Technische Universiteit Delft
Faculteit Elektrotechniek, Wiksunde en Informatica
Delft Institute of Applied Mathematics

"De onvolledigheidsstellingen van Gödel"

(Gödels incompleteness theories)

Verslag ten behoeve van het
Delft Institute for Applied Mathematics
als onderdeel ter verkrijging

van de graad van

BACHELOR OF SCIENCE
in
TECHNISCHE WISKUNDE

door

ROSA MEIJER

Delft, Nederland
Augustus 2008

Inhoudsopgave

1 Inleiding

Op 28 april 1906 werd in Brno (gelegen in het huidige Tsjechië) een van de, wat later zou blijken, grootste logici aller tijden geboren: Kurt Friedrich Gödel. Zijn beroemdste stelling is zonder twijfel de **onvolledigheidsstelling**. Eigenlijk valt deze stelling uiteen in twee delen, de eerste en de tweede onvolledigheidsstelling van Gödel, maar deze twee zijn zeer nauw met elkaar verwant.

In het begin van de twintigste eeuw werd geprobeerd de hele wiskunde te beschrijven met één formeel systeem, een zogenaamd axiomatisch systeem. In een axiomatisch systeem wordt gebruik gemaakt van axioma's (stellingen die niet bewezen worden, maar wel als waar worden aangenomen) en afleidingsregels. Op deze manier zou de hele wiskunde terug te brengen zijn tot zuiver logische termen. Dan zou vervolgens voor elke uitspraak gekeken kunnen worden of deze uitspraak al dan niet een stelling was (oftewel, of de uitspraak al dan niet afleidbaar was uit de gegeven axioma's in combinatie met de afleidingsregels).

Russell en Whitehead dachten zo'n axiomatisch systeem gevonden te hebben en publiceerden in de jaren 1910 tot 1913 het uit drie delen bestaande "Principia Mathematica". Elke wiskundige waarheid zou naar hun idee af te leiden zijn met behulp van de gekozen axioma's en afleidingsregels.

Hoe mooi het idee ook was, Gödel liet in 1931 zien dat het bij een idee zou blijven. Hij liet niet alleen zien dat "Principia Mathematica" ontoereikend was om de eigenschappen van de natuurlijke getallen te beschrijven, hij liet bovendien zien dat **geen enkel** consistent axiomatisch systeem deze eigenschappen ooit zou kunnen beschrijven! De (eerste) onvolledigheidsstelling van Gödel zegt namelijk het volgende: **elk** axiomatisch systeem dat de basiseigenschappen van de natuurlijke getallen beschrijft is ofwel onvolledig ofwel inconsistent. Dit betekent dus dat er beweringen zullen zijn die wel waar zijn, maar niet bewezen kunnen worden, of juist dat er formules bewezen kunnen worden die niet waar zijn. Aangezien dit laatste in geen enkel systeem de bedoeling zou mogen zijn, reduceert de eerste onvolledigheidsstelling dus tot het volgende: Binnen geen enkel consistent axiomatisch systeem dat de eigenschappen van de natuurlijke getallen beschrijft, is het mogelijk om alle ware uitspraken (betreffende deze natuurlijke getallen) af te leiden!

Ook bewees Gödel nog iets anders: de tweede onvolledigheidsstelling. Deze stelling zegt dat een consistent axiomatisch systeem haar eigen consistentie niet kan bewijzen.

2 Eerste-Orde Logica

Er zijn, zoals dat vaak het geval is bij stellingen, meerdere manieren waarop de eerste onvolledigheidsstelling van Gödel bewezen kan worden.
Voordat ik een van deze manieren uit zal werken, zal ik eerst aandacht besteden aan de manier waarop de eerste-orde logica is opgebouwd. Dit is belangrijk omdat de eigenschappen van de natuurlijke getallen met behulp van eerste-orde logica beschreven zullen worden. Ik zal in dit hoofdstuk dan ook voornamelijk definities uitwerken.

Allereerst zal ik twee (waarschijnlijk bekende) begrippen toelichten: **functies** en **relaties**.

Als A een verzameling is en n is een natuurlijk getal, dan is een n-aire **functie** f, die werkt op A, een afbeelding van A^n naar A. Met andere woorden: f beeldt elke n-tupel $(a_1, a_2, \ldots, a_n)$ bestaande uit elementen van A af op een uniek element uit A.

Als A weer een verzameling is en n een natuurlijk getal, dan is een n-aire **relatie** r op A een deelverzameling van A^n. Anders gezegd: r bestaat uit een collectie n-tupels $(a_1, a_2, \ldots, a_n)$ bestaande uit elementen van A.

Nu kan het begrip **taal** ingevoerd worden:

Een eerste-orde **taal** is een verzameling van verschillende symbolen, waarbij die symbolen in een van de volgende categorieën moeten vallen:

- haakjes "(" en ")"[1]
- connectieven $(\vee, \wedge, \rightarrow, \leftrightarrow, \neg)$
- kwantoren $(\forall, \exists)$
- functiesymbolen (noem de verzameling van functiesymbolen $\mathcal{F}$)
- gelijkheidssymbool $(=)$
- relatiesymbolen (noem de verzameling van relatiesymbolen $\mathcal{R}$)
- constanten (noem de verzameling van constanten $\mathcal{C}$)
- variabelen (een oneindig aantal)

[1] In het vervolg van dit verslag zal ik deze haakjes niet altijd op dezelfde manier gebruiken. In grote formules zijn ze onontbeerlijk voor de duidelijkheid, maar wanneer de duidelijkheid niets te wensen overlaat, zal ik zo weinig mogelijk haakjes gebruiken, om zo de leesbaarheid te vergroten. De totale formules zal ik, om diezelfde reden, doorgaans ook niet omsluiten door haakjes. Ook worden de haakjes natuurlijk puur als leestekens gebruikt, zonder verdere wiskundige betekenis.

Vaak ook wordt de verzameling $\mathcal{L} = \mathcal{C} \cup \mathcal{F} \cup \mathcal{R}$ een **eerste-orde taal** genoemd. De kwantoren en dergelijke worden dan niet vermeld, omdat deze symbolen voor alle talen hetzelfde zijn en hun vermelding dus niets specifieks toevoegt aan een bepaalde taal.

In een eerste-orde taal $\mathcal{L}$ kunnen vervolgens **termen**, **atomaire formules** en **formules** gedefinieerd worden.

Een **term** t van $\mathcal{L}$ is ofwel een variabele, ofwel een constante (uit $\mathcal{C}$), ofwel t wordt gegeven door $ft_1 \dots t_n$ waarbij f een n-air functiesymbool is (uit $\mathcal{F}$) en elke t_i een term van $\mathcal{L}$ is.

Nu kunnen de **formules** van een taal $\mathcal{L}$ inductief gedefinieerd worden. Te beginnen met de **atomaire formules**.

Atomaire formules zijn er in twee vormen: ze zijn ofwel van de vorm $(s = t)$ waarbij s en t termen moeten zijn, ofwel ze zijn van de vorm $(rt_1 \dots t_n)$ waarbij r een n-air relatiesymbool is en t_1 tot en met t_n termen zijn.

Een atomaire formule is uiteraard ook gewoon een **formule**. Verder geldt nu dat als F een formule is, $(\neg$ F) dat ook is. Als F en G beide formules zijn, geldt dat ook voor (F $\vee$ G), (F $\wedge$ G), (F $\rightarrow$ G) en (F $\leftrightarrow$ G). Bovendien geldt dat $((\forall x)$F) en $((\exists x)$F) formules zijn, als F een formule is en x een variabele.

Dan is er nog een laatste definitie: Een **zin** is een formule waarin geen vrije variabelen voorkomen. Waarbij een variabele x een vrije variabele is, als er geen kwantor is die deze variabele als argument heeft.

Aan alleen een taal heb je nog niet zo veel. Het is eigenlijk gewoon een betekenisloze verzameling symbolen. Ook de bijbehorende formules en termen zijn weinigzeggend, aangezien je niet weet wat de functie- en relatiesymbolen betekenen en je zodoende dus ook geen enkele uitspraak kan doen over of een formule al dan niet "waar" is.

Vaak wordt er allereerst voor gekozen een verzameling van gesloten formules te kiezen die vanaf dan als waar worden beschouwd. Zo'n verzameling gesloten formules wordt een **theorie** genoemd, en de gesloten formules die deze theorie bevat, noemt men ook wel **axioma's**. Een **axioma** is dus een niet bewezen, maar als grondslag aanvaarde uitspraak.

De **stellingen** van de theorie zijn de zinnen die met behulp van afleidingsregels (waar ik later op terug zal komen), uit de axioma's afgeleid kunnen worden.

Axioma's komen doorgaan tot stand wanneer er binnen verschillende wiskundige gebieden eenzelfde soort gedrag wordt waargenomen. Zo is bijvoorbeeld de theorie der groepen ontstaan toen bleek dat onder andere permutaties, matrices en

getallen veel gemeen hadden.
De taal van deze groepentheorie bevat één constante (e) en twee functiesymbolen (f en i).

De bijbehorende axioma's worden gegeven door:

1. $(\forall x)(\forall y)(\forall z)(ffxyz = fxfyz)$
2. $(\forall x)(fxe = fex = x)$
3. $(\forall x)(fxix = fixx = e)$

Elke wiskundige groep is (per definitie) een **structuur** voor deze theorie, zoals zodirect zal blijken

Wanneer je axioma's geformuleerd hebt zoek je een **structuur**, zodanig dat de axioma's uit je eerder gekozen **theorie** daarin waar zijn. In een dergelijke structuur wordt aan de elementen uit je taal een interpretatie toegekend en bovendien wordt er een verzameling gekozen waarop de functie- en relatiesymbolen zullen werken. Zo'n structuur heet dan een **model** voor je theorie.

Een **interpretatie** I van een eerste-orde taal $\mathcal{L}$, gedefinieerd op een niet-lege verzameling A, is een afbeelding die aan elk symbool uit $\mathcal{L}$ een functie, relatie of constante toekent op de volgende manier:

- $I(c)$ is een element uit A voor elke constante c uit $\mathcal{C}$
- $I(f)$ is een n-aire functie op A voor elk n-aire functiesymbool f uit $\mathcal{F}$
- $I(r)$ is een n-aire relatie op A voor elk n-aire relatiesymbool r uit $\mathcal{R}$

Een $\mathcal{L}$**-structuur A** wordt vervolgens gedefinieerd door $\mathbf{A}=(A, I)$, waarbij I de interpretatie van $\mathcal{L}$ op A is. Meestal wordt deze notatie wat veranderd, door de structuur weer te geven als: $(A, \mathcal{C}, \mathcal{F}, \mathcal{R})$. (De interpretatie van de constanten, de functie- en relatiesymbolen spreekt vaak voor zich.)

In een structuur is dus zowel de taal, als de interpretatie van deze taal op een bepaalde verzameling gedefinieerd. En bovendien is de structuur (noem deze voor het gemak $\mathfrak{S}$) zodanig gekozen dat de axioma's uit de theorie **waar** zijn in deze structuur. Dit wordt als volgt aangegeven: $\mathfrak{S} \models$ "axioma".

Verder geldt er uiteraard dat $\mathfrak{S} \models t_1 = t_2$, met t_1 en t_2 termen dan en slechts dan als deze termen aan elkaar gelijk zijn (de interpretatie van een term is uiteindelijk gewoon een element uit de verzameling waar je mee werkt, dus dit is makkelijk te beslissen) en dat $\mathfrak{S} \models rt_1t_2 \ldots t_3$ dan en slechts dan als er daadwerkelijk aan de relatie is voldaan (het relatiesymbool heeft immers een unieke interpretatie gekregen, en zo zou er dus bijvoorbeeld vast kunnen liggen dat 3 kleiner is dan 4). Als F gelijk is aan $\neg$G, zal F waar zijn dan en slechts dan als G

niet waar is, en op een dergelijke manier kan ook een waarheidswaarde worden toegekend aan F wanneer F gelijk is aan G$\vee$H, G$\wedge$H, G$\rightarrow$H, G$\leftrightarrow$H, indien de waarheidswaarden van G en H (soms is het al genoeg om de waarheidswaarde van één van beiden te weten) bekend zijn.
Als F(x) gelijk is aan $\forall y$G(y, x), is F(a) waar (waarbij a is ingevuld als waarde voor x) dan en slechts dan als G(y, a) waar is voor elke mogelijke y, en als F(x) gelijk is aan $\exists y$G(y, x), is F(a) waar dan en slechts dan als er een y is waarvoor G(y, a) waar is.

Om nu weer terug te komen op het voorbeeld van de groepentheorie: wanneer als structuur wordt gekozen voor bijvoorbeeld de wiskundige groep ($\mathbb{Z}$, +) geldt de volgende interpretatie voor de constante en de functiesymbolen:
f wordt gegeven door "+" en de interpretatie van f is de binaire functie optellen, i wordt gegeven door "-" en de interpretatie van i is de unaire functie "tegengesteld maken" en e wordt gegeven door "0" waarmee gewoon het getal nul wordt bedoeld.
De axioma's kunnen nu als volgt geïnterpreteerd worden:
axioma 1 geeft aan dat optellen een associatieve functie is,
axioma 2 geeft aan dat 0 het eenheidselement/neutrale element is, en
axioma 3 geeft aan dat $-x$ de inverse van x is voor alle $x \in \mathbb{Z}$.

Nu zal ik de taal, theorie en de structuur beschrijven, waarin de eigenschappen van de natuurlijke getallen worden beschreven. Met deze taal, theorie en structuur zal ik de rest van dit verslag werken.

Hierna zullen we altijd met de volgende taal werken, de taal van de getaltheorie:
$\mathcal{L}_{NT} = \{0, S, +, \cdot, E, <\}$

Als theorie kiezen we voor een verzameling axioma's, die de basiseigenschappen van de natuurlijke getallen aardig beschrijft. (In feite een versimpelde versie van de bekende verzameling Peano axioma's.)

Deze verzameling van axioma's zal aangegeven worden met "N" en bevat de volgende axioma's:

1. $(\forall x)\neg(Sx = 0)$.
2. $(\forall x)(\forall y)(Sx = Sy \rightarrow x = y)$.
3. $(\forall x)(x + 0 = x)$.
4. $(\forall x)(\forall y)\big(x + Sy = S(x + y)\big)$.
5. $(\forall x)(x \cdot 0 = 0)$.
6. $(\forall x)(\forall y)\big(x \cdot Sy = (x \cdot y) + x\big)$.
7. $(\forall x)(xE0 = S0)$.
8. $(\forall x)(\forall y)\big(xE(Sy) = (xEy) \cdot x\big)$.
9. $(\forall x)\neg(x < 0)$.
10. $(\forall x)(\forall y)\big(x < Sy \leftrightarrow (x < y \vee x = y)\big)$.
11. $(\forall x)(\forall y)\big((x < y) \vee (x = y) \vee (y < x)\big)$.

(NB: Bij het geven van de axioma's heb ik de infix notatie gebruikt ($Sx = 0$ ipv $= Sx0$) omdat deze notatie naar mijn mening net wat duidelijker is dan de prefix notatie. In de rest van dit stuk zal ik echter de prefix notatie gebruiken omdat de codering die Gödel gebruikte daarop ingesteld is.)

Als laatste moet nu een structuur gevonden worden waarin bovenstaande axioma's waar zijn, waarin gewerkt wordt met de natuurlijke getallen en waarin alle constanten, functie- en relatiesymbolen uit $\mathcal{L}_{NT}$ een betekenis krijgen.

Hierna zullen we werken met het standaard model van de natuurlijke getallen (de toevoeging "standaard" slaat erop dat we echt alleen werken met de natuurlijke getallen en niet met zogenaamde "niet-standaard natuurlijke getallen"):
$\mathfrak{N} = (\mathbb{N}, 0, S, +, \cdot, E, <)$
Hierbij is $\mathbb{N}$ de verzameling natuurlijk getallen. De constante "0" staat voor het getal 0, "S" is de functie van de opvolger (dus $S0 = 1$, $SS0 = 2$, etc.), "+" staat voor optellen, "$\cdot$" voor vermenigvuldigen, "E" staat voor de exponentfunctie (Exy is dus eigenlijk x^y) en het relatiesymbool "$<$" betekent niets anders dan "kleiner dan".

Hiermee zijn alle begrippen die specifiek zijn voor de eerste-orde logica uitgelegd.

3 Overige begrippen

Afgezien van de begrippen die specifiek betrekking hebben op de eerste-orde logica, zal ik ook nog gebruik maken van enkele andere belangrijke definities. Deze zal ik binnen dit hoofdstuk kort toelichten.

Om te beginnen zal ik de begrippen **definieerbare verzameling** en **recursieve verzameling** toelichten.

3.1 Definieerbare en Recursieve verzamelingen

Een verzameling A ($\subseteq \mathbb{N}^k$) heet **definieerbaar**, als er een $\mathcal{L}_{NT}$-formule $\phi(\underset{\sim}{x})$ bestaat (een formule die alleen symbolen uit de eerder gedefinieerde taal $\mathcal{L}_{NT}$ bevat) die waar is in ons model dan en slechts dan als de x een element van A is. Om het wiskundig op te schrijven:
Er moet een formule $\phi(\underset{\sim}{x})$ zijn zo dat

$$\begin{array}{ll} \forall \underset{\sim}{a} \in A & \mathfrak{N} \models \phi(\overline{\underset{\sim}{a}}) \\ \forall \underset{\sim}{b} \notin A & \mathfrak{N} \models \neg\phi(\overline{\underset{\sim}{b}}) \end{array}$$

De formule ϕ **definieert** de verzameling A.

