Universiteit Utrecht

Department Wiskunde

Bachelorscriptie

Bewijsbaarheid in zwakkere modellen van de rekenkunde

Auteur:
Bart Keller

Begeleider:
Dr. Jaap van Oosten

April-Juni 2017

Inhoudsopgave

1 Inleiding **2**

2 Voorkennis **3**

2.1 Een inleiding tot zwakkere theorieën 3

2.2 Notatie en conventies 8

3 Het duiventilprincipe **9**

4 De cofinaliteit van priemgetallen **21**

5 Verbeteringen en nieuwe bevindingen **28**

5.1 Een zwakkere aanname 28

5.2 De eindige axiomatisering van $I\Delta_0$ 29

A Appendix: Een kleine inleiding tot computationele complexiteitstheorie **30**

1 Inleiding

Rekenen met natuurlijke getallen is iets wat vrijwel iedere wiskundige extensief tegenkomt. Aan het eind van de negentiende eeuw was het de Italiaanse wiskundige Giuseppe Peano die een formalisering gaf van de rekenkunde van natuurlijke getallen. Deze axioma's worden tot op de dag van vandaag vrijwel identiek aan de definitie van Peano gebruikt in onderzoek binnen de getaltheorie. In eerste instantie bleef het blang van een formalisering van rekenkunde binnen de gebieden van logica en getaltheorie. Later bleek dat er vanuit de logica veel verbanden gelegd kunnen worden met andere vakgebieden. Mede daardoor werd in de jaren veertig en vijftig van de vorige eeuw een basis gelegd voor een nieuw soort formalisering van rekenkunde. Deze nieuwe formaliseringen zijn gebaseerd op de axioma's van Peano, maar gebruiken slechts een beperkte vorm van inductie. De bewijsbaarheid van bepaalde stellingen binnen deze zwakkere theorieën hangt nauw samen met grote wiskundige problemen in andere vakgebieden, zoals bijvoorbeeld het P=NP-probleem.

In deze scriptie behandelen we het bewijs van enkele resultaten over het bewijs van zekere stellingen in een zwakkere theorie van de rekenkunde. Specifiek bekijken we de theorie van begrensde inductie, genaamd $I\Delta_0$. We volgen hierbij het materiaal dat wordt gepresenteerd in [1].

In sectie 2 bekijken we eerst een introductie tot zwakkere systemen van de rekenkunde. Er zullen enkele resultaten behandeld worden waarmee in een meer of mindere mate wordt aangegeven wat de sterkte is van deze theorieën. Daarnaast wordt er enkele notatie geïntroduceerd die in de secties daarna gebruikt zal worden. In sectie 3 zullen we laten zien dat onder bepaalde voorwaarden in $I\Delta_0$ een zwakkere vorm van het duiventilprincipe kan worden bewezen. We zullen ook zien dat dit probleem samenhangt met de vraag of $I\Delta_0$ eindig axiomatiseerbaar is. In sectie 4 wordt voortgebouwd op de resultaten van sectie 3 om te bewijzen dat onder vergelijkbare voorwaarden bewezen kan worden dat de verzameling priemgetallen cofinaal is. In sectie 5 wordt dan nog kort behandeld welke resultaten er zijn behaald met betrekking tot deze problemen nadat deze bron verschenen is.

Enige bekendheid met basisprincipes van modeltheorie is gewenst. Concepten zoals modellen, niet-standaard elementen van een model en andere basistermen met betrekking tot de eerste-orde logica worden bekend geacht te zijn.

2 Voorkennis

In deze sectie behandelen we enkele principes die zullen worden gebruikt in het hoofdgedeelte van deze scriptie. Allereerst wordt er een inleiding gegeven tot verschillende theorieën van rekenkunde, samen met enkele stellingen die bewezen kunnen worden in deze theorieën. Veel van deze informatie is terug te vinden in [2]. Daarna wordt enkele notatie gegeven die in het vervolg van deze scriptie gebruikt zal worden.

2.1 Een inleiding tot zwakkere theorieën

Algemene principes

Laat $L_0 = \{0, 1, +, \cdot, \leq\}$ de eerste-orde taal van de rekenkunde zijn[1]. Aan de hand van deze taal kunnen we de *theorie van Peano rekenkunde* opstellen. Peano rekenkunde is opgebouwd uit de volgende axioma's:

Definitie 2.1.

$$\neg(x + 1 = 0) \tag{1}$$
$$x + 1 = y + 1 \Rightarrow x = y \tag{2}$$
$$\neg(x = 0) \Rightarrow \exists y(x = y + 1) \tag{3}$$
$$x + 0 = x \tag{4}$$
$$x + (y + 1) = (x + y) + 1 \tag{5}$$
$$x \cdot 0 = 0 \tag{6}$$
$$x \cdot (y + 1) = (x \cdot y) + x \tag{7}$$
$$x \leq y \Leftrightarrow \exists z(z + x = y) \tag{8}$$

De axioma's van Peano rekenkunde kunnen verkregen worden door toevoeging van het volgende axiomaschema, waarbij er voor iedere formule $\phi(\vec{u}, x)$ er een axioma is van de volgende vorm:

$$(\phi(\vec{u}, 0) \wedge \forall x(\phi(\vec{u}, x) \Rightarrow \phi(\vec{u}, x + 1))) \Rightarrow \forall x\phi(\vec{u}, x)$$

Dit is de rekenkunde zoals de meesten gewend zijn. Voor veel stellingen uit de rekenkunde geldt echter dat het inductieschema niet ten volle gebruikt hoeft te worden. Het zou volstaan om een slechts een bepaalde klasse formules in het inductieschema op te nemen. Door een verzwakte versie van het indutieschema te gebruiken in plaats van het volledige schema, zijn er modellen te vormen die zich anders gedragen dan de modellen van Peano rekenkunde, maar waarin wel nog allerlei eigenschappen van de natuurlijke getallen te bewijzen zijn.

