurige oneindige rijtje is het oneindige bitrijtje Ω, geïntroduceerd door Chaitin. Ω is de limiet van een bepaalde berekenbare opsomming van eindige bitrijtjes $r_1, r_2, r_3, \ldots$ zodanig dat de $n$de bit van $\Omega = i$ dan en slechts dan als er een k is zodat de $n$de bit van r_m is i voor elke $m > k$. We kunnen dus de rijtjes $r_1, r_2, r_3, \ldots$ produceren middels berekeningen, maar de bits van Ω zelf zijn niet te berekenen.

[2] zie onderaan pagina 143 voor een duidelijk voorbeeld

Chaitin bewees dat elk formeel systeem slechts een eindig aantal juiste zinnen van de vorm "Het $n$de bit van Ω is i" kan beslissen en bovendien dat een formeel systeem van complexiteit n hoogstens $n+c$ zulke zinnen kan beslissen, voor een bepaalde constante c. Chaitin is erg onder de indruk van al deze resultaten. Hij stelt: "Gödel ontdekte onvolledigheid, Turing ontdekte onberekenbaarheid, en ik heb willekeurigheid ontdekt - het verbazingwekkende feit dat er wiskundige stellingen zijn die waar zijn zonder reden, ze zijn toevallig waar." *Waar zonder reden* lijkt te betekenen: niet middels redeneren te beslissen. Een analogie kan e.e.a. verhelderen: in de natuurkunde is willekeurigheid een bekend begrip, het verval van een bepaald radioactief atoom bijvoorbeeld is een niet te voorspellen proces, er kan slechts een statistische beschrijving van gegeven worden, er ligt geen mechanisme aan ten grondslag.[3] Maar zo'n onderscheiding heeft in de wiskunde geen zin: er zijn geen "natuurwetten van de wiskunde" waardoor sommige wiskundige waarheden *veroorzaakt* worden terwijl andere "zomaar" waar zijn. Als het vermoeden van Goldbach waar is dan is dat omdat elk even getal groter dan 2 de som is van twee priemgetallen. Als de stelling "Het $n$de bit van Ω is i" waar is, dan is dat zo omdat het $n$de bit van Ω inderdaad i is.

Een andere formulering van Chaitin geeft duidelijker weer wat zijn punt is, zonder dat daar meteen allerlei conclusies aan verbonden zijn (waar "willekeurig" vervangen is door "niet reduceerbaar"): "de bits van Ω zijn niet reduceerbaar, ze kunnen niet uit axioma's verkregen worden die eenvoudiger zijn dan de bits zelf". Maar wat houdt nu deze notie van *eenvoud* in die Chaitin hier bezigt? Als de eenvoudigheid van een rijtje gegeven is door een natuurlijk getal dan is het triviaal dat er rekenkundige stellingen zijn die niet uit eenvoudigere ware stellingen afgeleid kunnen worden. Chaitin kan er dus niet op doelen *dat* er zulke onafleidbare stellingen zijn. Ook kan hij niet bedoelen dat zijn stellingen van de vorm "Het $n$de bit van Ω is i" niet uit axioma's afgeleid kunnen worden die eenvoudiger zijn dan die zin zelf. Uit zijn bewijs dat elk formeel systeem slechts een eindig aantal juiste zinnen van de vorm "Het $n$de bit van Ω is i" kan beslissen volgt hoogstens het gegeven dat de eigenschappen van zo'n formeel systeem samen met de definitie van Ω bepalen welke zinnen van die vorm door het systeem beslist worden. Te stellen dat de bits van Ω niet middels "redeneren" bewezen kunnen worden maar uitsluitend gepostuleerd kunnen worden vereist een explicatie van wat "redeneren" dan wel precies is, en zo'n explicatie mist volledig in Chaitins werk. Het lijkt erop dat Chaitins enthousiaste uitspraak over het "verbazingwekkende feit dat er wiskundige stellingen zijn die waar zijn zonder reden" stoelt op de common sense-betekenis van het woord "willekeurig".

[3] Dat is tenminste een wijd geaccepteerde stellingname in de huidige natuurkunde, er zijn daarnaast veel wetenschappers die zulke antideterministische conclusies niet zonder meer willen trekken.