Bovenstaande notatie verdient nog wat extra uitleg. De "$\underset{\sim}{\ }$" in $\overline{\underset{\sim}{a}}$ duidt erop dat a een vector is ($\overline{\underset{\sim}{a}}$ is dus een afkorting voor $\overline{a_1}, \overline{a_2}, \ldots, \overline{a_n}$). Verder wordt $\overline{a}$ als afkorting gebruikt voor $\underbrace{SSS\ldots S}_{a\,S'en}0$. Dit moet aangezien de enige constante die we hebben in onze taal de constante 0 is.

De definitie van een **recursieve verzameling** gaat verder dan die van een **definieerbare verzameling**. In een recursieve verzameling is er namelijke niet alleen sprake van "waar zijn in een model" maar van "bewijsbaar zijn uit een verzameling axioma's". Als F bewijsbaar is uit onze verzameling axioma's N wordt dit met symbolen als volgt aangegeven: $N \vdash$ F. Een formule F heet "bewijsbaar" uit N, als F afleidbaar is met behulp van de axioma's waarop al dan niet afleidingsregels zijn toegepast. (Welke afleidingsregels dit zijn doet er vooralsnog niet toe.)

De definitie is als volgt: Een verzameling A heet **recursief** als er een $\mathcal{L}_{NT}$-formule is zo dat

$$\begin{array}{ll} \forall \underset{\sim}{a} \in A & N \vdash \phi(\overline{\underset{\sim}{a}}) \\ \forall \underset{\sim}{b} \notin A & N \vdash \neg\phi(\overline{\underset{\sim}{b}}) \end{array}$$

Men zegt nu dat de formule ϕ de verzameling A **representeert**.

Elke recursieve verzameling is dus ook automatisch definieerbaar en wel door

de formule die de verzameling representeert. De omkering hoeft niet automatisch te gelden. Wanneer de verzameling echter door een speciale formule wordt gedefinieerd, geldt er wél direct dat de verzameling ook door die formule wordt gerepresenteerd. Dit geldt als de definiërende formule een **Δ-formule** is.

Voordat ik hier verder op in zal gaan, zal ik eerst kort uitleggen wat een **Δ-formule** precies is. Tevens zal ik de begrippen Σ- en Π**-formules** invoeren, omdat ook deze begrippen (en dan met name de eerste) belangrijk zullen worden in het bewijs van de eerste onvolledigheidsstelling.

Ook wil ik nog het volgende opmerken: er bestaan ook **recursieve functies**. In feite zou je een functie $f : \mathbb{N}^k \to \mathbb{N}$ op kunnen vatten als een deelverzameling van $\mathbb{N}^{k+1}$. Wanneer je nu van deze verzameling bewijst dat deze recursief is, kun je ook zeggen dat de functie recursief is. Als $N \vdash \phi(\underline{a}, \underline{y})$ als $y = f(\underline{a})$ (waarbij f de functie is) en $N \vdash \neg\phi(\underline{a}, \underline{y})$ als $y \neq f(\underline{a})$, zeg je dat ϕ de functie f representeert (en dus eigenlijk de verzameling van alle (vector,getallen)-paren die er uitzien als ($\underline{a}$,$f(\underline{a})$) representeert). De functie f heet nu recursief.

3.2 Δ - , Σ - en Π - formules

Een Σ**-formule** kan het volgende zijn:

1. een atomaire formule
2. de negatie van een atomaire formule
3. een combinatie van 1 en 2, door gebruik van de connectieven $\wedge$ of $\vee$
4. een combinatie van 1,2 en 3 met daaraan één (of meer) begrensde kwantor(en), dan wel de kwantor "$\exists$" toegevoegd (of meerdere van deze kwantoren)

Een begrensde kwantor is een kwantor van de vorm "$\forall x < u$" of "$\exists x < u$". Verder geldt dat de kwantoren niet zomaar binnenin de Σ-formule voor mogen komen, maar dat de formule in **prenex vorm** geschreven moet zijn. De prenex vorm van een formule F wordt gegeven door $Q_1 x_1 \ldots Q_n x_n \mathrm{G}$, waarbij de Q_i's de kwantoren weergeven en in G geen kwantoren meer voorkomen.

De definitie van een Π**-formule** is identiek aan die van een Σ-formule, afgezien van het feit dat de kwantor "$\exists$" door "$\forall$" vervangen moet worden.

Een **Δ-formule** kan alleen begrensde kwantoren bevatten, maar is verder op dezelfde wijze samengesteld als de Σ- en Π-formules.

De formele definities van deze drie soorten formules bevatten alleen de connectieven "$\neg$", "$\wedge$" en "$\vee$". De verzameling van standaardconnectieven bevat

natuurlijk ook nog de symbolen "$\rightarrow$" en "$\leftrightarrow$". Toch kan er binnen Σ-, Π- en Δ-formules gewoon gewerkt worden met deze laatste twee connectieven. Dit kan aangezien deze laatste connectieven uit te drukken zijn in de eerste drie. Zo geldt bijvoorbeeld dat "P$\rightarrow$Q" (met P en Q formules), ook geschreven kan worden als "$\neg$P$\vee$Q" en ook voor "P$\leftrightarrow$Q" kan een dergelijke uitdrukkingen gevonden worden. De verzameling $\{\neg, \wedge, \vee\}$ is een zogeheten **adequate** verzameling.

Wat bovenstaande formules bijzonder maakt (en wat ik ook al kort heb genoemd) is het volgende:

Propositie 3.2.1. *Als $\phi(\underset{\sim}{x})$ een Σ-formule is met vrije variabelen $\underset{\sim}{x}$, als $\underset{\sim}{t}$ termen zijn, waarin geen variabelen voorkomen en als geldt dat $\mathfrak{N} \models \phi(\underset{\sim}{t})$, dan geldt bovendien dat $N \vdash \phi(\underset{\sim}{t})$.*

Stel dus dat $\phi(\underset{\sim}{x})$ een Σ-formule is, die waar is voor bepaalde waarden van $\underset{\sim}{x}$. Dan geldt dus bovendien dat de zin, die ontstaat door in $\phi(\underset{\sim}{x})$ de $\underset{\sim}{x}$ te vervangen door een "termvector" $\underset{\sim}{t}$ waarin geen variabelen voorkomen en waarvoor $\phi(\underset{\sim}{t})$ waar is (elk element van $\underset{\sim}{t}$ is dus gewoon een constante, of de uitkomst van een functie waarin constanten ingevuld zijn), bewijsbaar is in ons axiomatisch systeem N! De omkering geldt helaas niet: Als $\mathfrak{N} \models \neg\phi(\underset{\sim}{t})$, kan niet **bewezen** worden dat $\neg\phi(\underset{\sim}{t})$ waar is. Dit heeft alles te maken met het feit dat $\neg((\exists x)\phi)$ gelijk is aan $(\forall x)\neg\phi$. Een negatie van een Σ-formule hoeft dus geen Σ-formule te blijven, maar kan veranderen in een Π-formule, waarvoor bovenstaande propositie niet geldt.

Immers: als $\mathfrak{N} \models (\exists x)\phi(x)$, dan is er een $n \in \mathbb{N}$ (even aannemend dat het argument slechts uit één element bestaat), met $\mathfrak{N} \models \phi(n)$, en zodoende hoeft alleen maar aangetoond te worden dat $N \vdash \phi(\underbrace{SSS\ldots S}_{n S'en}0)$.
Maar als $\mathfrak{N} \models (\forall x)\phi(x)$, zijn er opeens oneindig veel bewijzen nodig:
$N \vdash \phi(0)$, $N \vdash \phi(S0)$, $N \vdash \phi(SS0)$, enzovoorts.
Hiervoor kunnen echt verschillende bewijzen nodig zijn, zodat $N \vdash (\forall x)\phi(x)$ niet waar hoeft te zijn. (Een bewijs moet namelijk eindig zijn.)

Neem nu aan dat ϕ een Δ-formule is. Aangezien ϕ dan bovendien een Σ-formule is, weten we nu dat als $\mathfrak{N} \models \phi$ geldt, er ook geldt dat $N \vdash \phi$. Maar stel nu dat ϕ niet waar is, oftewel dat geldt dat $\mathfrak{N} \models \neg\phi$. Uiteraard is $\neg\phi$ ook weer een Δ-formule (de eventuele gebonden kwantoren blijven gebonden, alleen verandert de "$\exists$" in een "$\forall$" en omgekeerd), en dus geldt ook dat $\neg\phi$ een Σ-formule is en uit **Propositie 3.2.1** volgt dan dat $N \vdash \neg\phi$. Dit geeft de volgende propositie:

Propositie 3.2.2. *Als $\phi(\underset{\sim}{x})$ een Δ-formule is met vrije variabelen $\underset{\sim}{x}$, als $\underset{\sim}{t}$ termen zijn waarin geen variabelen voorkomen, en als er geldt dat $\mathfrak{N} \models \phi(\underset{\sim}{t})$, dan geldt er dat $N \vdash \phi(\underset{\sim}{t})$. Anderzijds is het zo dat als $\mathfrak{N} \models \neg\phi(\underset{\sim}{t})$ geldt, ook $N \vdash \neg\phi(\underset{\sim}{t})$ geldt.*

Deze propositie zegt dus precies wat al eerder werd gezegd: Als een Δ-formule een verzameling definieert ($\mathfrak{N} \models \phi(\overline{a})$ desda $\underset{\sim}{a}$ een element van de verzameling is), dan wordt de verzameling bovendien door deze formule gerepresenteerd! Voor elk mogelijk argument van ϕ kan dus worden bewezen of dit argument al dan niet tot de gegeven verzameling behoort!

Om dit ook weer door te trekken naar de representatie van functies: wanneer een Δ-formule ϕ een functie f definieert ($\mathfrak{N} \models \phi(\overline{a}, \overline{y})$ desda $y = f(\underset{\sim}{a})$), representeert de formule de functie ook. Wanneer een functie gerepresenteerd wordt, houdt dit het volgende in:

$$N \vdash (\forall y)\big(\phi(\overline{a}, y) \leftrightarrow y = \overline{f(\underset{\sim}{a})}\big).$$

Het kunnen representeren van verzamelingen (en functies) met behulp van Δ-formules zal van groot belang zijn in het bewijs van de onvolledigheidsstelling.

4 Het idee achter het bewijs

Om Gödels eerste onvolledigheidsstelling te bewijzen is het volgende nodig: een formule ϕ zodat

$$\mathfrak{N} \models \phi \text{ maar } N \nvdash \phi.$$

Dat wil zeggen: een **ware**, maar niet **bewijsbare** uitspraak.

Om aan deze eis te voldoen construeerde Gödel:

een formule ϕ die van zichzelf "zegt" dat ze onbewijsbaar is (gegeven een willekeurig consistent axiomatisch systeem).

Stel dat ϕ inderdaad niet bewijsbaar is in ons axiomatisch systeem. In dat geval is ϕ dus een ware formule (ϕ zegt dat ze onbewijsbaar is en is dit ook daadwerkelijk). Hiermee is dus een ware maar onbewijsbare formule geconstrueerd en dit houdt in dat het axiomatische systeem **onvolledig** is!
Stel nu dat ϕ wél bewijsbaar is. Dan is ϕ dus onwaar (ϕ zegt dat ze onbewijsbaar is, maar is toch te bewijzen). Hieruit zou volgen dat we in staat zijn onwaarheden af te leiden in ons model. Bovendien zal later blijken, dat wanneer een dergelijke ϕ bewezen kan worden, daaruit direct volgt dat ook $\neg\phi$ bewijsbaar is. Als zowel ϕ als $\neg\phi$ bewijsbaar zijn, is ons systeem **inconsistent**.
Aangezien ϕ ofwel bewijsbaar ofwel onbewijsbaar is, en de aanname dat ze bewijsbaar is tot de conclusie leidt dat ons systeem inconsistent is, moet, gezien de aanname van een consistent systeem, wel gelden dat ϕ onbewijsbaar is. De formule ϕ is dus waar en onbewijsbaar en hieruit volgt dat het axiomatisch systeem onvolledig is.

Om een dergelijke ϕ te kunnen construeren moet er grofweg aan twee voorwaarden voldaan worden:

1. De bewijsbaarheid van formules moet in een $\mathcal{L}_{NT}$-formule kunnen worden uitgedrukt.
2. Een formule ϕ moet kunnen refereren aan haar eigen bewijsbaarheid.

In de komende hoofdstukken zullen deze voorwaarden uitgewerkt worden.

5 Gödelnummering

Om te bewijzen of een getal/vector al dan niet tot een bepaalde verzameling behoort, is het genoeg een Δ-formule te vinden die deze verzameling definieert. Een dergelijke constructie zou misschien ook gebruikt kunnen worden om van een bepaalde $\mathcal{L}_{NT}$-uitdrukking te bepalen of deze bijvoorbeeld een term is, of misschien zelfs te kunnen bepalen of er sprake is van een $\mathcal{L}_{NT}$-formule die bewijsbaar is in een bepaald axiomatisch systeem. Maar hoe is de constructie van recursieve verzamelingen van elementen uit $\mathbb{N}^k$ door te trekken naar recursieve verzamelingen met als elementen $\mathcal{L}_{NT}$-uitdrukking?

Het antwoord op deze vraag is het volgende: dit is mogelijk door de $\mathcal{L}_{NT}$-uitdrukkingen te coderen en zodoende aan elke uitdrukking een uniek natuurlijk getal te koppelen.

5.1 Codering van getallenrijen

In de codering zal het van groot belang worden aan een rij getallen $\langle k_1, k_2, \ldots, k_n \rangle$ een uniek getal toe te kunnen kennen.
Een getal c is een codering voor de rij getallen $\langle k_1, k_2, \ldots, k_n \rangle$ dan en slechts dan als $c = 2^{k_1} 3^{k_2} \ldots p_n^{k_n}$, waarbij p_n het n^e priemgetal is.

Is het nu mogelijk om, gegeven een bepaald getal, te bewijzen of dit getal al dan niet een codering van een rij getallen is? En een nog interessantere vraag: kun je, gegeven een code, terugkomen tot het oorspronkelijke rijtje waarvan dit de code is?

Om de eerste vraag met "ja" te kunnen beantwoorden, is het voldoende aan te tonen dat de verzameling van codenummers (voor getallenrijen) een recursieve verzameling is. En om dat aan te tonen is het vervolgens weer voldoende een Δ-formule te vinden die waar is (in het standaardmodel van de natuurlijke getallen waar we mee werken), wanneer het argument een codenummer is, en die niet waar is wanneer het argument dat niet is.

Zo'n Δ-formule bestaat en is de volgende:

$Codenumber(c)$ is:

$$Divides(SS0, c) \wedge (\forall z < c)(\forall y < z)$$
$$\big((Prime(z) \wedge Divides(z, c) \wedge Primepair(y, z)) \rightarrow Divides(y, c)\big)$$

De formules $Divides(x, y)$ ($\mathfrak{N} \models Divides(\overline{x}, \overline{y})$ desda x een deler is van y), $Prime(x)$ ($\mathfrak{N} \models Prime(\overline{x})$ desda x een priemgetal is) en $Primepair(y, z)$ ($\mathfrak{N} \models Primepair(\overline{y}, \overline{z})$ desda z het eerste priemgetal is dat na priemgetal y komt) zijn allen Δ-formules (zie [1]).

Deze formule zegt in woorden het volgende: c is deelbaar door 2 en als een bepaald priemgetal een deler is van c, dan zijn alle kleinere priemgetallen dat ook. Kortom: c codeert een rij getallen op de net besproken manier! En dus geldt er: $\mathfrak{N} \models Codenumber(\overline{c})$ desda c een rij getallen codeert.
Aangezien $Codenumber(c)$[2] een Δ-fomule is (x en y zijn begrensd door het getal wat je voor de variabele c invult), geldt er nu $N \vdash Codenumber(\overline{c})$ als c een rij codeert en $N \vdash \neg Codenumber(\overline{c})$ als c geen codenummer is dat een rij getallen codeert!

Je weet nu bijvoorbeeld dat:

$$N \vdash Codenumber(\overline{18}) \quad (18 = 2^1 3^2)$$

en

$$N \vdash \neg Codenumber(\overline{45}) \quad (2 \text{ is geen deler van } 45).$$

Het is dus mogelijk om gegeven een getal, te bewijzen of dit getal al dan niet een codenummer is. Rest nog de vraag of het ook mogelijk is van een gegeven codenummer terug te komen tot het oorspronkelijke rijtje getallen.
Als je van een gegeven codenummer c zou willen weten wat het 4^e getal was uit het oorspronkelijke rijtje, zul je dus te weten moeten komen wat de exponent is horende bij het 4^e priemgetal. Om in N uitspraken te kunnen doen over getallen uit het originele rijtje moet N dus de verschillende priemgetallen kunnen herkennen en localiseren (N moet gegeven een i en een x kunnen vaststellen of deze x het i^e priemgetal is).