Voordat we een aantal van deze zwakkere theorieën en hun eigenschappen bekijken, geven we eerst de volgende definities, die zullen helpen bij het definiëren van deze theorieën.

[1] In sommige teksten zal de constante 1 zijn vervangen door het eenplaatsige functiesymbool S, waarbij $S(x)$ equivalent is aan $x + 1$. Voor het overzicht gebruiken we echter deze taal.

Definitie 2.2. Een *begrensde* kwantor is een kwantor van de vorm $\exists x : (x \leq y \wedge \phi)$ of van de vorm $\forall x : ((x \leq y) \Rightarrow \phi)$. Deze zullen in het vervolg afgekort worden door $\exists x \leq y : \phi$ respectievelijk $\forall x \leq y : \phi$. Een forumle is begrensd dan en slechts dan als alle kwantoren die in deze formule voorkomen begrensd zijn.

Met behulp van het concept van begrensde formules kunnen we een zekere hiërarchie opstellen op formules, die als volgt wordt gedefineerd:

Definitie 2.3. Laat de *rekenkundige hiërarchie* als volgt gedefinieerd zijn:

- $\Sigma_0 = \Pi_0 = \Delta_0 =$ de begrensde formules.
- Σ_{n+1} zijn de formules van de vorm $\exists \vec{x} \phi$ waarbij $\phi \in \Pi_n$.
- Π_{n+1} zijn de formules van de vorm $\forall \vec{x} \phi$ waarbij $\phi \in \Sigma_n$.

Dus een formule in Σ_n heeft de vorm van een begrensde formule voorafgegaan door n onbegrensde kwantoren, waarvan de eerste existentieel is, die afwisselend existentieel en universeel zijn.

We bekijken nu enkele theorieën die zwakker zijn dan Peano rekenkunde.

Open inductie

De theorie van open inductie, in het vervolg aangegeven met I_{open}, bestaat uit de acht axioma's van Definitie 2.1 plus het inductieschema voor open formules, dat wil zeggen, kwantorvrije formules. Ondanks dat dit inductieschema haast marginaal aandoet tegenover het complete schema, is er toch veel te bewijzen in I_{open}. Het is onder andere te bewijzen dat optelling en vermenigvuldiging commutatief en associatief zijn. Ook is het mogelijk om het volgende te bewijzen:

Stelling 2.4. *In I_{open} is het volgende te bewijzen:*

$$x \leq y \wedge y \leq z \Rightarrow x \leq z$$
$$x \leq y \wedge y \leq x \Rightarrow x = y$$
$$x \leq y \vee y \leq z$$

Dus alleen al in I_{open} kan je bewijzen dat het relatiesymbool $\leq$ een discrete lineaire ordening is, met kleinste element 0. Zo zijn er nog meer elementaire eigenschappen van de natuurlijke getallen die al in I_{open} te bewijzen zijn.

Deze theorie heeft echter ook zijn zwakke punten. Het is bijvoorbeeld in [3] bewezen dat dat er modellen zijn van I_{open} waarin de verzamling van priemgetallen niet cofinaal is. In zo'n model is er dus een x te vinden zodat $\forall p : (p \text{ priem } \Rightarrow p \leq x)$. Ook is het mogelijk om modellen te vinden zodat er een oneven priemgetal is dat geen niet-kwadraatrest heeft. Zo zijn er nog meer eigenschappen die onafhankelijk zijn van I_{open}, waarvan het vervelend is dat je ze niet uit kan sluiten.

Het is onder meer door die reden dat I_{open} niet vaak beschouwd wordt in de zoektocht van bewijsbaarheid van bepaalde stellingen, omdat het in deze redelijk eenvoudige gevallen al aangetoond kan

worden dat iets niet bewezen kan worden.

$I\Delta_0$

De theorie van $I\Delta_0$ bestaat, zoals de naam al doet vermoeden, uit de acht axioma's van Definitie 2.1 en het inductieschema voor formules die Δ_0 zijn, of met andere woorden, begrensd zijn. Deze theorie zal het hoofdonderwerp van deze scriptie zijn.

In $I\Delta_0$ is het mogelijk om al meer wiskundige concepten te definiëren en te bewijzen, zoals het volgende principe:

Stelling 2.5. *$I\Delta_0$ bewijst het* least number principle*; dat wil zeggen: voor elke $\phi \in \Delta_0$ geldt in $I\Delta_0$ dat:*

$$(\exists x : \phi(x)) \Rightarrow \exists x : (\phi(x) \wedge \forall y < x : \neg\phi(y))$$

Bewijs. We gebruiken tegenspraak. Stel dat er een x is waarvoor het gevraagde niet geldt, ofwel gezegd dat geldt dat:

$$(+) \quad (\exists x : \phi(x)) \wedge \forall x(\phi(x) \Rightarrow (\exists y < x : \phi(y))$$