8.3 Onvolledigheid en oneindigheid

Veelzijdige Onvolledigheden

Er bestaan tal van onvolledige systemen die als zodanig zijn ontworpen om uiteenlopende redenen. Zulke systemen voldoen veelal niet eens aan de eisen waardoor Gödels stelling erop van toepassing zou zijn, hun onvolledigheid blijkt duidelijk uit de betreffende definities. Maar zelfs als we ons beperken tot theorieën waarop de onvolledigheidsstelling van toepassing is zijn er significante verschillen tussen verschillende onvolledigheidsresultaten. We bekijken ZFC onder de aanname dat ZFC correct is wat betreft haar rekenkundige stellingen.

Allereerst weten we natuurlijk dat de rekenkundige component van ZFC onvolledig is omdat daarop Gödels onvolledigheidsstelling van toepassing is, maar de onbeslisbare stellingen die we daarmee identificeren zijn nauwelijks van wiskundige interesse. Ten tweede echter bewijst ZFC het bestaan van hele hordes oneindige sets, maar laat vele uitspraken over die sets onbeslist. Het meest bekend is de continuümhypothese (CH) van Cantor, die stelt dat elke oneindige subset van $\mathbb{R}$ ofwel dezelfde cardinaliteit heeft als $\mathbb{R}$ ofwel aftelbaar oneindig is, dat er dus geen cardinaalgetal x bestaat waarvoor geldt $|\mathbb{R}| > x > |\mathbb{N}|$. Het bewijs van deze onbeslisbaarheid heeft niets te maken met Gödels onvolledigheidsstelling, en de aanname van CH of $\neg$CH impliceert geen nieuwe rekenkundige stellingen. Ten derde blijkt het zo te zijn dat ZFC geen uitspraken doet over hoe "grote" oneindigheden er nou eigenlijk bestaan. Een bepaalde groep stellinge n, axioma's van oneindigheid geheten, doet uitspraken over deze onbepaaldheid in ZFC. Zo'n axioma van oneindigheid A heeft de eigenschap in ieder geval niet bewijsbaar te zijn in ZFC (dat betekent: ZFC + $\neg A$ is consistent), terwijl de weerlegbaarheid vaak problematisch is (dat betekent: ZFC + A zou inconsistent kunnen zijn). Deze groep stellingen is opgedeeld in twee subgroepen: zwakke axioma's van oneindigheid (the universe of sets has certain closure properties and therefore contains very large sets) en sterke axioma's van oneindigheid (that isolate some property of the smallest infinite set $\mathbb{N}$ and simply state that there are larger infinite sets with a corresponding property)

Gödels connectie

Waarom dit voorgaande over die vrij esoterische axioma's van oneindigheid? Welnu, er is een connectie tussen deze axioma's van oneindigheid en de onvolledigheid m.b.t. rekenkundige stellingen, welke Gödel zelf reeds opmerkte: uitbreidingen van een theorie T met axioma's van oneindigheid hebben altijd rekenkundige consequenties die niet in T zelf te bewijzen zijn. Om dat begrijpelijk te maken een voorbeeld. ZFC zelf bevat reeds het zwakste axioma van oneindigheid: $\exists\mathbb{N}(\varnothing \in \mathbb{N} \wedge \forall x(x \in \mathbb{N} \rightarrow x \cup \{x\} \in \mathbb{N}))$, ofwel: $\mathbb{N}$ bestaat. Met dit axioma kunnen we het bestaan van een *model* van de overige axioma's van ZFC bewijzen, waarmee dus meteen de consistentie daarvan bewezen is. Dus als we ZFC zonder dit axioma van oneindigheid ZFC$^{-\omega}$ noemen dan geldt ZFC $\vdash$

Con(ZFC$^{-\omega}$). ZFC$^{-\omega}$ is zelf een theorie waarop de onvolledigheidsstelling van toepassing is en dus zijn eigen consi stentie *niet* bewijst. Dus we zien dat het toevoegen van dit zwakste axioma van oneindigheid nieuwe rekenkundige stellingen bewijsbaar maakt, in het bijzonder de consistentie van ZFC$^{-\omega}$ en daarmee van PA (want ZFC$^{-\omega}$ is in zijn rekenkundige onderdeel equivalent aan PA). Verdere axioma's van oneindigheid bewerken op eenzelfde wijze uitbreidingen van de rekenkundige stellingen van ZFC. De consequenties van sterke axioma's van oneindigheid zijn verreweg van duidelijk. Maar ook hier geldt weer dat er onder deze uitbreidingen van de rekenkundige stellingen van ZFC tot nog toe geen stellingen gevonden zijn die van substantieel wiskundig belang zijn.