Om te kijken of dit inderdaad mogelijk is, zal ik de volgende functie introduceren: $IthPrime(i, y)$, waarvan ik zou willen dat $\mathfrak{N} \models IthPrime(\overline{i}, \overline{y})$ desda $y = p_i$ (y is het i^e priemgetal). Als $IthPrime(i, y)$ bovendien een Δ-formule zou zijn, gold er bovendien dat in N te bewijzen is of een zeker getal het i^e priemgetal is. Zo'n Δ-formule $IthPrime(i, y)$ bestaat inderdaad, maar het vergt nog wat voorwerk voordat deze formule echt kan worden gemaakt.

Eerst zal ik een verzameling YARDSTICK (maatstaf) aanmaken, waarvan de elementen van de vorm $2^1 3^2 5^3 \ldots p_i^i$ zijn. Zo zijn 2, 18, 2250 en 5402250 bijvoorbeeld elementen van deze verzameling. Deze verzameling YARDSTICK is recursief en wordt gedefinieerd/gerepresenteerd door de volgende Δ-formule:

[2]Merk op dat de variabele c hier niet met een streepje ($\overline{c}$) wordt weergegeven, terwijl dat wel zo is in de uitdrukkingen $N \vdash Codenumber(\overline{c})$ en $\mathfrak{N} \models Codenumber(\overline{c})$. Dit omdat een uitspraak pas waar of bewijsbaar kan zijn als er een specifiek getal ($\overline{c}$) in is ingevuld, terwijl een formule die nog niet waar of onwaar is, afhangt van willekeurige variabelen (c).

$Yardstick(a)$ is:

$$Codenumber(a) \wedge Divides(SS0, a) \wedge \neg Divides(SSSS0, a) \wedge$$
$$(\forall y < a)(\forall z < a)(\forall k < a)$$
$$\Big(\big(Divides(z, a) \wedge Primepair(y, z)\big) \rightarrow \big(Divides(y^k, a) \leftrightarrow$$
$$Divides(z^{Sk}, a)\big)\Big)$$

Wat hier feitelijk staat is dat a deelbaar is door 2 en niet door 4, en dat als z een priemgetal en een deler van a is, het voorgaande priemgetal één keer minder in a past dan z. (Verder nog een opmerking over de notatie: het zou consequenter zijn om in plaats van y^k, Eyk te schrijven, maar de eerste notatie is korter en bovendien duidelijker.)

Met behulp van $Yardstick(a)$ is $IthPrime(i, y)$ nu op de volgende manier te maken:

$IthPrime(i, y)$ is:

$$Prime(y)$$
$$\wedge(\exists a \leq (y^i)^i)\big(Yardstick(a) \wedge Divides(y^i, a) \wedge \neg Divides(y^{Si}, a)\big)$$

Als er een a te vinden is, die deelbaar is door y^i en niet meer door y^{Si} en als je bovendien weet dat y een priemgetal is, weet je vervolgens dat y ook het i^e priemgetal moet zijn. Als y een priemgetal zou zijn, dat na het i^e priemgetal kwam, zou y een element uit YARDSTICK ofwel niet delen, ofwel y^n met $n > i$ en dus y^{Si} zou een element uit YARDSTICK delen. Als y een eerder priemgetal zou zijn zou er geen element uit YARDSTICK te vinden zijn, waarvan y^i een deler was. (Dit hangt er uiteraard sterk mee samen dat een priemgetal niet deelbaar is door een ander getal dan zichzelf en 1 en dus ook zeker niet deelbaar is door een ander priemgetal).
De begrenzing van de kwantor $(\exists a \leq (y^i)^i)$ verdient wellicht ook nog enige aandacht. Als y inderdaad het i^e priemgetal is, is een van de a's die zeker aan bovenstaande formule voldoet van de vorm $a = 2^1 3^2 \ldots y^i$. Maar deze a is dan dus zeker kleiner of gelijk aan $\underbrace{y^i y^i \ldots y^i}_{i\times} = (y^i)^i$.

Met behulp van $IthPrime$ kan er nu gekeken worden wat bijvoorbeeld het vierde getal was, van de oorspronkelijke getallenrij waar we nu alleen nog maar het codenummer van kennen. Het volstaat immers te kijken naar de exponent horende bij het 4^e priemgetal.

Hiervoor maken we de formule $IthElement(e, i, c)$, die waar is dan en slechts dan als c een codenummer is (een rijtje codeert) en als e het getal is wat in de oorspronkelijke rij op plaats i stond. Deze formule is natuurlijk ook weer een Δ-formule en zo kan dus ook in N **bewezen** worden of een bepaald getal,

gegeven een codenummer, in de oorspronkelijke getallenrij op plaats i stond.

$IthElement(e, i, c)$ is:

$$Codenumber(c) \wedge (\exists y < c)(IthPrime(i, y) \wedge Divides(y^e, c) \wedge \neg Divides(y^{Se}, e))$$

Ook is het nu makkelijk de lengte te bepalen van de oorspronkelijke getallenrij.

$Length(c, l)$ is:

$$Codenumber(c) \wedge (\exists y < c)\Big(IthPrime(l, y) \wedge Divides(y, c) \wedge (\forall z < c)\big(PrimePair(y, z) \rightarrow \neg Divides(z, c)\big)\Big)$$

Hier staat dat als het l^e priemgetal c deelt, maar het $(l+1)^e$ priemgetal dat niet meer doet, de lengte van de rij, gecodeerd door c, gegeven wordt door l.

Nu het duidelijk is hoe een getallenrij gecodeerd kan worden en hoe, gegeven een code, de bijbehorende rij teruggevonden kan worden, kan er nu begonnen worden strings bestaande uit $\mathcal{L}_{NT}$-symbolen te coderen om zo ook recursieve verzameling te kunnen maken, die iets zeggen over de coderingen van deze $\mathcal{L}_{NT}$-symbolen en daarmee dus ook over de symbolen (en formules en termen) zelf.

5.2 Codering van strings bestaande uit $\mathcal{L}_{NT}$-symbolen

Ik zal nu een functie $\ulcorner\ \urcorner$ introduceren die aan elke $\mathcal{L}_{NT}$-formule ϕ een uniek getal toekent: het **Gödelgetal**, weergegeven door $\ulcorner\phi\urcorner$.

Definitie 5.2.1. *De functie $\ulcorner\ \urcorner$, met als domein de verzameling van eindige strings bestaande uit $\mathcal{L}_{NT}$- symbolen en met codomein $\mathbb{N}$ is als volgt gedefinieerd:*

$$\ulcorner s \urcorner = \begin{cases} 2^1 3^{\ulcorner\alpha\urcorner} & \text{als } s \text{ gelijk is aan } (\neg\alpha), \text{ met } \alpha \text{ een } \mathcal{L}_{NT}\text{-formule} \\ 2^3 3^{\ulcorner\alpha\urcorner} 5^{\ulcorner\beta\urcorner} & \text{als } s \text{ gelijk is aan } (\alpha \vee \beta), \text{ met } \alpha \text{ en } \beta\ \mathcal{L}_{NT}\text{-formules} \\ 2^5 3^{\ulcorner v_i\urcorner} 5^{\ulcorner\alpha\urcorner} & \text{als } s \text{ gelijk is aan } (\forall v_i)(\alpha), \text{ met } \alpha \text{ een } \mathcal{L}_{NT}\text{-formule} \\ 2^7 3^{\ulcorner t_1\urcorner} 5^{\ulcorner t_2\urcorner} & \text{als } s \text{ gelijk is aan } = t_1 t_2, \text{ met } t_1 \text{ en } t_2 \text{ termen} \\ 2^9 & \text{als } s \text{ gelijk is aan } 0 \\ 2^{11} 3^{\ulcorner t\urcorner} & \text{als } s \text{ gelijk is aan } St, \text{ met } t \text{ een term} \\ 2^{13} 3^{\ulcorner t_1\urcorner} 5^{\ulcorner t_2\urcorner} & \text{als } s \text{ gelijk is aan } +t_1 t_2, \text{ met } t_1 \text{ en } t_2 \text{ termen} \\ 2^{15} 3^{\ulcorner t_1\urcorner} 5^{\ulcorner t_2\urcorner} & \text{als } s \text{ gelijk is aan } \cdot t_1 t_2, \text{ met } t_1 \text{ en } t_2 \text{ termen} \\ 2^{17} 3^{\ulcorner t_1\urcorner} 5^{\ulcorner t_2\urcorner} & \text{als } s \text{ gelijk is aan } E t_1 t_2, \text{ met } t_1 \text{ en } t_2 \text{ termen} \\ 2^{19} 3^{\ulcorner t_1\urcorner} 5^{\ulcorner t_2\urcorner} & \text{als } s \text{ gelijk is aan } < t_1 t_2, \text{ met } t_1 \text{ en } t_2 \text{ termen} \\ 2^{2i} & \text{als } s \text{ de variabele } v_i \text{ is} \\ 3 & \text{anders} \end{cases}$$

Vanaf nu is het dus mogelijk $\mathcal{L}_{NT}$-formules om te zetten naar natuurlijk getallen (en op deze manier recursieve verzamelingen van natuurlijke getallen te definiëren die feitelijk betrekking hebben op $\mathcal{L}_{NT}$-uitdrukkingen).

Een klein voorbeeld van een codering is het volgende:
neem ϕ gelijk aan $\neg = 0S0$. De codering wordt nu:
$\ulcorner\phi\urcorner$ is $2^1 3^{\ulcorner=0S0\urcorner}$
Nu moet dus de codering van =0S0 gevonden worden: $\ulcorner= 0S0\urcorner$ is $2^7 3^{\ulcorner 0\urcorner} 5^{\ulcorner S0\urcorner}$.
De coderingen van 0 en S0 worden vervolgens gegeven door: $\ulcorner 0\urcorner$ is 2^9 en $\ulcorner S0\urcorner$ is $2^{11}3^{\ulcorner 0\urcorner}$ is $2^{11}3^{2^9}$.
Samengevoegd geeft dit nu:
$\ulcorner\neg = 0S0\urcorner$ is $2^1 3^{2^7 3^{2^9} 5^{2^{11} 3^{2^9}}}$.

Het is direct duidelijk dat zelfs het Gödelgetal van een erg simpele formule al ontzettend groot wordt! De getallen die eruit komen zijn echter op zich van geen enkel belang. Het enige wat van belang is, is dat de Gödelgetallen terug te voeren zijn tot de oorspronkelijke strings van symbolen en dat er op deze manier wat gezegd kan worden over deze strings.

6 Gödelgetallen van termen en formules

Nu het mogelijk is om strings van $\mathcal{L}_{NT}$-symbolen om te zetten tot natuurlijke getallen is natuurlijk de vraag: is het ook mogelijk om, gegeven een Gödelgetal, te kijken of de bijbehorende string een term of een formule is? (Als dit mogelijk is kun je je vervolgens zelfs af gaan vragen of de betreffende formule afleidbaar is in het axiomatisch syteem.)

Graag zou je een Δ-formule $Term(x)$ (resp. $Formula(x)$) hebben, zodat voor elk natuurlijk getal a geldt dat $\mathfrak{N} \models Term(\overline{a})$ (resp. $\mathfrak{N} \models Formula(\overline{a})$) dan en slechts dan als a het Gödelgetal is, dat hoort bij een term (resp. formule). Omdat het hier bovendien een Δ-formule betreft is het dan tevens mogelijk om in N te **bewijzen** of een getal a al dan niet een Gödelgetal is horende bij een term (resp. formule).

Dergelijke Δ-formules bestaan inderdaad en ik zal de afleiding van de formule $Term(x)$ geven. De afleiding van $Formula(x)$ gaat op eenzelfde manier, maar zal ik verder niet uitwerken.

Om nog even te herhalen wat een term is: Een **term** t van $\mathcal{L}_{NT}$ is ofwel een variabele, ofwel een constante (0), ofwel t wordt gegeven door ft_1 of ft_1t_2 waarbij f een unair (S) of binair ($+, \cdot, E$) functiesymbool is en elke t_i een term van $\mathcal{L}_{NT}$ is.

Om variabelen te kunnen herkennen en van een gegeven Gödelgetal te kunnen bewijzen of dit al dan niet een variabele is, zal ik allereerst de verzameling VARIABLE introduceren:
VARIABLE $= \{a \in \mathbb{N} | a = \ulcorner v \urcorner$ voor een variabele $v\}$.
Wanneer deze verzameling recursief is, geldt weer dat er bewezen kan worden of een Gödelgetal een variabele codeert en om aan te tonen dat deze verzameling recursief is, is het wederom weer voldoende een Δ-formule te vinden die de verzameling VARIABLE definieert (en daarmee dus representeert). Zo'n formule is de volgende:

$Variable(x)$ is:

$$(\exists y < x)(Even(y) \wedge 0 < y \wedge x = 2^y)$$

Het is eenvoudig in te zien dat $\mathfrak{N} \models (\overline{a})$ dan en slechts dan als a een element is van de verzameling VARIABLE (in het achterhoofd houdend dat een variabele van de vorm 2^{2i} is).

Het idee is nu om een term t in subtermen u (u is een substring van t en u is bovendien een $\mathcal{L}_{NT}$-term) op te splitsen en vervolgens te kijken of t op de juiste manier opgebouwd is (of de term slechts bestaat uit constanten en variabelen waarop vervolgens weer functiesymbolen toegepast kunnen zijn). Om dit idee wat concreter te maken, zal ik een voorbeeld geven.

Beschouw de term t gegeven door $+0Sv_1$. De rij van subtermen waaruit t is opgebouwd wordt gegeven door: $\langle v_1, Sv_1, 0, +0Sv_1\rangle$ (waarbij dus geldt dat een volgend element uit de rij ofwel een variabele of constante is, ofwel is gemaakt door een functiesymbool op één of meerdere eerdere elementen toe te passen).

Deze rij kan vervolgens door één natuurlijk getal gecodeerd worden, door alle subtermen te coderen en de rij vervolgens te coderen zoals in hoofdstuk 5.1 wordt besproken:
De rij met Gödelgetallen wordt gegeven door: $\langle 2^2, 2^{11}3^{2^2}, 2^9, 2^{13}3^{2^9}5^{(2^{11}3^{2^2})}\rangle$,
het getal dat deze rij codeert wordt nu: $c = 2^{(2^2)}3^{(2^{11}3^{2^2})}5^{(2^9)}, 7^{(2^{13}3^{2^9}5^{(2^{11}3^{2^2})})}$.

Om te weten of a het Gödelgetal van een term is, moet je dus nagaan of er een codenummer c bestaat, horende bij een "constructierij" van een term, waarvan a het laatste getal in de rij is.

Om het begrip "constructierij van een term"nog wat te verduidelijken zal ik de volgende definitie hanteren:

Definitie 6.0.2. *Een eindige rij van $\mathcal{L}_{NT}$-termen $\langle t_1, t_2, \ldots, t_l\rangle$ heet een **term constructierij voor** t_l als, voor elke i met $1 \leq i \leq l$, t_i ofwel een variabele, ofwel de constante 0 is, of gegeven wordt door $t_j, St_j, +t_jt_k, \cdot t_jt_k$ of Et_jt_k, waarbij $j < i$ en $k < i$.*

Mijn volgende doel is te bewijzen dat de verzameling TERMCONSTRUCTION-SEQUENCE = $\{(c, a)|$ c is het codenummer van de term constructierij voor de term met Gödelgetal $a\}$ recursief is.
Het volstaat weer om een Δ-formule te vinden die de verzameling definieert, en zo'n formule is de volgende:

$TermConstructionSequence(c, a)$ is:

$$
\begin{gathered}
Codenumber(c) \wedge \\
(\exists l < c)\Big(Length(c, l) \wedge IthElement(a, l, c) \wedge \\
(\forall e < c)(\forall i \leq l)\Big(IthElement(e, i, c) \rightarrow \\
Variable(e) \vee e = \overline{2}^{\overline{9}} \vee \\
(\exists j < i)(\exists k < i)(\exists e_j < c)(\exists e_k < c) \\
\big(IthElement(e_j, j, c) \wedge IthElement(e_k, k, c) \wedge \\
(e = e_j \vee e = \overline{2}^{\overline{11}} \cdot \overline{3}^{e_j} \vee \\
e = \overline{2}^{\overline{13}} \cdot \overline{3}^{e_j} \cdot \overline{5}^{e_k} \vee \\
e = \overline{2}^{\overline{15}} \cdot \overline{3}^{e_j} \cdot \overline{5}^{e_k} \vee e = \overline{2}^{\overline{17}} \cdot \overline{3}^{e_j} \cdot \overline{5}^{e_k}))\Big)\Big)
\end{gathered}
$$

Alles wat hier staat is dat (c, a) een element is uit TERMCONSTRUCTION-SEQUENCE dan en slechts dan als c een codenummer is met lengte l, als a het laatste getal in de door c gecodeerde rij is, en dat als e in de oorspronkelijke rij op positie i stond, e ofwel het Gödelgetal horende bij een variabele of constante 0 is, ofwel e een herhaling is van een al eerder voorgekomen Gödelgetal, of dat e het Gödelgetal is dat is ontstaan door S,+,$\cdot$ of E toe te passen op eerdere getallen in de door c gecodeerde rij. Aangezien alle kwantoren bovendien begrensd zijn, is dit inderdaad een Δ-formule die de verzameling TERMCONSTRUCTION-SEQUENCE definieert en zodoende is deze verzameling recursief!