We gebruiken nu inductie op de begrensde formule $\psi(x) = \forall y < x : \neg\phi(y)$ om een tegenspraak af te leiden. Het geval $\psi(0)$ is triviaal en dus waar. Stel nu dus dat $\psi(x)$ geldt. We bekijken $\psi(x+1)$. Er zijn nu twee mogelijkheden: ofwel $\phi(x)$, ofwel $\neg\phi(x)$. Als geldt dat $\phi(x)$ klopt, dan kunnen we $(+)$ gebruiken, en die beweert dat $\phi(x) \Rightarrow \exists y < x : \phi(y)$. We weten echter uit de inductiehypothese dat $\forall y < x : \neg\phi(y)$, dus aannemen dat $\phi(x)$ geldt leidt tot een tegenspraak. Dus we concluderen dat $\neg\phi(x)$. In dat geval geldt duidelijk dat $\forall y < x + 1 : \neg\phi(y)$, dus $\psi(x + 1)$ is waar. Met $I\Delta_0$ concluderen we dat $\forall x \forall y < x : \neg\phi(y)$. In het bijzonder geldt dan dat $\neg\exists x\phi(x)$. Dit is echter ook in tegenspraak met $(+)$. We concluderen dat $(+)$ niet waar kan zijn, dus het gevraagde volgt. ❑

Dit principe is niet te bewijzen in I_{open}. Aan de hand van het least number principle kunnen weer allerhande concepten worden gedefinieerd. Er bestaat dankzij dit principe bijvoorbeeld een Δ_0-definitie van de grootste gemene deler:

Definitie 2.6. Stel dat $x \neq 0, y \neq 0$. Dan geldt dat $\text{ggd}(x, y) = u$ dan en slechts dan wanneer u maximaal is in de eigenschap dat $u|x$ en $u|y$. Als $x = 0 \vee y = 0$, dan is $\text{ggd}(x, y) = 0$.

Uit het least number principle volgt dat $\text{ggd}(x, y)$ bestaat. Bekijk namelijk de volgende Δ_0-formule:

$$\chi(u) = \forall v \leq \min(x, y) : (u + 1 \leq v \Rightarrow \neg(v|x \wedge v|y))$$

Dan is voldoet $z = \min(x, y)$, dus met het least number principle geldt dat $\exists u : (\chi(u) \wedge \forall y < u : \neg\chi(y)$. Uit $\chi(u)$ volgt vervolgens dat deze u precies $\text{ggd}(x, y)$ is.

Een ander belangrijk concept wat in $I\Delta_0$ gedaan kan worden is, is het coderen van een begrensd rijtje door middel van een enkel getal. De formele definitie is complex en zal hier niet volledig behandeld worden. We geven wel enige intuïtie, aangezien het een vaak zal worden gebruikt in de komende bewijzen.

Heuristisch gezien is het concept van het coderen van rijtjes al deels bekend. Als we bijvoorbeeld een

rijtje van nullen en enen hebben, dan kunnen we dit beschouwen als een getal in het binair stelsel en dit "coderen"door middel van een getal in het tientallig stelsel. Het rijtje 011010 bijvoorbeeld wordt gecodeerd door het getal 26. Merk op dat voor een binair rijtje van lengte b de codering altijd een getal is dat kleiner is dan 2^b. Zo geldt in het algmeen dat een rijtje met b elementen die allemaal kleiner zijn dan een getal a gecodeerd kan worden door een getal kleiner dan $(a+1)^b$. De getallen b en a kunnen willekeurig groot worden, waarbij voor a zelfs geldt dat deze niet-standaard kan zijn. Het formele proces doet iets vergelijkbaars en kan volledig met Δ_0-formules worden geformaliseerd. Het voordeel hiervan is dat functies aan de hand van zo'n begrensd rijtje uniform gedefinieerd kunnen worden in hun variabelen.

In het hoofdgedeelte van deze scriptie zal een rijtje e_i van lengte $b+1$ met termen die alle kleiner zijn dan a aangegeven worden door $\exists$ rijtje $e_0, e_1, \ldots, e_b < a$. Als we willen verwijzen naar het daadwerkelijke getal waarmee een rijtje wordt gecodeerd, dan gebruiken we de notatie van de *code of sequences*: $\langle e_0, e_1, \ldots, e_b \rangle$. Dit concept van de code of sequences is origineel alleen gedefinieerd op rijtjes van natuurlijke getallen, maar werkt ook op andere aftelbare verzamelingen, zie bijvoorbeeld [6].

We zien ook echter dat $I\Delta_0$ tekortkomingen heeft. Om dit duidelijk te maken, wordt nu een definitie gegeven met daarchter een stelling, waarvan het bewijs te vinden is in [4].

Definitie 2.7. Laat T een theorie zijn die op zijn minst de acht axioma's van Definitie 2.1 bevat. Een formule $I(x)$ heet een *T-snede* als T de volgende dingen bewijst: $I(0)$, $\forall x : I(x) \Rightarrow I(x+1)$ en $\forall x \forall y : (y < x \wedge I(x) \Rightarrow I(y))$. Bovendien heet $I(x)$ *strikt* als T niet bewijst dat $\forall x : I(x)$.