De Paris-Harrington-stelling

Laatstgenoemd probleem houdt vele geesten bezig. Een eerste stap in de goede richting is een bewijs dat een bepaald combinatorisch principe onbewijsbaar is in PA uit 1977, bekend geworden als de Paris-Harrington-stelling. Het interessante aan dit bewijs is dat het eens niet om Gödelnummers of formele systemen gaat, maar om een ogenschijnlijk insignificante aanpassing van een gangbaar wiskundig principe. Dit bewijs is de moeite van het bekijken dus zeker waard.

Stel we hebben een eindige verzameling A van getallen. Een *n-elementen deelverzameling* van A is een verzameling B met n elementen, allemaal afkomstig uit A. Een *m-partitie* van alle n-deelverzamelingen van A sorteert deze deelverzamelingen in m categorieën $C_1, C_2, ..., C_m$ zodanig dat iedere n-elementen deelverzameling van A in precies één categorie komt. Tenslotte is een subset H van A *homogeen* voor de gegeven partitie als alle n-elementen deelverzamelingen van H in dezelfde categorie horen. De stelling van Ramsey betreft het bestaan van zulke homogene deelverzamelingen: voor elke n, m en k is er een getal p zodat als A minstens p elementen bevat er voor elke m-partitie van de n-deelverzameling van A een homogene deelverzameling H van A is met minstens k elementen.

Deze stelling gaat over eindige verzamelingen, maar door eindige sets van getallen middels getallen te representeren kan zij geformuleerd worden als een rekenkundige stelling en is bewijsbaar in PA. De *Paris-Harrington-stelling* betreft een lichte aanpassing hiervan. We zeggen dat een verzameling A van getallen *relatief groot* is als het aantal elementen van A groter is dan het kleinste getal in A. Ramsey's stelling blijft gelden als we aan H de eis stellen dat het een relatief grote verzameling moet zijn. Maar, zo laat de Paris-Harrington-stelling zien, dat is *niet* bewijsbaar in PA. Deze instantie van onvolledigheid blijkt een instantie van Gödelachtige onvolledigheid te zijn: deze licht aangepaste versie van Ramsey's stelling is equivalent met de stelling "PA is Σ-correct". Daaruit volgt dat deze stelling bewezen kan worden door de correctheid van PA te bewijzen, wat op basis van een axioma van oneindigheid binnen ZFC mogelijk is.

Latere ontwikkelingen

De Paris-Harrington-stelling suggereert dat er wellicht meer zulke combinatorische principes zijn in de wiskunde die onbewijsbaar blijken te zijn in ZFC maar middels axioma's van oneindigheid alsnog bewezen kunnen worden. Harvey Friedman heeft in deze richting een hoop werk verzet. Maar, ook al gaat het hier over combinatorieke stellingen die van wiskundig belang zijn, het zijn toch steeds weer vrij obscure stellingen vanuit wiskundig oogpunt, zodat, mocht zo'n combinatoriek principe de consistentie van een bepaald sterk axioma van oneindigheid impliceren, het zeker geen uitgemaakte zaak is of op grond daarvan zo'n axioma geaccepteerd moet worden. Gödel meende dat de consequenties van axioma's van oneindigheid voor de eindige wiskunde zo rijk en verhelderend zou kunnen zijn dat we ze, ondanks het feit dat ze wat betreft hun uitspraken over het bestaan van oneindige verzamelingen zeker niet vanzelfsprekend zijn, toch zouden moeten accepteren. Friedmans werk is zeker relevant voor dit idee, het zal moeten blijken wat de uiteindelijke uitkomst van zijn en vergelijkbaar onderzoek zal zijn.