Het ligt nu voor de hand om als formule voor $Term(a)$ te kiezen voor: $(\exists c)TermConstructionSequence(c, a)$. Het enige probleem is nog dat de c in deze formule niet begrensd is, en bovenstaande formule dus geen Δ-formule is. Er moet een bovengrens voor c gevonden worden. Aan de hand van enkele lemma's, waarvan ik er slechts één zal bewijzen, kan een dergelijke bovengrens gevonden worden.

Lemma 6.0.1. *Als t een $\mathcal{L}_{NT}$-term is en $\ulcorner t \urcorner = a$, dan is het aantal symbolen waaruit t bestaat kleiner dan a.*

Dit bewijs gaat met behulp van inductie naar de complexiteit van de term t. Voor de kleinst mogelijke termen, bestaande uit 1 symbool (de constante 0 of een variabele) is het direct duidelijk, wanneer je kijkt naar de daarbij horende Gödelgetallen. En met behulp van inductie kan het lemma dan ook voor complexere termen bewezen worden. (Intuïtief is het duidelijk dat dit lemma waar is. Neem bijvoorbeeld t is S0. Dan heeft t twee symbolen, terwijl $\ulcorner t \urcorner = a = 2^{11}3^{2^9}$, een getal wat duidelijk groter is dan 2.)

Lemma 6.0.2. *Als t een term is, is de lengte van de kortste constructierij van t kleiner of gelijk aan het aantal symbolen in t.*

Ook dit bewijs gaat met inductie naar de complexiteit van t. (In het achterhoofd houdende dat elk symbool uit t maar 1 keer toegevoegd hoeft te worden aan de constructierij, is ook dit lemma weer erg aannemelijk.)

Een combinatie van **lemma 6.0.1** en **6.0.2** geeft nu dat als a het Gödelgetal is van een term, er een constructierij van die term bestaat waarvan de lengte kleiner dan a is.

Lemma 6.0.3. *Stel dat t een $\mathcal{L}_{NT}$-term is en dat u een subterm van t is. Dan geldt $\ulcorner u \urcorner < \ulcorner t \urcorner$.*

(Dit hangt volledig samen met de Gödelgetallen. Het Gödelgetal van u zal ook in de codering van t terugkomen, maar dan als exponent in een groter getal (als $u \neq t$).)

Lemma 6.0.4. *Als a een natuurlijk getal groter of gelijk aan 1 is, geldt er dat $p_a \leq 2^{a^a}$, met p_a het a^e priemgetal.*

Het bewijs van dit laatste lemma is als volgt:

Neem $a = 1$: $p_1 = 2 \leq 2^{1^1}$. Voor $a = 1$ klopt het lemma: de Inductie Veronderstelling luidt: $p_n \leq 2^{n^n}$

Vervolgens zal ik gebruik maken van het feit dat p_{n+1} kleiner of gelijk is aan het kleinste priemgetal dat het getal $p_1 p_2 \dots p_n - 1$ deelt. Dit getal wordt immers niet gedeeld door p_1 tot en met p_n (p_i met $i \leq n$ is een deler van $p_1 \dots p_n$ en geen deler van 1, dus kan ook nooit een deler van $p_1 p_2 \dots p_n - 1$ zijn) en dus is de kleinste priemfactor die dit getal deelt, zeker groter dan p_n en dus ofwel gelijk aan p_{n+1} ofwel groter.

Noem de kleinste priemfactor die $p_1 p_2 \dots p_n - 1$ deelt, q. Nu geldt er:

$p_{n+1} \leq q \leq p_1 p_2 \dots p_n - 1 < p_1 p_2 \dots p_n \leq 2 \cdot 2^{2^2} \cdot 2^{3^3} \dots 2^{n^n} \leq 2^{1+2^2+3^3+\dots+n^n} \leq 2^{n \cdot n^n} = 2^{n^{(n+1)}} \leq 2^{(n+1)^{(n+1)}}$ $\square$

Nu kan eindelijk een bovengrens gegeven worden voor de kortste constructierij c van een term t met Gödelgetal $\ulcorner t \urcorner = a$.
Zo'n contruction sequence ziet er als volgt uit:
$\langle t_1, t_2, \dots, t_k = t \rangle$ waarbij $k \leq a$ (**lemma 6.0.1** en **6.0.2** gecombineerd) en waarbij elke t_i een subterm van t is.

De code voor deze constructierij wordt nu:
$c = 2^{\ulcorner t_1 \urcorner} 3^{\ulcorner t_2 \urcorner} \dots p_k^{\ulcorner t \urcorner}$
$\leq 2^a 3^a \dots p_k^a$ (**lemma 6.0.3**)
$\leq \underbrace{p_k^a p_k^a \dots p_k^a}_{k \text{ termen}}$
$\leq \underbrace{p_a^a p_a^a \dots p_a^a}_{a \text{ termen}}$ ($k \leq a$)
$\leq \left((2^{a^a})^a \right)^a$
$= (2^{a^a})^{a^2}$,
en dit geeft dan de gewenste bovengrens!

De Δ-formule $Term(a)$ die waar is dan en slechts dan als a het Gödelgetal van een term is, wordt nu gegeven door:

$Term(a)$ is:

$$\left(\exists c < \left(\overline{2}^{a^a} \right)^{a^{\overline{2}}} \right) TermConstructionSequence(c, a)$$

De verzameling TERM=$\{a \in \mathbb{N} |\ a$ is het Gödelgetal van een $\mathcal{L}_{NT}$-term$\}$ is dus een recursieve verzameling en dus is het mogelijk met behulp van de axioma's N voor elk getal a ofwel $Term(\overline{a})$ ofwel $\neg Term(\overline{a})$ te bewijzen!

Op een dergelijke manier (ook weer aan de hand van een constructierij, maar dan van een "formule constructierij") kan ook een Δ-formule $Formula(f)$ gevonden worden (zie [1]) die waar is dan en slechts dan als f het Gödelgetal van een formule is. En zo geldt dan dus ook weer dat de verzameling FORMULA=$\{a \in \mathbb{N} | a$ is het Gödelgetal van een $\mathcal{L}_{NT}$-formule$\}$ een recursieve verzameling is en dus dat voor elk getal f ofwel $Formula(\overline{f})$ ofwel $\neg Formula(\overline{f})$ te bewijzen is!

Ik zal de afleiding van deze formule $Formula(f)$ verder niet geven, maar er in het vervolg wel vanuit gaan dat deze bestaat.

7 De functies Num en Sub

In hoofdstuk 4 heb ik geprobeerd heel kort het idee achter het uiteindelijke bewijs weer te geven. Eén van de voorwaarden om het bewijs te kunnen maken was de volgende:

- Een formule ϕ moet kunnen refereren aan haar eigen bewijsbaarheid.

Om aan deze voorwaarde te kunnen voldoen zal het nodig blijken te zijn het Gödelgetal van een formule te substitueren in een andere formule. Om weer zinnige uitspraken te kunnen doen of een formule daadwerkelijk is ontstaan uit een andere formule waarop een zekere substitie is uitgevoerd, zullen er weer Δ-formules nodig zijn. Bovendien is er nog een functie Num(a)=$\ulcorner\overline{a}\urcorner$ nodig die het getal a afbeeldt op het bijbehorende Gödelgetal $\ulcorner\overline{a}\urcorner$.

Om een voorbeeld van de werking van deze functie te geven, beschouw ik het getal 2. Aangezien 2 niet bestaat in de taal, wordt 2 altijd weergegeven door $\overline{2}$ wat dan weer de verkorte schrijfwijze is voor $SS0$. Verder geldt dat $SS0$ op zichzelf een $\mathcal{L}_{NT}$-term is en dus een Gödelgetal heeft, zijnde:
$\ulcorner SS0\urcorner = 2^{11}3^{\ulcorner S0\urcorner} = 2^{11}3^{2^{11}3^{\ulcorner 0\urcorner}} = 2^{11}3^{2^{11}3^{2^9}}$

Er geldt nu dus dat Num(2) gelijk is aan $2^{11}3^{2^{11}3^{2^9}}$. Om nu een Δ-formule te hebben die de functie Num(a) representeert in onze theorie N, neem je de formule $Num(a, y)$ die waar is dan en slechts dan als y gelijk is aan $\ulcorner\overline{a}\urcorner$. Er kan weer bewezen worden dat deze formule $Num(a, y)$ een Δ-formule is (zie [1]), maar ik zal de afleiding slechts in grote lijnen geven.

Allereerst bestaat er ook nu weer een "constructierij", maar deze keer is dit een constructierij voor een getal. De constructierij voor $\overline{2} = SSO$ is bijvoorbeeld $\langle 0, S0, SS0\rangle$, en de rij van de bijbehorende Gödelgetallen wordt dan: $\langle 2^9, 2^{11}3^{2^9}, 2^{11}3^{2^{11}3^{2^9}}\rangle$, waarvan het codenummer c dan $2^{(2^9)}3^{(2^{11}3^{2^9})}5^{(2^{11}3^{2^{11}3^{2^9}})}$ wordt.
Merk op dat de lengte van de constructierij horende bij het Gödelgetal van $\overline{a}$ altijd gelijk zal zijn aan $a + 1$.

Nu kan er een formule $NumConstructionSequence(c, a, y)$ gedefinieerd worden waarvoor geldt dat $\mathfrak{N} \models NumConstructionSequence(\overline{c}, \overline{a}, \overline{y})$ dan en slechts dan als c het codenummer is voor een constructierij van lengte $a + 1$, waarvan y het laatste element is en y vervolgens weer gelijk is aan $\ulcorner\overline{a}\urcorner$.

De formule $Num(a, y)$ kan dan gedefinieerd worden als:

$$(\exists c)NumConstructionSequence(c, a, y).$$

Om deze formule tot een Δ-formule te maken moet er weer voor gezorgd worden dat de kwantor $\exists$ begrensd is. Dit is mogelijk, maar de details laat ik achterwege. In het vervolg mag er dus vanuit gegaan worden dat er een Δ-formule

$Num(a, y)$ bestaat die waar is dan en slechts dan als y gelijk is aan $\ulcorner\overline{a}\urcorner$.

Aangezien deze formule de functie Num representeert geldt er nu:

$$N \vdash (\forall y)\big(Num(\overline{a}, y) \leftrightarrow y = \overline{\mathrm{Num}(a)}\big)$$

en dus

$$N \vdash \big(Num(\overline{a}, y) \leftrightarrow y = \overline{\mathrm{Num}(a)}\big).$$

Nu kom ik bij de substitutieformules.

Wanneer je een term hebt, waarin een variabele voorkomt, zou het zo kunnen zijn dat je deze variabele wilt vervangen door bijvoorbeeld een getal, of door een andere term (NB: een getal is ook een term). De schrijfwijze voor een dergelijke substitutie is al volgt: wanneer je in een term u, de daarin voorkomende variabele x vervangt door een term t, wordt dit kort weergegeven als u_t^x.

De regels wat betreft substitutie van een term t voor een variabele x binnen een term u zijn (voor de hand liggend en) als volgt:

1. Als u een variabele is, die niet gelijk is aan x, is u_t^x gelijk aan u.
2. Als u gelijk is aan x, is u_t^x gelijk aan t.
3. Als u een constante is, is u_t^x gelijk aan u.
4. Als u gelijk is aan fu_1u_2 (waarbij f weer een functiesymbool is en u_1 en u_2 termen zijn), dan is u_t^x gelijk aan $f(u_1)_t^x(u_2)_t^x$ (idem voor unair functiesymbool S)

Het doel is om een een Δ-formule $TermSub(\ulcorner u\urcorner, \ulcorner x\urcorner, \ulcorner t\urcorner, y)$ te creëren die waar is dan en slechts dan als y het Gödelgetal is van u_t^x, waarbij wordt aangenomen dat u en t termen zijn en x een variabele.

Ik zal de afleiding van deze formule niet geven, alleen met behulp van een voorbeeld het idee schetsen:
Stel u is de term gegeven door $+ \cdot 0S0x$. Een constructierij van deze term zou bijvoorbeeld de volgende kunnen zijn: $\langle 0, x, S0, \cdot 0S0, + \cdot 0S0x\rangle$.
Stel je voor dat je x wilt vervangen door de term t gegeven door $SS0$. Dan wordt u_t^x $+ \cdot 0S0SS0$ en wordt de termconstructierij $\langle 0, SS0, S0, \cdot 0S0, + \cdot 0S0SS0\rangle$, waarin simpelweg alles x'en zijn vervangen door t. Deze nieuwe rij is helaas zelf geen constructierij meer aangezien de tweede term erin niet goed afgeleid is. Een rij die wél een constructierij is voor $+ \cdot 0S0SS0$ is de volgende:
$\langle 0, S0, SS0, 0, SS0, S0, \cdot 0S0, + \cdot 0S0SS0\rangle$.
Deze constructierij is gemaakt door de constructierij van SS0 (oftwel t) te plaatsen voor de rij, verkregen door alle x' en door t' s vervangen in de oorspronkelijke term constructierij van u.

Terug naar het algemene geval: Stel je voor dat er een termconstructierij voor u en een termconstructierij voor t te vinden is. Vervang nu in de constructierij voor u alle x'n door een t en voeg vervolgens de constructierij voor t samen met deze rij (de constructierij voor t is het begin van de nieuwe rij). Wanneer deze nieuwe rij nu ook weer een term constructierij is, is dit de termconstructierij voor u_t^x en is het dus mogelijk x door t te vervangen in de oude term u om op die manier een nieuwe term te maken.

Het blijkt mogelijk te zijn een Δ-formule $TermReplace(c, \ulcorner u \urcorner, d, \ulcorner x \urcorner, \ulcorner t \urcorner)$ te vinden (zie [1]) die waar is dan en slechts dan als c de constructierij voor u codeert en d het codenummer is dat hoort bij de rij, gekregen door in de constructierij voor u alle x'n te vervangen door t.
Ook is er een Δ-formule $Append(b, d, a)$ te maken (zie eveneens [1]), die waar is als a het codenummer van de rij is, die is ontstaan door de rijen met codenummer b en d aan elkaar te plakken.

Wanneer je nu de formule:

$TermSub(\ulcorner u \urcorner, \ulcorner x \urcorner, \ulcorner t \urcorner, y)$ is:

$$(\exists a)(\exists b)(\exists d)(\exists c)\big(TermConstructionSequence(c, \ulcorner u \urcorner) \wedge TermConstructionSequence(b, \ulcorner t \urcorner) \wedge TermReplace(c, \ulcorner u \urcorner, d, \ulcorner x \urcorner, \ulcorner t \urcorner) \wedge Append(b, d, a) \wedge TermConstructionSequence(a, y)\big)$$

definieert, is deze formule precies waar als y het Gödelgetal van u_t^x is.

Het enige wat nog moet gebeuren is grenzen vinden voor de kwantoren, om ervoor te zorgen dat $Termsub(\ulcorner u \urcorner, \ulcorner x \urcorner, \ulcorner t \urcorner, y)$ een Δ-formule is. Alles wat ik hierover zal zeggen is dat deze grenzen bestaan (zie [1]).

In de formule $TermSub(\ulcorner u \urcorner, \ulcorner x \urcorner, \ulcorner t \urcorner, y)$ gaat het om de substitutie van een term voor een variabele, binnen een **term**. Het is vooral belangrijk een dergelijke substitutie uit te kunnen voeren binnen een **formule**.

Bij substitutie van een term t voor een variabele x binnen een formule ϕ gelden de volgende regels:

1. Als ϕ gelijk is aan $= u_1 u_2$, dan is ϕ_t^x gelijk aan $= (u_1)_t^x (u_2)_t^x$.
2. Als ϕ gelijk is aan $< u_1 u_2$, dan is ϕ_t^x gelijk aan $< (u_1)_t^x (u_2)_t^x$.
3. Als ϕ gelijk is aan $\neg(\alpha)$, dan is ϕ_t^x gelijk aan $\neg(\alpha_t^x)$.
4. Als ϕ gelijk is aan $(\alpha \vee \beta)$, dan is ϕ_t^x gelijk aan $(\alpha_t^x \vee \beta_t^x)$.

5. Als ϕ gelijk is aan $(\forall y)(\alpha)$, dan geldt

$$\phi_t^x = \begin{cases} \phi & \text{als } x \text{ gelijk is aan } y \\ (\forall y)(\alpha_t^x) & \text{anders.} \end{cases}$$

Nu kan de formule $Sub(f, \ulcorner x \urcorner, \ulcorner t \urcorner, y)$ gedefinieerd worden, die waar is dan en slechts dan als y het Gödelgetal is van de formule ϕ_t^x die is ontstaan door in de formule ϕ (met Gödelgetal f) de variabele x door een term t te vervangen. Ook van deze formule kan weer worden bewezen dat het een Δ-formule is. (Analoog aan de afleiding van $TermSub$.)