Stelling 2.8. *Stel dat $I\Delta_0 \in T$. Als nu voor een T-snede $J(x)$ van een model M geldt dat deze gesloten is onder optellen en vermenigvuldigen, dan geldt dat $\{x \in M | M \models J(x)\} \models I\Delta_0$.*

Gevolg 2.9. *Zij een niet-standaard model M van Peano rekenkunde gegeven en laat a een niet-standaard element zijn. Bekijk de formule $I(x) = \exists n : x < a^n$. Dan is $I(x)$ duidelijk een T-snede. Aangezien hij ook gesloten is onder optellen en vermenigvuldigen, geldt dat $\{x \in M | M \models I(x)\} \models I\Delta_0$. Er geldt echter dat $a^a \notin \{x \in M | M \models I(x)\}$, dus deze verzameling is niet gesloten onder machtsverheffen.*

Er bestaan dus modellen van $I\Delta_0$ die niet gesloten zijn onder machtsverheffen. Dit heeft als gevolg dat de zin $\forall x \forall y \exists z : x^y = z$ niet bewezen kan worden in $I\Delta_0$. De functie is dus niet totaal. Wat echter wel bewezen kan worden, is dat er Δ_0-formule $\exp(x, y, z)$ bestaat met de volgende eigenschappen:

$$\exp(x, y, z_1) \wedge \exp(x, y, z_2) \Rightarrow z_1 = z_2$$

$$\exp(x, 0, 1)$$

$$\exp(x, y, z) \Rightarrow \exp(x, y+1, xz)$$

$$\exp(x, y, z) \wedge y' < y \Rightarrow \exists z' \exp(x, y', z')$$

Dus er kan binnen $I\Delta_0$ gesproken worden over machtsverheffen, en deze definitie voldoet aan redelijke eigenschappen die je zou verwachten bij machtsverheffen. De expliciete constructie van de functie exp is uitvoerig beschreven in [5]. Wat daarbij belangrijk is, is dat alleen gebruik wordt gemaakt van $\cdot$ en $+$.

Wat we echter wel kunnen bewijzen, is dat er een totale functie bestaat alle gewenste eigenschappen heeft van de logaritme. Dat wil zeggen dat er een functie is die voor iedere $x, z \in M$ de y geeft zodat y het grootste getal is dat voldoet aan de vergelijking $x^y \leq z$. Deze constructie staat ook beschreven in [2]. Als y het grootste getal is wat voldoet aan deze vergelijking, dan kunnen we zeggen dat $y = \lfloor \log_x(z) \rfloor$. In het vervolg zullen we spreken over $y = \log_x(z)$ in zulke gevallen, waarbij we in het achterhoofd houden dat we dit behandelen als een geheel getal.

$I\Delta_0 + \Delta_0$-duiventilprincipe

Het duiventilprincipe is een zeer fundamentele uitspraak binnen de wiskunde. Het stelt dat een functie die elementen van een verzameling naar een verzameing met strikt kleinere kardinaliteit stuurt niet injectief kan zijn. Formeel gedefinieerd is het duiventilprincipe het volgende schema, voor iedere formule $\theta(y, z)$:

$$\forall y \leq x+1 \exists z \leq x : \theta(y,z) \Rightarrow \exists y_1, y_2 \leq x+1 \exists z \leq x : (y_1 \neq y_2 \wedge \theta(y_1, z) \wedge \theta(y_2, z))$$

Hier dient de functie $\theta(y, z)$ dus gezien te worden als een functie die, heuristisch gezien, $x + 1$ duiven in x hokjes moet stoppen, waarbij er dus altijd in ten minste een enkel hokje twee duiven zitten. Als dit schema alleen beschouwd wordt voor $\theta(y, z) \in \Delta_0$, dan wordt gesproken over het Δ_0-duiventilprincipe.

Er bestaan ook zwakkere versies van het duiventilprincipe. De grenzen $x+1$ en x kunnen veranderd worden om zo minder sterke varianten te maken. Als de grenzen veranderd zijn in bijvoorbeeld m en n, dan zullen we daarnaar refereren als *het (Δ_0-)duiventilpricipe voor m en n.*

Het is onbekend of het Δ_0-duiventilprincipe bewezen kan worden in $I\Delta_0$. Het beste resultaat dat is behaald is dat het Δ_0-duiventilpricipe voor $\log_2(z)^k + 1$ en $\log_2(z)^k$ voor $k \in \mathbb{N}$. Dat wil dus zeggen dat voor $\theta(y, z) \in \Delta_0$ het volgende bewezen kan worden in $I\Delta_0$:

$$\forall y \leq \log_2(x)^k+1 \exists z \leq \log_2(x)^k : \theta(y,z) \Rightarrow \exists y_1, y_2 \leq \log_2(x)^k+1 \exists z \leq \log_2(x)^k : (y_1 \neq y_2 \wedge \theta(y_1, z) \wedge \theta(y_2, z))$$

$I\Delta_0 + \Delta_0$-duiventilprincipe is echter wel een sterke theorie. Het is bijvoorbeeld, onder andere, bewezen in [7] dat het volgende geldt:

Stelling 2.10.

$$I\Delta_0 + \Delta_0\text{-}\textit{duiventilprincipe} \vdash \forall x \exists y > x : (y \textit{ is priem})$$

Dus de cofinaliteit van de priemgetallen volgt al uit het aannemen van het Δ_0-duiventilprincipe. In het vervolg van deze scriptie zullen we laten zien dat een zwakkere versie van het Δ_0-duiventilprincipe al voldoet om de cofinaliteit te bewijzen en dat deze zwakkere variant ook bewezen kan worden in $I\Delta_0$, mits je nog een extra voorwaarde aanneemt.

2.2 Notatie en conventies

Voordat we deze bewijzen gaan behandelen, introduceren we eerst notatie die we in het vervolg van deze scriptie zullen gebruiken.