Net als het verband tussen de formule $Num(a, y)$ en de functie Num(a) ($Num(a, y)$ is waar dan en slechts dan als geldt dat Num(a)=y), is er ook een functie Sub($\ulcorner \phi \urcorner$,$\ulcorner x \urcorner$,$\ulcorner t \urcorner$)=$\ulcorner \phi_t^x \urcorner$ die, gegeven de Gödelgetallen van een formule, een variabele en een term, het Gödelgetal van de formule geeft waarin de variabele door de term is vervangen. (Kortom: $Sub(f, \ulcorner x \urcorner, \ulcorner t \urcorner, y)$ is waar dan en slechts dan als Sub(f,$\ulcorner x \urcorner$,$\ulcorner t \urcorner$)=y) En aangezien ook Sub een Δ-formule is, geldt er nu dat de formule $Sub(f, \ulcorner x \urcorner, \ulcorner t \urcorner, y)$ de functie Sub(f,$\ulcorner x \urcorner$,$\ulcorner t \urcorner$) representeert en geldt dus:

$$N \vdash \left(Sub(\overline{f}, \overline{\ulcorner x \urcorner}, \overline{\ulcorner t \urcorner}, y) \leftrightarrow y = \overline{\text{Sub}(f, \ulcorner x \urcorner, \ulcorner t \urcorner)} \right)$$

Nu is dus zowel de functie Num(a) als de functie Sub(f,$\ulcorner x \urcorner$,$\ulcorner t \urcorner$) gerepresenteerd door een Δ-formule.

Er is nog een klein detail wat ik tot nu toe heb genegeerd. In een term kun je een variabele altijd vervangen door een term. De term blijft gewoon een term en aangezien een term niet "waar" of "niet waar" kan zijn, kan daar ook niks mee misgaan. Voor een formule ligt dit anders. Aangezien een gesloten formule (een zin) een waarheidswaarde heeft, wil je graag dat de formule, na de substitutie, deze waarheidswaarde heeft behouden. Wanneer je de substitutie uitvoert zoals hierboven beschreven, hoeft aan deze voorwaarde niet voldaan te worden. Het zou namelijk kunnen gebeuren dat je een variabele vervangt door een term waarin ook weer een variabele voorkomt, zeg y, en dat y in de oorspronkelijke formule gebonden is door een kwantor. Vandaar dat ik het begrip **substitueerbaar** in zal voeren.

Neem aan dat ϕ een $\mathcal{L}_{NT}$-formule is, t een term en x een variabele. Dan heet t substitueerbaar voor x in ϕ, als:

1. ϕ is atomair, of
2. ϕ is gelijk aan $\neg(\alpha)$ en t is substitueerbaar voor x in α, of
3. ϕ is gelijk aan $(\alpha \vee \beta)$ en t is substitueerbaar voor x in zowel α als β, of

4. ϕ is gelijk aan $(\forall y)(\alpha)$ en ofwel

    a x is gebonden in ϕ, ofwel

    b y komt niet voor in t en t is substitueerbaar voor x in α.

De formule ϕ_t^x is dus gedefinieerd of t nu substitueerbaar is voor x of niet, maar wanneer je erbij eist dat t substitueerbaar is voor x weet je dat ϕ en ϕ_t^x dezelfde waarheidswaarde hebben in $\mathfrak{N}$.
Gelukkig bestaat er een Δ-formule $Substitutable(\ulcorner t \urcorner, \ulcorner x \urcorner, f)$ (zie [1]), die waar is dan en slechts dan als t een term is die substitueerbaar is voor de variabele x in de formule ϕ (met Gödelgetal f).

8 Bewijsbaarheid

In hoofdstuk 4 heb ik het idee van het bewijs geschetst, waarbij ik de volgende eis formuleerde:

- De bewijsbaarheid van formules moet in een $\mathcal{L}_{NT}$-formule kunnen worden uitgedrukt.

In dit hoofdstuk zal ik eerst precies maken wat "de bewijsbaarheidheid van een formule" inhoudt en vervolgens laten zien hoe dit kan worden uitgedrukt in een $\mathcal{L}_{NT}$-formule.

Per definitie is een $\mathcal{L}$-formule ϕ bewijsbaar in een axiomatisch systeem Σ, als er een eindige rij $\langle \phi_1, \phi_2, \ldots, \phi_n \rangle$ (een afleiding) van $\mathcal{L}$-formules bestaat waarbij $\phi_n = \phi$, zodanig dat voor iedere i, $1 \leq i \leq n$ het volgende geldt:

1. ϕ_i is een logisch axioma, of
2. $\phi_i \in \Sigma$ (ϕ_i is een (niet-logisch) axioma), of
3. ϕ_i is ontstaan door één van de afleidingsregels toe te passen op één of meerdere van de eerdere ϕ_j's.

Bovenstaande definitie is van toepassing op onze taal en ons axiomatisch systeem als we de taal $\mathcal{L}$ vervangen door $\mathcal{L}_{NT}$ en de theorie Σ door N.

Het enige wat nog moet worden toegelicht zijn de logische axioma's en de afleidingsregels.

De **logische axioma's** zijn de volgende:

(E1) $x = x$ voor elke variabele x

(E2) $\big((x_1 = y_1) \wedge (x_2 = y_2)\big) \rightarrow (f(x_1, x_2) = f(y_1, y_2))$

(E3) $\big((x_1 = y_1) \wedge (x_2 = y_2)\big) \rightarrow (r(x_1, x_2) \rightarrow r(y_1, y_2))$

(Q1) $(\forall x \phi) \rightarrow \phi^x_t$, als t subsitueerbaar is voor x in ϕ

(Q2) $\phi^x_t \rightarrow (\exists x \phi)$, als t substitueerbaar is voor x in ϕ

De eerste 3 axioma's zijn de "gelijkheids axioma's" ("equality axioms") en de laatste 2 zijn de "kwantor axioma's" ("quantifier axioms").

Nu kom ik bij de **afleidingsregels**. Binnen de **propositielogica** bestaat de volgende definitie:

Definitie 8.0.3. *Als $\Gamma = \{\gamma_1, \gamma_2, \ldots, \gamma_n\}$ een niet lege, eindige verzameling van propositieformules is, en ϕ is ook een propositieformule, dan is ϕ een propositioneel gevolg van (propositional consequence of) Γ als geldt dat elke waarheidstoekenning die alle formules in Γ waarmaakt, ook de formule ϕ waarmaakt.*

Merk op dat ϕ een propositioneel gevolg is van Γ dan en slechts dan als $(\gamma_1 \wedge \gamma_2 \wedge \cdots \wedge \gamma_n) \rightarrow \phi$ een tautologie is. Waarbij met een tautologie wordt bedoeld dat de formule waar is, ongeacht welke waarheidswaarden worden meegegeven aan de in de formules voorkomende propositievariabelen. Dit zal ik hieronder nog verder uitleggen.

De propositielogica verschilt behoorlijk van de eerste-orde logica. Binnen de propositielogica worden namelijk geen functie- en relatiesymbolen gebruikt, er wordt niet met kwantoren gewerkt en de enige constanten zijn "0" en "1", waarbij "0" correspondeert met "niet waar" en "1" met "waar". Wanneer weer dezelfde adequate verzameling connectieven als in hoofdstuk 3.2 wordt gebruikt $(\neg, \vee, \wedge)$ en wanneer we aannemen dat ϕ een propositieformule is dan en slechts dan als ϕ ofwel een propositievariabele is (A,B,C,...), ofwel van de vorm "$\neg\alpha$", "$\alpha \vee \beta$" of "$\alpha \wedge \beta$" is waarbij α en β propositieformules zijn, is het eenvoudig om te zien of een propositieformule waar of niet waar is. Het werkt als volgt: Aan elke propositievariabele kan ofwel de waarde "waar" ofwel de waarde "niet waar" worden meegegeven. Dit is ook te zien als een functie v met

$$v : \text{propositievariabelen} \rightarrow \{0, 1\}.$$

Een functie $\overline{v}$ die aan elke propositieformule een waarheidswaarde toekent ziet er nu als volgt uit:

$$\overline{v}(\phi) = \begin{cases} v(\phi) & \text{als } \phi \text{ een propositievariabele is} \\ 0 & \text{als } \phi \text{ gelijk is aan } (\neg\alpha) \text{ en } \overline{v}(\alpha) = 1 \\ 0 & \text{als } \phi \text{ gelijk is aan } (\alpha \vee \beta) \text{ en } \overline{v}(\alpha) = \overline{v}(\beta) = 0 \\ 0 & \text{als } \phi \text{ gelijk is aan } (\alpha \wedge \beta) \text{ en } \overline{v}(\alpha) = 0 \text{ en/of } \overline{v}(\beta) = 0 \\ 1 & \text{anders} \end{cases}$$

Een propositieformule ϕ is nu een tautologie dan en slechts dan als $\overline{v}(\phi) = 1$ voor elke waarheidstoekenning v.

Om nu terug te komen op het propositionele gevolg (PC-regel), als je al hebt bewezen dat γ_1 tot en met γ_n waar zijn en je weet bovendien dat $(\gamma_1 \wedge \gamma_2 \wedge \cdots \wedge \gamma_n) \rightarrow \phi$ een tautologie is, mag je hieruit concluderen dat ϕ bewijsbaar is.

Binnen de eerste-orde logica zou ook een dergelijke afleidingsregel gebruikt kunnen worden. Neem aan dat γ_1 tot en met γ_n bewijsbare $\mathcal{L}_{NT}$-formules zijn en dat de $\mathcal{L}_{NT}$-formule $(\gamma_1 \wedge \cdots \wedge \gamma_n) \rightarrow \phi$ waar is in de gekozen structuur. Hieruit zou je dan willen concluderen dat $N \vdash \phi$.

Het is helaas onmogelijk een dergelijke afleidingsregel in een Δ-formule te vangen, en vandaar dat we nu ook binnen de eerste orde logica terug zullen grijpen op het **propositionele gevolg** (ipv een "eerste-orde gevolg"). Eerst zullen de eerste-orde formules omgeschreven worden tot hun "propositionele equivalenten" en vervolgens zal dan van deze propositieformules bepaald worden of er sprake is van een propositioneel gevolg. In feite wordt de eerste-orde logica dus

teruggebracht tot de simpelere propositielogica.

Met behulp van het volgende algoritme kun je bij een gegeven $\mathcal{L}_{NT}$-formule β de corresponderende β_P vinden waarbij β_P een propositieformule is:

1. Vervang alle deelformules van de vorm $\forall x\alpha$, die niet begrensd zijn door een andere kwantor, door een propositievariabele. Dit moet op een zodanige manier gebeuren dat wanneer $\forall y Q(y, c)$ op meerdere plaatsen in β voorkomt, het in al die gevallen door dezelfde letter wordt vervangen. (NB: merk op dat $\exists x\alpha$, altijd omgeschreven kan worden in een uitdrukking waar geen $\exists$-kwantoren, maar nog slechts $\forall$-kwantoren in voorkomen.)

2. Vervang alle atomaire formules die nog over zijn op een systematische manier door nieuwe propositievariabelen (dezelfde formules moeten ook hier weer vervangen worden door dezelfde letters).

3. Nu is β omgezet in propositieformule β_P.

Als β_P nu een tautologie blijkt te zijn, weet je dat β waar is (en als β niet waar is, zal β_P geen tautologie zijn). Andersom geldt dit niet. Het is mogelijk dat β waar is en β_P geen tautologie is (wat maar weer eens laat zien dat de propositielogica minder krachtig is dan de eerste-orde logica).

Dit leidt tot de volgende definitie:

Definitie 8.0.4. *Neem aan dat Γ een eindige verzameling van $\mathcal{L}_{NT}$-formules is en dat ϕ ook een $\mathcal{L}_{NT}$-formule is. Dan heet ϕ een propositioneel gevolg van Γ als ϕ_P een propositioneel gevolg is van Γ_P waarbij ϕ_P en Γ_P ontstaan zijn door op ϕ en alle formules in de verzameling Γ het net beschreven algoritme toe te passen.*

De eerste afleidingsregel (de **PC-regel**) luidt nu als volgt:

Definitie 8.0.5. *Wanneer de $\mathcal{L}_{NT}$-formules γ_1 tot en met γ_n bewezen zijn en $\big((\gamma_1 \wedge \cdots \wedge \gamma_n) \to \phi\big)_P$ een tautologie is, is ϕ bewijsbaar*[3]*.*

De volgende twee afleidingsregels zijn de kwantor-regels (**QR-regels**). Wanneer x niet vrij is (dus gebonden is door een kwantor) in de formule ψ geldt het volgende:

1. Uit $N \vdash \psi \to \phi$ volgt $N \vdash \psi \to (\forall x\phi)$. (QR1)

2. Uit $N \vdash \phi \to \psi$ volgt $N \vdash (\exists x\phi) \to \psi$. (QR2)

[3]Merk op dat alle formules ϕ waarvan ϕ_P een tautologie is, afleidbaar zijn! Als er in N immers ook maar één formule (zeg α) afleidbaar is (en dat is natuurlijk zo, denk maar aan de (niet) logische axioma's), is $\alpha_P \to \phi_P$ een tautologie, aangezien ϕ_P dat is. En dan volgt met de PC-regel dat ϕ afleidbaar is!

Nu zijn dus zowel de afleidingsregels, als de logische en niet logische axioma's bekend, en rijst de vraag of voor een gegeven afleiding bepaald kan worden of deze aan de regels van een afleiding voldoet, zoals die aan het begin van dit hoofdstuk beschreven zijn. In het volgende hoofdstuk zal ik nader op deze vraag ingaan.

9 Afleidingen controleren met behulp van Δ-formules

Stel dat je beschikt over een rijtje formules $\langle \phi_1, \phi_2, \ldots, \phi_k \rangle$, waarbij ϕ_k gelijk is aan de formule ϕ, en je wilt weten of dit rijtje formules een afleiding is voor ϕ. Is het mogelijk om van zo'n rijtje formules te bewijzen of dit al dan niet een afleiding is van ϕ?

Voor elke formule in de rij moet je nu dus bepalen of deze formule ofwel een (niet-)logisch axioma is, of dat de formule met behulp van een afleidingsregel is ontstaan uit eerdere formules in de rij. Als dit geldt voor elke formule in de rij en als de laatste formule bovendien overeenkomt met ϕ, dan is het rijtje formules inderdaad een goede afleiding voor ϕ. Wat je feitelijk wilt, is een formule $Deduction(c, f)$, die waar is dan en slechts dan als c een afleiding codeert van de formule met Gödelgetal f. Wanneer $Deduction(c, f)$ een Δ-formule is, kan bovendien voor elk paar (c, f) bewezen worden of c al dan niet een afleiding voor de formule horende bij Gödelgetal f codeert.

Om deze formule te kunnen maken, moet allereerst de rij $\langle \phi_1, \phi_2, \ldots, \phi_k \rangle$ gecodeerd worden en vervolgens moet een constructie bepaald worden om voor elke element uit de rij te bepalen of dit een axioma is, of een gevolg van een afleidingsregel.

Om de rij te coderen op een manier, die nog niet eerder is gebruikt en die zich wel leent tot het terugvinden van de oorspronkelijke rij, gebruiken we de volgende codering: Neem $D = \langle \phi_1, \phi_2, \ldots, \phi_k \rangle$ de rij van formules. De codering van de rij D (sequence code of D) wordt dan gegeven door: $\ulcorner D \urcorner = 5^{\ulcorner \phi_1 \urcorner} 7^{\ulcorner \phi_2 \urcorner} \ldots p_{k+2}^{\ulcorner \phi_k \urcorner}$.

Als D op deze manier gecodeerd wordt zijn ook weer de Δ-formules $SequenceCode(c)$, $SequenceLength(c, l)$ en $IthSequenceElement(e, i, c)$ te maken (zie [1]), die respectievelijk waar zijn dan en slechts dan als c een rij $\mathcal{L}_{NT}$-formules codeert, c een rij van l formules codeert, en c een rij formules codeert waarbij de i^e formule Gödelgetal e heeft.

Nu moeten formules gemaakt worden die van een formule uit de rij D bepalen of deze formule een axioma is of dat deze formule uit een afleidingsregel is voortgekomen.

9.1 (Niet-)logische axioma's

Om te kijken of ϕ_i een axioma uit N is, volstaat het het Gödelgetal van ϕ_i te vergelijken met de Gödelgetallen die horen bij de axioma's van N (zie hoofdstuk 2).

Dit geeft de volgende Δ-formule:

$AxiomOfN(e)$ is:

$$e = \overline{\ulcorner(\forall v_1)\neg(Sv_1 = 0)\urcorner}\vee$$
$$e = \overline{\ulcorner(\forall v_1)(\forall v_2)\big(Sv_1 = Sv_2 \rightarrow v_1 = v_2\big)\urcorner}\vee$$
$$\vdots$$
$$\vee e = \overline{\ulcorner(\forall v_1)(\forall v_2)\big((v_1 < v_2) \vee (v_1 = v_2) \vee (v_2 < v_1)\big)\urcorner}$$

Voor elke formule uit de rij kan dus eenvoudig worden bewezen of deze formule al dan niet een formule is die in de theorie N voorkomt.

Om te kijken of een formule een logisch axioma is, is iets moeilijker. Het aantal logische axioma's is namelijk niet eindig (ze gelden voor de variabele v_1, maar ook voor v_n) en een opsomming geven, zoals ik net deed met de axioma's uit N, kan nu dus niet.

Neem het eerste logische axioma: $x = x$ voor elke variabele x.
Om te testen of een gegeven Gödelgetal e dit axioma weergeeft, zou je moeten kijken of er een variabele x is zodanig dat e gelijk is aan $2^7 3^{\ulcorner x\urcorner} 5^{\ulcorner x\urcorner}$ (de codering van $x = x$).
Als je wilt weten of e gelijk is aan het tweede logische axioma ($\big((x_1 = y_1)\wedge(x_2 = y_2)\big) \rightarrow \big(f(x_1, x_2) = f(y_1, y_2)\big)$) moet je dit axioma uitschrijven voor de verschillende functiesymbolen die er in de taal van de getaltheorie voorkomen.
Voor de functie S zou je dus na moeten gaan of er variabelen x en y te vinden zijn, zodanig dat e gelijk is aan het Gödelgetal dat hoort bij de formule $(x = y) \rightarrow (Sx = Sy)$ (dit getal wordt gegeven door $2^3 3^{2^1 3^{2^7 3^{\ulcorner x\urcorner} 5^{\ulcorner y\urcorner}}} 5^{2^7 3^{2^{11} 3^{\ulcorner x\urcorner}} 5^{2^{11} 3^{\ulcorner y\urcorner}}}$ waarbij de implicatiepijl is vervangen door de negatie in combinatie met de of-operator).
Op dezelfde manier kan dit ook gedaan worden voor de functiesymbolen "+", "$\cdot$", "E" en voor het relatiesymbool "$<$" (horende bij het derde logische axioma).

Voor de kwantoraxioma's kan ook iets soortgelijks gedaan worden.
Om te testen of e een Gödelgetal van het eerste kwantoraxioma $((\forall x\phi) \rightarrow \phi^x_t$, als t subsitueerbaar is voor x in ϕ) is, moet er gekeken worden of er een formule ϕ, een variabele x en een term t te vinden is, waarbij t substitueerbaar is voor x en y gelijk is aan ϕ^x_t zodanig dat e gelijk is aan het Gödelgetal van de formule $(\forall x\phi) \rightarrow \phi^x_t$ $(e = 2^3 3^{2^1 3^{2^5 3^x 5^{\ulcorner\phi\urcorner}}} 5^{\ulcorner y\urcorner}$.

Een Δ-formule die waar is dan en slechts dan als het argument het Gödelgetal van een logisch axioma is, heeft dus de volgende vorm:

$LogicalAxiom(e)$ is:

$$(\exists x < e)(Variable(x) \wedge e = \overline{2}^{\overline{7}}\overline{3}^{x}\overline{5}^{x}) \vee$$
$$\vdots$$
(E2) en (E3) op eenzelfde manier
$$\vdots$$
$$\vee(\exists f, x, t, y < e)(Formula(f) \wedge Variable(x) \wedge Term(t) \wedge$$
$$Substitutable(t, x, f) \wedge Sub(f, x, t, y) \wedge$$
$$e = \overline{2}^{\overline{3}}\overline{3}^{\overline{2}^{\overline{1}}\overline{3}^{\overline{2}^{\overline{5}}\overline{3}^{x}\overline{5}^{f}}}\overline{5}^{y}) \vee$$
(Q2) op dezelfde manier

Met behulp van de Δ-formules $AxiomOfN$ en $LogicalAxiom$ kan nu dus per formule in een te controleren afleiding bepaald (bewezen) worden of deze formule al dan niet een axioma is.

Hiermee ben ik aangekomen bij de afleidingsregels.

9.2 Afleidingsregels

Ga weer uit van een rijtje formules $\langle \phi_1, \phi_2, \ldots, \phi_k \rangle$ waarvan bepaald moet worden of dit een afleiding is. Stel dat $\phi_i = \psi \rightarrow (\forall x \zeta)$. Dan zegt de eerste kwantor regel dat ϕ_i bewijsbaar is, als er al eerder in de rij een ϕ_j voorkomt met $\phi_j = \psi \rightarrow \zeta$, onder de aanname dat x niet vrij is in ψ.
Wanneer dus een ϕ_i van de vorm $\psi \rightarrow (\forall x \zeta)$ wordt gevonden, moet er gekeken worden of er eerder in de rij een ϕ_j van de vorm $\phi_j = \psi \rightarrow \zeta$ voorkomt.

Gegeven een codering voor een rij formules, en de i^e exponent uit die codering (dat is het Gödelgetal van de i^e formule in de afleiding) moet er dus een Δ-formule zijn die kijkt of er formules ψ en ζ en een variabele x te vinden zijn zodat x niet vrij is in ψ en de exponent gelijk is aan $2^3 3^{2^1 3^{\ulcorner \psi \urcorner}} 5^{2^5 3^{\ulcorner x \urcorner} 5^{\ulcorner \zeta \urcorner}}$.
Als dat zo is, is de i^e formule dus van de vorm $\psi \rightarrow (\forall x \zeta)$. Vervolgens moet de Δ-formule kijken of er in een eerdere exponent is die het Gödelgetal is van $\phi_j = \psi \rightarrow \zeta$.

Dat zo'n Δ-formule bestaat is makkelijk aan te nemen, als je weet dat de formule $Free(x, f)$ bestaat (zie [1]), een Δ-formule die waar is dan en slechts dan als x een variabele codeert die vrij is in de formule die hoort bij het Gödelgetal f.

De Δ-formule $QRRule1(c, e, i)$, waarbij c de codering is van een formulerij en e het Gödelgetal van de i^e formule in die rij, doet precies wat hierboven beschreven staat en is dus waar dan en slechts dan als de i^e formule in de formulerij (die door c gecodeerd wordt) verkregen is door de eerste kwantorregel toe te passen op een eerder voorkomende formule in deze rij. De precieze afleiding zal ik wederom niet geven (zie hiervoor [1]). (De uiteindelijk formule doet sterk denken aan de

formule horende bij de kwantorregels binnen de formule $LogicalAxiom(e)$.)

Een dergelijke formule kan ook gevonden worden voor de tweede kwantorregel (zie [1]) en samen geeft dit de volgende Δ-formule:

$QRRule(c, e, i)$ is:

$$QRRule1(c, e, i) \vee QRRule2(c, e, i)$$

die waar is als c een rij formules codeert, e de i^e exponent is in die codering en in de oorspronkelijke rij de i^e formule met behulp van één van de kwantorregels is af te leiden.

De enige afleidingsregel die nog besproken moet worden is het propositionele gevolg. De afleiding die we controleren wordt als vanouds gegeven door: $\langle \phi_1, \phi_2, \ldots, \phi_k \rangle$. De i^e formule uit deze rij is een propositioneel gevolg (zoals ook al in het voorafgaande hoofdstuk is beschreven) als $(\phi_{1\,P} \wedge \cdots \wedge \phi_{i-1\,P}) \rightarrow \phi_{i\,P}$ een tautologie is.

Allereerst moet deze propositieformule geconstrueerd worden, en vervolgens moet elke propositievariabele een waarheidswaarde krijgen, moet er gekeken worden of de totale formule waar of niet waar is, en moet dit herhaald worden tot alle mogelijke waarheidswaardencombinaties zijn toegekend. Als nu blijkt dat de totale formule altijd waar is, is er sprake van een tautologie en kan dus voor de eerste-orde formule ϕ_i geconcludeerd worden dat deze formule het propositioneel gevolg is van de eerdere eerste-orde formules.

Allereerst moeten alle "priemcomponenten" van een formule gevonden worden. Deze priemcomponenten zijn de deelformules die van de vorm $\forall x \alpha$ zijn en niet begrensd zijn door een andere kwantor, en alle atomaire deelformules die op hun beurt ook niet begrensd zijn door een kwantor. (Precies die deelformules die in het algoritme in hoofdstuk 8 beschreven staan.) Er bestaat een Δ-formule $PrimeComponent(u, f)$ (zie [1]) die waar is dan en slechts dan als u het Gödelgetal is van een priemcomponent van een formule ϕ met Gödelgetal f. Deze formule zal ik verder niet afleiden.

Vervolgens is het mogelijk de Δ-formule $Primelist(c, i, r)$ te maken. Hierbij codeert r de "PrimeList" (lijst van alle priemcomponenten) van de eerste i formules uit de afleidingsrij die gecodeerd wordt door c. Deze priemcomponentenrij bevat enkel priemcomponenten van de eerste i formules uit de afleiding, de rij bevat bovendien alle priemcomponenten van deze eerste i formules, er komen geen dubbele priemcomponenten voor en r is het kleinst mogelijke Gödelgetal van een rij die aan alle bovenstaande eisen voldoet. Ik zal formule $PrimeList(c, i, r)$ niet verder uitwerken (zie ([1] voor een preciezere uitwerking), omdat de formule alleen maar lang is en verder weinig ingenieus in elkaar zit.

Vervolgens moet aan elke priemcomponent een waarheidswaarde toegekend worden. Vandaar dat er een formule moet worden ontworpen die aan elke priemcomponent de waarde "1" of "2" meegeeft, waarbij "1" correspondeert met "niet waar" en "2" met "waar". Om dit te doen wordt eerst een rij van 1'en en 2'en gemaakt, die net zo lang is als de rij priemcomponenten. Deze rij wordt vervolgens gecodeerd.

$TruthAssignment(c, i, r, v)$ is:

$$\begin{gathered} PrimeList(c, i, r) \wedge CodeNumber(v) \wedge \\ (\exists l < r)\Big(Length(r, l) \wedge Length(v, l) \wedge \\ (\forall i \leq l)(\forall e < v)\big(IthElement(e, i, v) \rightarrow \\ (e = \overline{1} \vee e = \overline{2})\big)\Big). \end{gathered}$$

$TruthAssignment(c, i, r, v)$ is dus waar dan en slechts dan als v een rij 1'en en 2'en codeert, die van dezelfde lengte is als de rij priemcomponenten die de priemlijst r codeert (horende bij de eerste i formules uit de afleidingsrij c).

Nu aan alle priemcomponenten een waarheidswaarde toegekend is, moet worden bepaald of de formules ϕ_1 tot en met ϕ_i waar zijn (waarheidswaarde 2 hebben). De manier waarop dat gaat, zal ik illustreren aan de hand van een willekeurige formule.

Neem als formule $\forall x((x < y) \wedge (y < 0)) \vee \neg(x \cdot y < 0)$. Een mogelijke formule constructierij is:
$\langle x < y, y < 0, x \cdot y < 0, (x < y) \wedge (y < 0), \neg(x \cdot y < 0), \forall x((x < y) \wedge (y < 0)),$
$\forall x((x < y) \wedge (y < 0)) \vee \neg(x \cdot y < 0)\rangle$.
De priemfactorenlijst die bij deze formule hoort is de volgende:
$\langle \forall x((x < y) \wedge (y < 0)), x \cdot y < 0\rangle$.
Neem aan dat als waarheidswaardetoekenning gekozen is voor de string $\langle 2, 1\rangle$.

Om nu de waarheidswaarde van de hele formule te vinden, moet het volgende gedaan worden:
Aan elk element uit de constructierij wordt een waarheidswaarde toegekend, om uiteindelijk tot de waarheidswaarde van het laatste element uit de constructierij te komen. Dit is dan natuurlijk de waarheidswaarde van de totale formule.
Aan een element dat ook in de priemfactorenrij voorkomt, wordt de waarheidswaarde toegekend die in de corresponderende waarheidstoekenningsrij staat. Wanneer het element niet in de priemfactorenrij voorkomt is het volgende aan de hand:

- Het is een atomaire formule die binnen de gehele formule door een kwantor begrensd is, of een formule van de vorm $\forall x\alpha$, die eveneens door een

(tweede) kwantor begrensd is. In deze gevallen wordt aan het element de waarheidswaarde "3" meegegeven, wat staat voor "onbepaald".

- het element is ontstaan door de negatie te nemen van een eerder element uit de constructierij, of door eerdere elementen samen te voegen door conjunctie of disjunctie. In dat geval is de waarheidswaarde te bepalen, met behulp van de eerder bepaalde waarheidswaarden. Wanneer ook maar één van deze waarden "3" is, wordt de waarheidswaarde van dit laatste element ook gelijk aan "3".

Op deze manier worden de waarheidswaarden van de constructierij-elementen van de zojuist genoemde voorbeeldformule dus:
$\langle 3, 3, 1, 3, 2, 2, 2 \rangle$.

De Δ-formule $Evaluate(e, r, v, y)$ (zie [1]) is op dit idee gebaseerd en is waar dan en slechts dan als e het Gödelgetal is dat hoort bij een formule ϕ, als r de lijst van alle priemcomponenten horende bij die formule codeert, als v een waarheidswaardetoekenningsrij is en als y bovendien de waarheidswaarde van ϕ_P is, gegeven waarheidstoekenning v.

Het is nu dus mogelijk, met behulp van de formule $Evaluate(e, r, v, y)$, de waarheidswaarde van de propositieformule, horende bij een gegeven formule te bepalen (gegeven de waarheidswaarden van de priemcomponenten). En wanneer dat mogelijk is, is het vervolgens ook mogelijk van een functie ϕ_i uit een afleidingsrij, te bepalen of deze functie een propositioneel gevolg is van de voorgaande functies in die rij. Dit is immers het geval als $(\phi_{1\,P} \wedge \cdots \wedge \phi_{i-1\,P}) \rightarrow \phi_{i\,P}$ een tautologie is.
Om dit te controleren volstaat het te bekijken of elke waarheidswaardetoekenning die $\phi_{1\,P}$ tot en met $\phi_{i-1\,P}$ waar maakt, ook $\phi_{i\,P}$ waar maakt.

De volgende Δ-formule controleert dit precies. $PCRule(c, e, i)$ is namelijk waar dan en slechts dan als de i^e component met code e uit een nog te controleren afleidingsrij, gecodeerd door c, tot stand is gekomen door het toepassen van het propositionele gevolg op de eerdere elementen uit de afleidingsrij.

$PCRule(c, e, i)$ is:

$$
\begin{array}{c}
IthSequenceElement(e, i, c) \wedge \\
(\exists r < \left(\overline{2}^{(c^{\overline{2}})^{(c^{\overline{2}})}}\right)^{c^{\overline{3}}}) \\
(\forall v < \left(\left(\overline{2}^{(c^{\overline{2}})^{(c^{\overline{2}})}}\right)^{\overline{\ulcorner\overline{2}\urcorner}}\right)^{c^{\overline{2}}}) \\
\Big((PrimeList(c, i, r) \wedge TruthAssignment(c, i, r, v)) \rightarrow \\
\Big(((\forall j < i)(\exists e_j < c) \\
(IthSequenceElement(e_j, j, c) \wedge Evaluate(e_j, r, v, \overline{2}))) \\
\rightarrow Evaluate(e, r, v, \overline{2})\Big)\Big)
\end{array}
$$

Op de twee laatste regels staat precies dat $(\phi_{1\,P} \wedge \cdots \wedge \phi_{i-i\,P}) \rightarrow \phi_{i\,P}$ een tautologie is. Als immers voor een waarheidstoekenning v geldt dat deze de eerste i-1 elementen van de afleiding waarmaakt, moet dit ook gelden voor het i^e element, en dit als geheel moet dan weer voor elke v gelden.

9.3 $Deduction(c, f)$

Ik begon dit hoofdstuk met de volgende zinnen:

"Stel dat je beschikt over een rijtje formules $\langle \phi_1, \phi_2, \ldots, \phi_k \rangle$, waarbij ϕ_k gelijk is aan de formule ϕ, en je wilt weten of dit rijtje formules een afleiding is voor ϕ. Is het mogelijk om van zo'n rijtje formules te bewijzen of dit al dan niet een afleiding is van ϕ?"

Vervolgens introduceerde ik de formule $Deduction(c, f)$, die waar zou zijn dan en slechts dan als c een afleiding codeerde van de formule met Gödelgetal f. De vraag was toen nog of zo'n formule bestond, en zo ja, of deze formule een Δ-formule zou zijn.

Deze twee vragen kan ik inmiddels allebei met "ja" beantwoorden. De formule $Deduction(c, f)$, zoals hierboven beschreven, bestaat, is een Δ-formule en ziet er als volgt uit:

$Deduction(c, f)$ is:

$$SequenceCode(c) \wedge Formula(f) \wedge$$
$$(\exists l < c)\Big(SequenceLength(c, l) \wedge IthSequenceElement(f, l, c) \wedge$$
$$(\forall i \leq l)(\forall e < c)\Big(IthSequenceElement(e, i, c) \rightarrow$$
$$\big(LogicalAxiom(e) \vee AxiomOfN(e) \vee$$
$$QRRule(c, e, i) \vee PCRule(c, e, i)\big)\Big)\Big).$$

Voor elke gegeven, nog te controleren, afleiding kan dus gecheckt worden, of dit inderdaad een afleiding is!

Nu we de formule $Deduction(c, f)$ hebben, kunnen we ook de formule $(\exists c)(Deduction(c, f))$ creëren. Deze laatste formule is waar dan en slechts dan als f het Gödelgetal is van een formule die te bewijzen is in N (ook wel een **stelling** genoemd).