- Stel dat voor een model M van een bepaalde theorie geldt dat $a, b \in M$. De notatie $F : a \to b$ zal gebruikt worden om aan te geven dat de functie F getallen kleiner dan a stuurt naar getallen kleiner dan b. Formeler gezegd is het domein van F alle elementen x zodat $x < a$ en het beeld alle elementen y zodat $y < b$.
- We zullen ook de notatie $F : a \rightarrowtail b$ gebruiken als geldt dat F een injectieve functie is. In het bijzonder zal het duiventilprincipe ook wel als volgt aangegeven worden:

  $$\neg\exists x : (F : x + 1 \rightarrowtail x)$$

  Op een vergelijkbare manier kunnen ook de zwakkere varianten van het duiventilprincipe genoteerd worden.
- Voor een model M van Δ_0 zeggen we van een bepaalde subset $X \subseteq M$ dat $X \in \Delta_0^M$ wanneer deze gedefinieerd kan worden door een Δ_0-formule met parameters uit M. Hetzelfde kunnen we zeggen over functies, met als extra voorwaarde dat de definitie van deze functies uniform moet zijn in de parameters.
- Voor subsets $X \subseteq M$ geldt ook de volgende notatie:

  $$X \subseteq a \Leftrightarrow \forall x \in X : x < a$$

- In het vervolg van deze scriptie zijn alle logaritmes die voorkomen van het grondtal 2. We zullen ze zonder grondtal noteren als $\log(x)$.
- In deze scriptie zullen termen zoals $(1 + \epsilon)x$, waarbij ϵ een breuk is. Net als bij $\log(x)$ zal hiermee bedoeld worden dat wordt gekeken naar $\lfloor(1 + \epsilon)x\rfloor$.
- Modellen van $I\Delta_0$ zullen aftelbaar groot zijn, tenzij expliciet anders vermeld.
- Wanneer in het vervolg gerefereerd wordt naar het duiventilprincipe, zal daarmee het Δ_0-duiventilprincipe bedoeld worden, tenzij expliciet anders vermeld.

3 Het duiventilprincipe

In deze sectie zullen we beginnen met het bewijzen van de resultaten. We volgen hierbij [1]. In deze sectie behandelen we eerst de resultaten met betrekking tot het duiventilprincipe. Voor het verschijnen van eerdergenoemd artikel werd vooral gekeken naar varianten van het duiventilprincipe voor $m+1$ en m, voor een zekere m. Er zijn echter betere resultaten te behalen wanneer het verschil tussen de twee waardes wordt vergroot. In de volgende stelling wordt bewezen dat uit de voorwaarde dat voor een gegeven x binnen een model $x^{\log^k(x)}$ bestaat voor een $k \in \mathbb{N}$ meteen volgt dat het duiventilprincipe voor x^2 en x geldt.

Stelling 3.1. *Voor $k \in \mathbb{N}$ en $F \in \Delta_0$ geldt dat:*

$$I\Delta_0 \vdash \forall x(x^{\log^k(x)} \textit{ bestaat} \wedge x > 1 \Rightarrow \neg(F : x^2 \rightarrowtail x))$$

Bewijs. We bekijken eerst het geval dat $k = 1$. Dus de stelling die we nu bewijzen is:

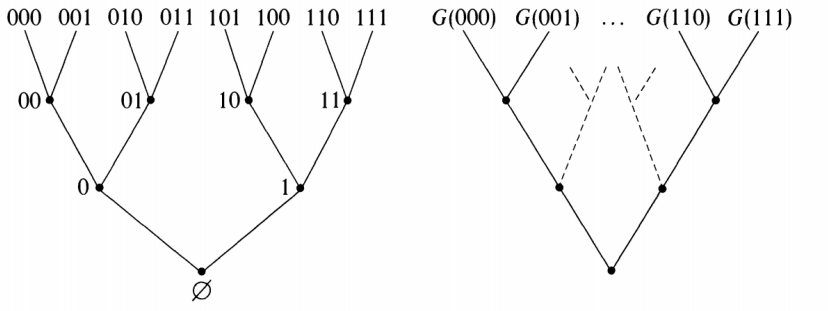
$$I\Delta_0 \vdash \forall x(x^{\log(x)} \text{ bestaat} \wedge x > 1 \rightarrow \neg(F : x^2 \rightarrowtail x))$$

Het idee van het bewijs is nu als volgt: we bekijken functies van 2^b naar a, met b zo gekozen dat $a^b \in M$, wat altijd kan voor $b = 1$. We definiëren dan aan de hand van F een klasse Δ_0-functies en laten dan vervolgens zien dat iedere functie van 2^b naar a gelijk moet zijn aan een van deze functies. Daarna laten we zien dat iedere functie uit deze klasse uniek kan worden geassocieerd met een getal $c < a$, maar dan kan met een diagonaalargument bewezen worden dat dit tot een tegenspraak leidt.

Merk op dat ieder getal kleiner dan $y < 2^b$ geschreven kan worden als een binair getal met b cijfers, eventueel aangevuld met nullen. We kunnen dus voor alle $x < b$ spreken over het x'de cijfer in de binaire expansie van y. Dit geven we vanaf nu aan met $\text{bin}_y(x)$.

Dus we nemen nu voor een willekeurige $a > 1$ aan dat $M \models a^{\log(a)}$ bestaat en dat er een injectieve functie $F : a^2 \rightarrowtail a$ bestaat met $F \in \Delta_0^M$. We gaan nu eerst laten zien hoe je de functies van 2^b naar a kan aftellen.