En dit is dan de formule waar we al die tijd naar toe gewerkt hebben!

$Thm_N(f)$ is:

$$(\exists c)(Deduction(c, f)).$$

Aangezien je van tevoren geen idee hebt hoe groot een afleiding kan zijn, is het helaas niet mogelijk een bovengrens voor de c te vinden. De formule $Thm_N(f)$ (f is het Gödelgetal van een stelling in N) is dan ook geen Δ-formule. Het is echter wel een Σ-formule, en dat houdt in dat, wanneer er een bewijs binnen N bestaat van een zekere formule ϕ, en de formule $Thm_N(\ulcorner \phi \urcorner)$ dus waar is in $\mathfrak{N}$, ook **bewezen** kan worden dat dit bewijs inderdaad bestaat! (zie **Propositie 3.2.1**)
Om het wiskundig te maken: uit $\mathfrak{N} \models Thm_N(\overline{f})$ volgt $N \vdash Thm_N(\overline{f})$.

Hiermee is voldaan aan de eerste voorwaarde die ik stelde in hoofdstuk 4! De bewijsbaarheid van formules is nu uit te drukken in een $\mathcal{L}_{NT}$-formule, die bovendien een Σ-formule blijkt te zijn.

In het volgens hoofdstuk kom ik terug op de tweede voorwaarde:

- Een formule ϕ moet kunnen refereren aan haar eigen bewijsbaarheid.

10 Het Self-reference Lemma

Op dit moment hebben we de beschikking over de Σ-formule $Thm_N(f)$ die waar is dan en slechts dan als f het Gödelgetal is dat hoort bij een in N bewijsbare formule ϕ.

In hoofdstuk 4 heb ik beschreven hoe het bewijs van de eerste onvolledigheidsstelling er globaal uit zou gaan zien:
Er moest een formule θ gemaakt worden, die van zichzelf zou zeggen onbewijsbaar te zijn.

Als we nog even uitgaan van het axiomatisch syteem N (in het volgende hoofdstuk zal ik laten zien dat elk axiomatisch systeem dat de natuurlijk getallen beschrijft voor N in de plaats gezet kan worden), is het nu mogelijk om te praten over de Gödelgetallen van stellingen (bewijsbare formules) in N.

Het wordt moeilijker om θ te laten "spreken" over $Thm_N(\ulcorner\theta\urcorner)$. Om een dergelijke constructie mogelijk te maken (een constructie waarin θ refereert aan haar eigen bewijsbaarheid), is het **self-reference lemma** nodig.

Lemma 10.0.1. *Gödels Self-Reference Lemma*
Laat $\psi(v_1)$ een $\mathcal{L}_{NT}$-formule zijn, met maar één vrije variabele v_1. Dan is er een zin (gesloten formule) ϕ zodanig dat:

$$N \vdash \big(\phi \leftrightarrow \psi(\overline{\ulcorner\phi\urcorner})\big).$$

Bewijs:
Allereerst definieer ik de formule $\gamma(v_1)$ (die overigens afhangt van de gekozen ψ) als volgt:

$$\forall y \forall z \Big(\big(Num(v_1, y) \wedge Sub(v_1, \overline{4}, y, z) \big) \rightarrow \psi(z) \Big).$$

Hierbij heeft $\psi(z)$ dus de eigenschappen zoals vermeldt in het lemma.
Neem nu voor ϕ de formule $\gamma(\overline{m})$, met $m = \ulcorner\gamma(v_1)\urcorner$. De zo gekozen ϕ is een gesloten formule en het zal zometeen blijken dat deze ϕ voldoet aan het lemma.

Daarvoor zijn nog de volgende twee observaties nodig:

- In hoofdstuk 7 heb ik achtereenvolgens de functies Num en Sub gedefinieerd, waarbij $\mathrm{Num}(a)=\ulcorner\overline{a}\urcorner$ en $\mathrm{Sub}(\ulcorner\alpha\urcorner,\ulcorner x\urcorner,\ulcorner t\urcorner)=\ulcorner\alpha^x_t\urcorner$. Aangezien deze functies worden gerepresenteerd door de Δ-formules Num en Sub geldt nu het volgende (zie ook hoofdstuk 7):

  $N \vdash \Big(Num(\overline{a}, y) \leftrightarrow y = \overline{\mathrm{Num}(a)} \Big)$ (1)
  $N \vdash \Big(Sub(\overline{a}, \overline{b}, \overline{c}, z) \leftrightarrow z = \overline{\mathrm{Sub}(a,b,c)} \Big)$ (2)

- Verder wil ik alvast de volgende afleiding maken:
  $\mathrm{Sub}(m, 4, \ulcorner\overline{m}\urcorner) = \mathrm{Sub}(\ulcorner\gamma(v_1)\urcorner, \ulcorner v_1\urcorner, \ulcorner\overline{m}\urcorner) = \ulcorner\gamma(v_1)^{v_1}_{\overline{m}}\urcorner$
  $= \ulcorner\gamma(\overline{m})\urcorner = \ulcorner\phi\urcorner$ (3)
  (NB: $\ulcorner v_1\urcorner = 4$.)

Wanneer je dit weet, is de equivalentie van de volgende formules bewijsbaar in N:

ϕ	
$\gamma(\overline{m})$	definitie van ϕ
$\forall y \forall z \Big(\big(Num(\overline{m}, y) \wedge Sub(\overline{m}, \overline{4}, y, z) \big) \to \psi(z) \Big)$	v_1 door $\overline{m}$ vervangen in $\gamma(v_1)$
$\forall y \forall z \Big(Num(\overline{m}, y) \to \big(Sub(\overline{m}, \overline{4}, y, z) \to \psi(z) \big) \Big)$	$(A \wedge B) \to C$ is gelijk aan $A \to (B \to C)$
$\forall y \forall z \Big(y = \overline{\mathrm{Num}(m)} \to \big(Sub(\overline{m}, \overline{4}, y, z) \to \psi(z) \big) \Big)$	Num representeert Num, zie (1)
$\forall y \forall z \Big(y = \overline{\ulcorner\overline{m}\urcorner} \to \big(Sub(\overline{m}, \overline{4}, y, z) \to \psi(z) \big) \Big)$	$\mathrm{Num}(m) = \ulcorner\overline{m}\urcorner$
$\forall z \Big(Sub(\overline{m}, \overline{4}, \overline{\ulcorner\overline{m}\urcorner}, z) \to \psi(z) \Big)$	eerste kwantoraxioma
$\forall z \Big(z = \overline{\mathrm{Sub}(m, 4, \ulcorner\overline{m}\urcorner)} \to \psi(z) \Big)$	Sub representeert Sub, zie (2)
$\forall z \Big(z = \overline{\ulcorner\phi\urcorner} \to \psi(z) \Big)$	$\mathrm{Sub}(m, 4, \ulcorner\overline{m}\urcorner) = \ulcorner\phi\urcorner$ (zie (3))
$\psi(\overline{\ulcorner\phi\urcorner})$	eerste kwantoraxioma

En hieruit volgt het gezochte: $N \vdash \phi \leftrightarrow \psi(\overline{\ulcorner\phi\urcorner})$. $\square$

Merk op dat bovenstaande ϕ een Π-formule is, en dat ψ dus ook een Π-formule zal zijn. (Het is ook mogelijk ϕ enigszins aan te passen, zodat ψ equivalent moet zijn aan een Σ-formule.)

Met het **self-reference lemma** en de formule $Thm_N(f)$ kan nu eindelijk de eerste onvolledigheidsstelling van Gödel bewezen worden!

11 De eerste onvolledigheidsstelling

In de afgelopen hoofdstukken zijn allerlei Δ-formules afgeleid, met als eindresultaat de Σ-formule $Thm_N(f)$. De eerste opmerking die ik hier wil maken is dat de onvolledigheidsstelling **elk** axiomatisch systeem betreft, niet alleen het axiomatisch systeem N waar ik de afgelopen hoofdstukken mee heb gewerkt. Vandaar dat we graag een formule $Thm_A(f)$ zouden hebben, die waar is dan en slechts dan als de formule, horende bij Gödelgetal f, bewijsbaar is in een willekeurig axiomatisch systeem A, dat de natuurlijke getallen beschrijft, en waarvan de axioma's herkenbaar zijn. Je zou immers een axiomatisch systeem kunnen creëren waarbij je als axioma's kiest voor "alle ware formules", maar in dat geval wordt het toch lastig (zeg gerust onmogelijk) om van een gegeven formule te bepalen of deze formule al dan niet een axioma is, en dan kan van een formule niet meer bepaald worden of deze is voortgekomen uit een combinatie van de axioma's en afleidingsregels.

Kortom: je kiest voor een axiomatisch systeem A waarvan de axioma's herkenbaar zijn, wat wiskundig gezien betekent dat de verzameling **AXIOMOFA**$=$ $\{\ulcorner\alpha\urcorner|\alpha \in A\}$ een recursieve verzameling is. Verder stel je als voorwaarde dat A consistent is.

Wanneer voor een dergelijke theorie A wordt gekozen, kan de formule $Thm_N(f)$ makkelijk worden uitgebreid naar de formule $Thm_A(f)$. De enige verandering die hier voor nodig is, is namelijk de Δ-formule $AxiomOfN$ te vervangen door de Δ-formule $AxiomOfA$ en we weten dat deze laatste formule bestaat aangezien de set axioma's recursief is.

Nu komt dan eindelijk het bewijs van de eerste onvolledigheidsstelling!

Propositie 11.0.1. *Gödels eerste onvolledigheidsstelling*
Neem aan dat A een consistente en recursieve verzameling van axioma's uit de taal $\mathcal{L}_{NT}$ is. Dan is er een gesloten Π-formule θ zodanig dat $\mathfrak{N} \models \theta$ maar $A \nvdash \theta$.

Bewijs:
De formule $Thm_A(f)$ is gedefinieerd als $(\exists c)(Deduction_A(c, f)$ en is dus een Σ-formule. Uit **propositie 3.2.1** volgt nu:

$$\text{Als } \mathfrak{N} \models Thm_A(\overline{f}), \text{ dan } N \vdash Thm_A(\overline{f}).$$

Er mag vanuit gegaan worden dat in A ook alle axioma's uit N te bewijzen zijn. Als dat niet het geval is, hebben we direct de ware, maar onbewijsbare Π-formule gevonden.

Gebruik nu het self-reference lemma om een zin θ te creëren zodat:

$$N \vdash \Big(\theta \leftrightarrow \neg Thm_A\big(\overline{\ulcorner\theta\urcorner}\big)\Big).$$

(De formule $\neg Thm_A\big(\overline{\ulcorner\theta\urcorner}\big)$ is een Π-formule, dus θ kan equivalent aan een Π-formule gekozen worden.)
Als je weet dat $\theta \leftrightarrow \neg Thm_A\big(\overline{\ulcorner\theta\urcorner}\big)$ bewijsbaar is, weet je ook (aangezien je hebt aangenomen dat je een consistent axiomatisch systeem hebt!) dat $\theta \leftrightarrow \neg Thm_A\big(\overline{\ulcorner\theta\urcorner}\big)$ waar is, en dat dus het volgende geldt:

$$\mathfrak{N} \models \Big(\theta \leftrightarrow \neg Thm_A\big(\overline{\ulcorner\theta\urcorner}\big)\Big)$$

Hieruit volgt nu:

$$\begin{aligned} \mathfrak{N} \models \theta \quad &\leftrightarrow \quad \mathfrak{N} \not\models Thm_A\big(\overline{\ulcorner\theta\urcorner}\big) \\ &\leftrightarrow \quad \ulcorner\theta\urcorner \notin THM_A \\ &\leftrightarrow \quad A \nvdash \theta. \end{aligned}$$

Dus ofwel θ is waar in $\mathfrak{N}$ en niet bewijsbaar uit A, ofwel θ is onwaar in $\mathfrak{N}$ en wél bewijsbaar uit A!

Stel dat dit laatste het geval is: θ is bewijsbaar uit A, maar onwaar. Dan geldt $A \vdash \theta$, en dus $\mathfrak{N} \models Thm_A\big(\overline{\ulcorner\theta\urcorner}\big)$. Aangezien $Thm_A(f)$ een Σ-formule is, geldt nu $N \vdash Thm_A\big(\overline{\ulcorner\theta\urcorner}\big)$. Uit de formules $N \vdash Thm_A\big(\overline{\ulcorner\theta\urcorner}\big)$ en $N \vdash \Big(\theta \leftrightarrow \neg Thm_A\big(\overline{\ulcorner\theta\urcorner}\big)\Big)$ volgt nu dat $N \vdash \neg\theta$. Aangezien A alle axioma's uit N kan bewijzen (en dus minstens zo "sterk" is als A) geldt bovendien $A \vdash \neg\theta$.
De aanname was dat $A \vdash \theta$ en nu blijkt ook $A \vdash \neg\theta$ te gelden! Dit impliceert dat A een inconsistent axiomatisch systeem is, wat tegen de aanname van consistentie ingaat.

De optie die overblijft is nu dus dat $\mathfrak{N} \models \theta$, terwijl $A \nvdash \theta$. De formule θ is waar, maar onbewijsbaar! De eerste onvolledigheidsstelling is hiermee bewezen! $\square$

12 De tweede onvolledigheidsstelling

Nu de eerste onvolledigheidsstelling bewezen is, komt de tweede aan bod. Deze tweede onvolledigheidsstelling zegt het volgende: En consistent axiomatisch systeem (dat minstens zo sterk is als de Peano rekenkunde en waarvan de axioma's gerepresenteerd kunnen worden door een Σ-formule) kan haar eigen consistentie niet bewijzen!

Om te beginnen zal ik het begrip **Peano Rekenkunde (Peano Arithmetic)** invoeren:

Definitie 12.0.1. *De axioma's van de Peano Rekenkunde, oftewel PA, zijn de elf reeds ingevoerde axioma's uit N, samen met de volgende "axioma verzameling":*

$$\Big(\phi(0) \wedge (\forall x)\big(\phi(x) \to \phi(Sx)\big)\Big) \to (\forall x)\phi(x)$$

voor alle $\mathcal{L}_{NT}$-formules ϕ met één vrije variabele.

Ook hier geldt weer dat de verzameling axioma's recursief is en dat er een Δ-formule $AxiomOfPA$ bestaat en daarmee ook de Σ-formule $Thm_{PA}(f)$, die waar is dan en slechts dan als f bewijsbaar is uit de Peano-axioma's.

In de Peano rekenkunde gelden bovendien (met dank aan het "inductie-axioma") de volgende drie eigenschappen voor alle formules ϕ (zie [3] en [1]):

$$\text{Als } PA \vdash \phi, \text{ dan } PA \vdash Thm_{PA}(\overline{\ulcorner \phi \urcorner}). \quad (R1)$$

$$PA \vdash \Big(Thm_{PA}(\overline{\ulcorner \phi \urcorner}) \to Thm_{PA}(\overline{\ulcorner Thm_{PA}(\overline{\ulcorner \phi \urcorner})\urcorner})\Big). \quad (R2)$$

$$PA \vdash \Big(\big(Thm_{PA}(\overline{\ulcorner \phi \urcorner}) \wedge Thm_{PA}(\overline{\ulcorner \phi \to \psi \urcorner})\big) \to Thm_{PA}(\overline{\ulcorner \psi \urcorner})\Big). \quad (R3)$$

Aan de hand van deze eigenschappen is het nu mogelijk de tweede onvolledigheidsstelling te bewijzen.

Het is van belang eerst nog even stil te staan bij de betekenis van consistent. In een consistent systeem kan nooit zowel een formule als haar negatie bewezen worden.

Wanneer we nu de formule $\big((\forall x)x = x\big) \wedge \neg\big((\forall x)x = x\big)$ nemen (in het vervolg genoteerd als $\bot$), geldt het volgende:
De zin Con_{PA} kan gekozen worden als $\neg Thm_{PA}(\overline{\ulcorner \bot \urcorner})$.
Het is namelijk zo dat $\mathfrak{N} \models Con_{PA}$ dan en slechts dan als PA een consistent axiomatisch systeem is. Zou PA inconsistent zijn, dan is elke formule bewijsbaar, en $\bot$ dus ook, en indien PA wel consistent is, moet $\bot$ onbewijsbaar zijn, aangezien $\neg \bot$ wel bewijsbaar is ($\neg A \vee A$ is immers een tautologie) en in een consistent systeem niet zowel de negatie als de formule zelf bewijsbaar mogen zijn!

Nu de consistentie is uitgedrukt in formulevorm kan het uiteindelijke bewijs gegeven worden.

Propositie 12.0.2. *Gödels tweede onvolledigheidsstelling*
Als de Peano Rekenkunde consistent is, dan geldt dat $PA \nvdash Con_{PA}$.

Bewijs:
Neem θ vergelijkbaar aan de θ in de eerste onvolledigheidsstelling:

$$PA \vdash \Big(\theta \leftrightarrow \neg Thm_{PA}\big(\overline{\ulcorner\theta\urcorner}\big)\Big)$$

(Dit kan aangezien PA minstens zo "sterk" is als N en $\neg Thm_{PA}\big(\overline{\ulcorner\theta\urcorner}\big)$ een Π-formule is.)