We bekijken, om wat intuïtie te krijgen bij dit bewijs,voor een gegeven functie $G : 2^b \rightarrow a$ eerst het volgende plaatje :



Figuur 1: Een binaire boom en zijn associatie voor $b = 3$.

Aangezien het domein van G de eerste 2^b elementen van M zijn, kan je deze elementen van het domein op de plek van de bladeren van een binaire boom neerzetten. De elementen zijn hier in binair opgeschreven. Wat we nu doen is dat we deze binaire boom gaan associëren met een andere boom waarin, in de plaats van alleen maar nullen en enen, waardes van F zijn ingevuld. Zo werken we de hele boom af, tot we onderaan op een waarde c terechtkomen die uniek is voor een gegeven G.

We handelen nu als volgt: we associëren de bladeren van deze boom met hun beeld onder G. Dat wil zeggen, we associëren 000 met $G(000)$ etc. Nu doen we iets vergelijkbaars voor de knopen eronder, maar nu gebruiken we ook de functie F. We associëren 00 met $F(G(000) + a \cdot G(001))$, en 01 met $F(G(010) + a \cdot G(011))$, tot we alles met twee cijfers hebben gehad. Zo doorredenerend associëren we 0 met $F(F(G(000) + a \cdot G(001)) + a \cdot F(G(010) + a \cdot G(011)))$ en 1 net zo. Uiteindelijk kunnen we dus $\varnothing$ associëren met een bepaalde waarde $c < a$. Er geldt echter dat deze uniek bepaald wordt door G, en vice versa, want F is een injectieve functie. Dit geeft dus dat je de functies van 2^b naar a kan aftellen, omdat het er minder dan a zijn.

We zullen nu deze redenering formeel maken voor een algemene b.

Voor een gegeven, vaste b, die zo is gekozen zodat $a^b \in M$, definiëren we nu voor $c < a$ en $d \leq b$ de functie $H_c^d : 2^d \to a$ zodat:

$$\begin{aligned} H_c^d(y) = r \Leftrightarrow & \exists \text{ rijtje } e_0, \ldots, e_d < a : e_0 = c \wedge e_d = r \\ & \wedge \forall 0 < i \leq d : (\mathrm{bin}_y(i-1) = 0 \to \exists x < a : F(e_i + ax) = e_{i-1}) \\ & \wedge \forall 0 < i \leq d : (\mathrm{bin}_y(i-1) = 1 \to \exists x < a : F(ae_i + x) = e_{i-1}) \end{aligned}$$

Merk op dat $F(e_i + ax)$ goed gedefinieerd is, aangezien uit $e_i < a$ en $x < a$ volgt dat $e_i + ax \leq a - 1 + a(a-1) = a - 1 + a^2 - a = a^2 - 1 < a^2$.

Deze definitie is het beste te begrijpen door te kijken hoe de functie zich gedraagt voor kleine d. Het geval $d = 0$ is niet bijster interessant, aangezien uit de definitie volgt dat $H_c^0(y) = r \Leftrightarrow c = r$. Dus bekijk $d = 1$. De verzameling 2^d bestaat dan uit de elementen 0 en 1, die toevallig gelijk zijn aan hun binaire expansie. Volgens de definitie van H_c^1 geldt nu dat

$$\mathrm{bin}_y(0) = 0 \Rightarrow \exists x < a : F(e_1 + ax) = F(r + ax) = e_0 = c,$$

En op eenzelfde manier geldt dat

$$\mathrm{bin}_y(0) = 1 \Rightarrow \exists x < a : F(ae_1 + x) = F(ar + x) = e_0 = c$$

Zo zien we dus dat de e_i vanaf e_d recursief van hoog naar laag worden gedefinieerd door de functie F totdat je bij e_0 uitkomt. We weten echter ook uit de aanname dat F een injectieve functie is, dus de waardes r van $H_c^b(y)$ bepalen op unieke wijze c en dat geldt ook andersom, juist doordat de functie recursief van boven wordt opgebouwd.

Aangezien we weten dat de grafiek van de exponentiële functie gedefinieerd kan worden in $I\Delta_0$ ([5]) en aangezien het rijtje $e_0, e_1, \ldots, e_d$ kan worden gecodeerd in het grondtal a door een getal $s < a^{d+1} \leq a^{b+1}$, volgt dat H_c^d een Δ_0 definitie in M die uniform is in a, c, d en F.

Nu we de functies H_c^d hebben gedefinieerd, kunnen we nu de volgende claim bewijzen:

Claim 1. *Voor iedere afbeelding $G : 2^b \to a$ is er een $c < a$ zodat $G = H_c^b$.*
Bewijs. We laten zien met inductie op $d \leq b$ dat geldt dat:

$$\forall y < 2^{b-d} \exists c < a \forall z < 2^d H_c^d(z) = G(y \frown z)$$

Hierbij is $y \frown z$ het getal dat je krijgt wanneer je de binaire expansies van y en z naast elkaar zet.

We beginnen met $d = 0$. Zij nu een $y < 2^b$ gegeven. Aangezien, zoals boven is laten zien, geldt dat $H_c^0(z) = r \Leftrightarrow c = r$, voldoet $c = G(y)$, want dan geldt $H_{G(y)}^0(0) = G(y)$.

Stel nu dat de claim geldt voor $d-1$, dus dat wil zeggen: zij een $y < 2^{b-d+1}$ gegeven, dan geldt dat daarvoor een $c < a$ zodat $\forall z < 2^{d-1} H_c^{d-1}(z) = G(y \frown z)$.