Uit het bewijs van de eerste onvolledigheidsstelling weten we dat $PA \nvdash \theta$. Wanneer nu ook kan worden aangetoond dat

$$PA \vdash \big(Con_{PA} \rightarrow \theta\big)$$

geldt, weten we dat $PA \nvdash Con_{PA}$. Immers, als $PA \vdash Con_{PA}$, geldt ook dat $PA \vdash \theta$ (mbv de PC-regel en het feit dat $((A \rightarrow B) \wedge A) \rightarrow B$ een tautologie is), en dit levert een tegenstelling op!

Het volstaat nu dus $PA \vdash (Con_{PA} \rightarrow \theta)$ te bewijzen.

Aangezien de eigenschappen (R1),(R2) en (R3) geldig zijn voor willekeurige formules ϕ, kan ϕ vervangen worden door θ. Dit geeft voor (R2) het volgende:

$$PA \vdash \Big(Thm_{PA}(\overline{\ulcorner\theta\urcorner}) \rightarrow Thm_{PA}(\overline{\ulcorner Thm_{PA}(\overline{\ulcorner\theta\urcorner})\urcorner})\Big). \quad (1)$$

Daar θ zo gekozen is dat $PA \vdash \Big(\theta \leftrightarrow \neg Thm_{PA}\big(\overline{\ulcorner\theta\urcorner}\big)\Big)$ weten we bovendien dat de zin

$$Thm_{PA}\Big(\overline{\ulcorner Thm_{PA}(\overline{\ulcorner\theta\urcorner}) \rightarrow \neg\theta\urcorner}\Big)$$

een ware Σ-zin is. En omdat N (en PA dus ook) sterk genoeg is om ware Σ-zinnen te bewijzen (zie **propositie 3.2.1**) geeft dit nu:

$$PA \vdash Thm_{PA}\Big(\overline{\ulcorner Thm_{PA}(\overline{\ulcorner\theta\urcorner}) \rightarrow \neg\theta\urcorner}\Big) \quad (2)$$

Wanneer we nu in (R3) ϕ vervangen door $Thm_{PA}(\overline{\ulcorner\theta\urcorner})$ en ψ door $\neg\theta$, kunnen we uit de combinatie van deze vernieuwde (R3) en (2) (weer dmv de PC-regel)

$$PA \vdash Thm_{PA}\Big(\overline{\ulcorner Thm_{PA}(\overline{\ulcorner\theta\urcorner})\urcorner}\Big) \rightarrow Thm_{PA}(\overline{\ulcorner\neg\theta\urcorner}) \quad (3)$$

afleiden. In combinatie met (1) levert dit (NB: $((A \to B) \wedge (B \to C)) \to (A \to C)$ is weer een tautologie)

$$PA \vdash Thm_{PA}(\overline{\ulcorner \theta \urcorner}) \to Thm_{PA}(\overline{\ulcorner \neg\theta \urcorner}). \quad (4)$$

Merk nu op dat $\theta \to \big((\neg\theta) \to \bot\ \big)$ een tautologie is en dus bewijsbaar is en dat daaruit volgt dat

$$Thm_{PA}\Big(\overline{\ulcorner \theta \to \big((\neg\theta) \to \bot\ \big)\urcorner}\Big)$$

een ware Σ-zin is, waaruit dan weer volgt dat:

$$PA \vdash Thm_{PA}\Big(\overline{\ulcorner \theta \to \big((\neg\theta) \to \bot\ \big)\urcorner}\Big) \quad (5)$$

Wanneer we nu in (R3) ϕ vervangen door θ en ψ door $\neg\theta \to \bot$, en de ontstane formule combineren met (5) kunnen we de formule

$$PA \vdash Thm_{PA}(\overline{\ulcorner \theta \urcorner}) \to Thm_{PA}(\overline{\ulcorner \neg\theta \to \bot \urcorner}) \quad (6)$$

afleiden. Nu gebruiken we nogmaals (R3), deze keer in combinatie met (6), vervangen in (R3) ditmaal ϕ door $\neg\theta$ en ψ door $\bot$, en houden in herinnering dat $(A \wedge B) \to C$ gelijk is aan $B \to (A \to C)$. Dit geeft dan:

$$PA \vdash Thm_{PA}(\overline{\ulcorner \theta \urcorner}) \to \big(Thm_{PA}(\overline{\ulcorner \neg\theta \urcorner}) \to Thm_{PA}(\overline{\ulcorner \bot \urcorner})\big)$$

Wanneer je dit combineert met (4) en maar weer eens de PC-regel gebruikt $(((A \to (B \to C)) \wedge (A \to B)) \to (A \to C)$ is een tautologie) krijg je

$$PA \vdash Thm_{PA}(\overline{\ulcorner \theta \urcorner}) \to Thm_{PA}(\overline{\ulcorner \bot \urcorner}),$$

wat weer equivalent is aan

$$PA \vdash \neg Thm_{PA}(\overline{\ulcorner \bot \urcorner}) \to \neg Thm_{PA}(\overline{\ulcorner \theta \urcorner}).$$

Uit de definitie van θ en de PC-regel volgt nu direct

$$PA \vdash \neg Thm_{PA}(\overline{\ulcorner \bot \urcorner}) \to \theta,$$

wat per definitie gelijk is aan

$$PA \vdash Con_{PA} \to \theta.$$

Hiermee is het bewijs van de tweede onvolledigheidsstelling geleverd! $\square$

Voor sterkere axiomatische systemen is het bewijs uiteraard identitiek. Als er maar voor gezorgd wordt dat de axioma's herkend kunnen worden.

13 Volledigheidsstelling vs. Onvolledigheidsstelling

Nu beide onvolledigheidsstellingen bewezen zijn, leek het me leuk nog even terug te grijpen naar een eerder werk van Gödel: zijn **volledigheidsstelling**.

De namen van beide stellingen klinken nogal tegengesteld, en wanneer de volledigheidsstelling met de eerste onvolledigheidsstelling vergeleken wordt, lijken ze ook niet direct samen te kunnen gaan.

De volledigheidsstelling luidt namelijk als volgt:

Propositie 13.0.3. *Gödels volledigheidsstelling*
Stel dat Σ een verzameling $\mathcal{L}$-formules is en ϕ is eveneens een $\mathcal{L}$-formule. Dan geldt het volgende:

$$\textit{Als } \Sigma \models \phi, \textit{ dan } \Sigma \vdash \phi.$$

Dit lijkt nogal haaks te staan op de eerste onvolledigheidsstelling, die zegt dat er binnen elk consistent axiomatisch systeem dat de natuurlijk getallen beschrijft, altijd een ware, maar onbewijsbare formule te vinden is.

Maar.. In de volledigheidsstelling gaat het niet om zomaar een model van Σ, het gaat om alle modellen!
Met de notatie "Als $\Sigma \models \phi$, dan $\Sigma \vdash \phi$" wordt bedoeld dat wanneer ϕ waar is in **elk** model voor Σ, ϕ ook uit Σ bewezen kan worden.

Om er zeker van te zijn dat binnen een theorie Σ alle ware uitspraken over de natuurlijke getallen bewezen kunnen worden, moeten deze axioma's dus zo gekozen worden, dat ze waar zijn in structuren (één is ook al voldoende) waarin ook alle ware uitspraken over de natuurlijke getallen waar zijn en verder in geen enkele andere structuur.

Wanneer het gaat om axiomatische systemen die de eigenschappen van de natuurlijke getallen beschrijven is er echter het volgende aan de hand: Er kunnen meerdere modellen zijn waarin een bepaalde verzameling axioma's waar is, maar in het ene model is formule ϕ wél en in het andere model niet waar! Zo'n ϕ kan dus nooit bewezen worden, ook niet in het model waarin deze formule wél waar is. Immers: als ϕ wel enkel met de gekozen axioma's bewezen zou kunnen worden, zou dit in beide modellen mogelijk moeten zijn, en een onware formule is in een consistent systeem uiteraard niet bewijsbaar. Maar de volledigheidsstelling spreekt dit niet tegen!

De conclusie is, wat iedereen al vantevoren aan zag komen: de volledigheidsstelling en de onvolledigheidsstellingen kunnen gewoon naast elkaar bestaan!

14 Voorbeeld van onbewijsbare (maar ware) formule

Voordat ik aan mijn conclusie begin wil ik graag nog even terugkomen op de formule θ die "zegt" dat ze onbewijsbaar is. Als alleen dergelijke metamathematische formules niet bewijsbaar zijn, is er misschien nog niet zo veel aan de hand. Wanneer zou je zo'n formule überhaupt willen bewijzen?

Dat de eerste onvolledigheidsstelling van Gödel ook van toepassing is op andere formules dan de metamathematische, wordt mooi neergezet in het artikel *"Accessible independence results for Peano Arithmetic"*, geschreven door L Kirby en J Paris (1982).

Ik zal nu één van de twee voorbeelden van ware, maar binnen de Peano Rekenkunde onbewijsbare, formules geven, die in het artikel beschreven worden.

Laat m en n natuurlijke getallen, groter dan 1 zijn. De *representatie van m met grondtal n* wordt dan als volgt gedefinieerd:
Schrijf m als de som van machten van n. Schrijf vervolgens elke exponent als de som van machten van n. Doe hetzelfde met de exponenten van de exponenten en ga zo door totdat de representatie niet meer verandert.

Om een getallenvoorbeeld te geven met m=266 en n=2:
$266 = 2^8 + 2^3 + 2^1 = 2^{2^3} + 2^{2+1} + 2^1 = 2^{2^{2+1}} + 2^{2+1} + 2^1$.

Vervolgens wordt $G_n(m)$ als volgt gedefinieerd: als $m = 0$ is $G_n(m)$ gelijk aan 0. Anders geldt dat $G_n(m)$ het getal is dat ontstaat door elke n in de representatie van m met grondtal n te vervangen door $n+1$ en er vervolgens 1 vanaf te trekken. ($G_2(266)$ is dus $3^{3^{3+1}} + 3^{3+1} + 2$.)

De Goodstein rij voor m, beginnend bij n=2 wordt nu gegeven door:

$$m_0 = m, m_1 = G_2(m_0), m_2 = G_3(m_1), m_3 = G_4(m_2), \ldots.$$

Wanneer we weer uitgaan van m=266, wordt deze rij:

$$\begin{aligned}
266_0 &= 266 = 2^{2^{2+1}} + 2^{2+1} + 2 \\
266_1 &= 3^{3^{3+1}} + 3^{3+1} + 2 \\
266_2 &= 4^{4^{4+1}} + 4^{4+1} + 1 \\
266_3 &= 5^{5^{5+1}} + 5^{5+1} \\
&\vdots
\end{aligned}$$

Uiteraard kan een dergelijke Goodstein rij geconstrueerd worden voor willekeurige m, beginnende bij een eveneens willekeurige n.

Nu geldt er bovendien het volgende (zie voor het bewijs van deze stelling [4]):

Propositie 14.0.4.
(1) $\forall m \exists k m_k = 0$. *Met andere woorden: voor elke* $m, n > 1$ *bereikt de Goodstein rij van* m*, beginnende bij* n *uiteindelijk 0.*[4]
(2) $\forall m \exists k m_k = 0$ *is niet bewijsbaar in* PA.

Alhoewel we deze formule binnen de Peano Rekenkunde kunnen **formuleren**, kunnen we hem niet **bewijzen**. Dit komt omdat het verschrikkelijk lang kan duren voor een Goodstein rijtje uiteindelijk nul bereikt. Het inductie-axioma van de Peano Rekenkunde is niet meer toereikend en er moet een andere vorm van inductie aangeboord worden (zoals met ordinaalgetallen, waar het bewijs in het artikel op gebaseerd is).

Hierbij is dus geïllustreerd dat er ook minder "flauwe" ware, maar onbewijsbare formules bestaan.

[4]NB: Het lijkt of de elementen uit de rij explosief zullen stijgen en in het begin klopt dit ook. De term "-1" zal er echter uiteindelijk voor gaan zorgen dat de elementen toch naar nul toe gaan. Om een heel eenvoudig voorbeeldje te geven van hoe dit werkt neem ik $m = 3$ en $n = 2$. Het bijbehorende rijtje wordt nu:

$$\begin{aligned} m_0 &= 2^1 + 1 \\ m_1 &= 3^1 \\ m_2 &= 4^1 - 1 = 3 \\ m_3 &= 2 \\ m_4 &= 1 \\ m_5 &= 0 \end{aligned}$$

15 Hoe nu verder?

Nu zowel de eerste als de tweede onvolledigheidsstelling besproken en bewezen is, is het tijd om ons af te vragen wat voor impact deze stellingen hebben gehad in de (wiskundige) wereld. In dit laatste hoofdstuk zal ik kort twee conclusies bespreken die door velen getrokken zijn (zie ook [5] en [6]): één naar aanleiding van de eerste onvolledigheidsstelling en één naar aanleiding van de tweede.

Ik zal beginnen met de eerste onvolledigheidssteling. Nu we weten dat er altijd stellingen zullen zijn die, binnen een bepaald systeem, niet bewezen kunnen worden op de "wiskundige manier" (dat wil zeggen: met behulp van axioma's en afleidingsregels), is een mogelijke (pessimistische) conclusie dat we altijd zullen blijven twijfelen over oneindig veel uitspraken.

Bij deze conclusie vallen gelukkig kanttekeningen te plaatsen.

De mensen die deze conclusie zullen trekken gaan er vanuit dat je een stelling alleen als waar aan kan nemen, indien deze via de op dit moment gangbare manier bewezen kan worden.

Maar is het combineren van axioma's met afleidingsregels de enige manier om achter de waarheid te komen ? Hebben we tijdens het bewijs van de eerste onvolledigheidsstelling niet al kunnen zien dat een "metamathematische wijze van redeneren" ook zijn vruchten af kan werpen? Van de formule θ die zei onbewijsbaar te zijn, kon immers al bij voorbaat worden vastgesteld dat, indien θ wel bewijsbaar zou zijn, θ onwaar zou zijn en andersom. Een dergelijke manier van bewijsvoering is dan wel niet de wiskundige manier, maar toch ook zeker niet per definitie een onjuiste manier.

Wanneer we kijken naar de tweede onvolledigheidsstelling is er één gedachte die direct naar boven komt: hoe kunnen we ooit nog weten of we geen onzin produceren binnen onze axiomatische systemen? De consistentie van een systeem is binnen dat systeem immers niet te bewijzen, en mocht de consistentie van systeem A wel in systeem B bewezen worden, dan kan weer worden getwijfeld aan de consistentie van systeem B en dus ook aan de uitspraak dat systeem A consistent is. Het lijkt een visieuze cirkel waar men nooit meer uit zal komen.

En toch.. zou er eigenlijk niks aan onze kijk op de wiskunde moeten veranderen nu we de tweede onvolledigheidsstelling van Gödel kennen en wel om de volgende reden:
Als we niet twijfelen aan de consistentie van een theorie, is een bewijs van consistentie niet meer nodig. Indien we wél twijfelen aan de consistentie van een theorie zal een bewijs, gegeven binnen die theorie, van de consistentie ervan die twijfel niet wegnemen. Binnen een inconsistent systeem kan immers alles bewezen worden!

Gödels tweede onvolledigheidsstelling zou dan ook zeker niet moeten leiden tot wanhoop! Degene die al vertrouwen hadden, moeten dit vertrouwen zeker houden, en zij die nooit vertrouwen hebben gehad, zullen het ook nooit krijgen.

De tweede onvolledigheidsstelling dient dan ook vooral als illustratie van de waarheid van de eerste onvolledigheidsstelling. Binnen een consistent systeem (sterk genoeg om de eigenschappen van de natuurlijke getallen te beschrijven) zal de eigen consistentie nooit bewezen kunnen worden: een duidelijk voorbeeld van een ware maar onbewijsbare formule!

Als afsluiting zou ik graag de laatste zin uit het boek *"Gödels Proof"* ([6]) citeren. Over Gödels onvolledigheidsstelling wordt daar het volgende gezegd:
"It is an occasion, not for dejection, but for a renewed appreciation of the powers of creative reason."

Hierbij sluit ik mij volledig aan! Laten we vooral blijven zoeken naar nieuwe vormen van bewijzen en het geloof dat we hadden in de wiskunde voor eeuwig behouden.

Referenties

[1] C.C. Leary. *A friendly introduction to Mathematical Logic*. Prentice Hall, Upper Saddle River, New Jersey (2000)

[2] S.N. Burris. *Logic for Mathematics and Computer science*. Prentice Hall, Upper Saddle River, New Jersey (1998)

[3] H.B.Enderton. *A mathematical introduction to logic - second edition*. Harcourt/Academic Press, Burlington, Massachusetts (2001)

[4] L. Kirby, J. Paris. Accessible independence results for Peano arithmetic. *Bull. London Math. Soc. 14*, no. 4, p. 285-293 (1982)

[5] T. Franzén. *Gödel's Theorem. An incomplete guide to its use and abuse*. A K Peters Ltd, Wellesley, Massachusetts (2005)

[6] E. Nagel, J.R. Newman, edited and with a new foreword by D.R. Hofstadter. *Gödels Proof - revised edition*. New York University Press, New York and London (2001)