We kijken nu dus naar een gegeven $y' < 2^{b-d}$. Aangezien voor zowel $y' \frown 0$ en $y' \frown 1$ geldt dat ze kleiner zijn dan 2^{b-d+1}, voldoen ze aan de inductiehypothese en dus zijn er c_0 en c_1 zodat

$$\forall z < 2^{d-1} H_{c_0}^{d-1}(z) = G(y' \frown 0 \frown z),\ \forall z < 2^{d-1} H_{c_1}^{d-1}(z) = G(y' \frown 1 \frown z)$$

In dit geval geldt dat voor $c = F(c_0 + ac_1)$ geldt dat $H_c^d(z) = G(y' \frown z)$. We weten immers vanuit de inductiestap dat er een rijtje $e'_0, \ldots, e'_{d-1}$ bestaat dat aan de voorwaardes voldoet voor het geval van $d-1$. Het rijtje voor het geval van d zal nu dan als volgt zijn: $e_0 = F(c_0 + ac_1), e_1 = e'_0, \ldots, e_d = e'_{d-1}$.

Dit rijtje klopt met de definitie van H_c^d. Voor $1 < i \leq d$ hoeven we dat niet te controleren, want dit volgt uit de inductiehypothese. Dus stel $i = 1$. Als $\text{bin}_z(0) = 0$, dan is $e_1 = e'_0 = c_0$, dus stel $x = c_1 < a$, dan geldt dat $e_0 = F(c_0 + ac_1) = F(e_1 + ax)$. Dus de dit volgt uit de definitie van H_c^d. Het geval dat $\text{bin}_z(0) = 1$ is analoog en volgt dus ook.

Hiermee is met inductie het bewijs compleet. Neem nu dan $d = b$, dan volgt dat:

$$\exists c < a \forall z < 2^b H_c^b(z) = G(z)$$

Daarmee is de claim bewezen.

□

We stellen nu $b = 1 + \log(a)$ en gebruiken de claim.[2]. We weten nu dus dat iedere afbeelding $G : 2^{1+\log(a)} \to a$ uniek wordt gegeven door een $H_c^{1+\log(a)}$ die dus weer uniek wordt bepaald door c. Met andere woorden, er bestaat dus een surjectieve functie van c naar alle Δ_0^M afbeeldingen van $2^{1+\log(a)}$ naar a. Bekijk nu echter de volgende afbeelding die $y < 2^{1+\log(a)}$ stuurt naar ofwel 1, ofwel 0:

$$H(y) = \begin{cases} 1 & \text{als } H^{1+\log(a)}_{\min(y,a-1)}(y) = 0 \\ 0 & \text{als } H^{1+\log(a)}_{\min(y,a-1)}(y) > 0 \end{cases}$$

[2]Dit mag aangezien $a^{1+\log(a)} = a \cdot a^{\log(a)}$ en M is gesloten onder vermenigvuldigen, dus samen met de aanname dat $a^{\log(a)}$ bestaat, volgt dat $a^b \in M$.

Deze afbeelding H kan niet gelijk zijn aan een van de afbeeldingen $H_c^{1+\log(a)}$. Immers, H is niet gelijk aan $H_0^{1+\log(a)}$, want $H(0) = 0 \Leftrightarrow H_0^{1+\log(a)}(0) > 0$, en dit argument is te herhalen voor alle $c \leq a-1$. Dus uit de aannames die we hebben gedaan volgt een tegenspraak. Hieruit volgt nu dat er niet een functie F kan bestaan zoals deze is gedefinieerd. Dus dit bewijst het gevraagde voor $k = 1$.

Het bewijs voor $k = 2$ en hoger volgt op een gelijke wijze. De claim hierboven kan opnieuw bewezen worden voor $b = 2 + \log^2(a)$. Dit geeft ons een functie $H^{2+\log^2(a)}$ waarvoor voor $c < a$ geldt dat $H_c^{2+\log^2(a)}$ een aftelling is van alle afbeeldingen van $2^{2+\log^2(a)}$ naar a. En aangezien $2^{2+\log^2(a)} = 4 \cdot 2^{\log^2(a)} \geq 4\log(a) \geq \log(a) + 1$, is $H^{2+\log^2(a)}$ in het bijzonder ook een aftelling van alle afbeeldingen van $\log(a)+1$ naar a. We kunnen nu dezelfde methode van bewijzen gebruiken zoals we hebben gedaan voor $k = 1$, met een klein verschil: aangezien we niet meer kunnen aannemen dat $a^{\log(a)} \in M$ kunnen we het rijtje $e_0, e_1, \ldots, e_d$ niet meer coderen met een getal kleiner dan $a^{1+\log(a)}$, aangezien dit getal mogelijk niet meer gedefinieerd is in M. We kunnen dit rijtje wel op een andere manier coderen met behulp van $H^{2+\log^2(a)}$. Dit zorgt er in ieder geval voor dat de gebruikte functies Δ_0 blijven.

Voor $k = 3$ kan je dit proces twee keer toepassen, en zo volgt de rest van de natuurlijke getallen analoog. ❑

Uit de aanname dat $x^{\log^k(x)}$ maar voor een enkele $k \in \mathbb{N}$ hoeft te bestaan volgt dus al het gevraagde. Het is echter niet bekend of dit ook bewezen kan worden in $I\Delta_0$ voor een $k \in \mathbb{N}$. Nemen we echter aan dat $x^{\log(x)}$ bestaat voor alle $x \in M$ dan kunnen we nog iets veel sterkers bewijzen. Dit wordt in de volgende stelling bewezen.

Stelling 3.2. *Voor $F \in \Delta_0$ en een standaard rationaal getal $\epsilon > 0$ geldt:*

$$I\Delta_0 + \forall x(x^{\log(x)} \text{ bestaat}) \vdash \neg\exists x(F : (1+\epsilon)x \rightarrowtail x \wedge (1+\epsilon)x > x)$$

Bewijs. Allereerst merken we het volgende op: uit het bestaan van $F : (1+\epsilon)x \rightarrowtail x$ kan worden afgeleid dat er een F' bestaat zodat $F' : (1+\epsilon)x + \epsilon x \rightarrowtail (1+\epsilon)x$. Deze twee functies samengestellen geeft $F(F') : x + 2\epsilon x \rightarrowtail x$. Dus we kunnen ϵ twee keer zo groot maken en er is nog een functie die voldoet aan het gegeven. Ook geldt dat wanneer $\epsilon > 3$ en $(1+\epsilon)x > x$, dat $\epsilon = 3$ dan ook voldoet, we mogen voor F immers altijd ϵ kleiner maken, en dan geldt nog steeds dat $F : (1+\epsilon)x \rightarrowtail x$. Dus we kunnen zonder verlies van algemeenheid stellen dat $\epsilon = 3$. Dus in het vervolg van het bewijs dient eigenlijk het getal 4 gelezen te worden als $1 + \epsilon$.

We bekijken de volgende functie G. Uit het bestaan van deze G en het feit dat G een Δ_0-functie is construeren we een functie $G' : a^2 \rightarrowtail a$, en dat is met de vorige stelling een tegenspraak. De functie $G : a^2 \rightarrowtail a^2$ die we bekijken is de volgende:

$$G(4ab + c) = ab + F(c)$$

Hier geldt dat $0 \leq c < 4a$. Deze functie heeft een Δ_0-definitie, en wel de volgende:

$$G(x) = y \Leftrightarrow \forall b < a \forall c < 4a : (x = 4ab + c \Rightarrow y = ab + F(c))$$

Deze functie lijkt een merkwaardige vorm van invoer te hebben, maar dit is slechts schijn. Ieder

getal $x < a^2$ kan bekeken worden modulo $4a$. Het getal wat daaruitkomt is de c die in de invoer staat aangegeven. Bekijk je dan $x - c$ dan is dat dus deelbaar door $4a$, en dus van de vorm $4a \cdot b$. Aangezien $4ab + c < a^2$ moet gelden dat $b < a$, dus daaruit volgt dat $ab + F(c) < a(a-1) + a = a^2$. Ook geldt dat ieder getal een unieke decompositie heeft modulo $4a$ en daarbij hoort ook een unieke decompositie modulo a, en dit is wat er gebeurt in het beeld van G; wat G feitelijk doet, is de decompositie van een getal omzetten van modulo $4a$ naar modulo a.

In het bijzonder geldt op deze manier dat $G(x) < a$ als $x < 4a$, want dan geldt $b = 0$ en $F(c) < a$. Voor $x \geq 4a$ geldt dus dat $b \geq 1$, dus er geldt dat:

$$G(x) = G(4ab + c) = ab + F(c) < ab + a \leq ab + ab = 2ab$$

Dus voor $x \geq 4a$ geldt dat $G(x) < x/2$. Dus geldt ook dat $G^2(x) < x/2^2$ als x voldoende groot is. Dit leidt tot de volgende conclusie:

$$G^{\log(a)+1} : a^2 \rightarrowtail \max(4a, a^2/2^{\log(a)+1}) \leq 4a,$$

want $a^2/2^{\log(a)+1} \leq a^2/2a = a/2$. Dus er volgt dat $G^{\log(a)+2} : a^2 \rightarrowtail a$. Nu moet alleen nog gelden dat $G^{\log(a)+2}$ een Δ_0-definitie heeft. De functie G zelf heeft een Δ_0-definitie en deze definitie is uniform in a, b, c en F. De definitie van $G^{\log(a)+2}$ wordt dan als volgt:

$$\begin{aligned} G^{\log(a)+2}(x) = y \Leftrightarrow &\exists \text{ rijtje } e_0, e_1, \ldots, e_{\log(a)+2} < a^2 : e_0 = x \wedge e_{\log(a)+2} = y \\ &\wedge \forall 0 < i \leq \log(a) + 2 : [G(e_{i-1}) = e_i] \end{aligned}$$

Dit rijtje kan worden gecodeerd door een getal kleiner dan $(a^2)^{\log(a)+1}$, en wegens het bestaan van $a^{\log(a)}$ middels de voorwaarde, geldt dat $G^{\log(a)+2}$ een Δ_0-definitie heeft, en zo volgt de tegenspraak door middel van de vorige stelling, dus de functie F kan niet bestaan. ❑

De voorwaarde $\forall x(x^{\log(x)}$ bestaat) is een sterke voorwaarde. Het is onderhand bekend dat deze voorwaarde afgezwakt kan worden; zie daarvoor sectie 5.1. Wat ook bewezen kan worden, is dat deze voorwaarde in Stelling 3.1 overbodig is als je aaneemt dat $I\Delta_0$ kan worden beschreven door middel van eindig veel axioma's. Het is nog een open probleem of $I\Delta_0$ daadwerkelijk eindig axiomatiseerbaar is. Deelresultaten voor dit probleem zijn te vinden in sectie 5.2. Het zou in ieder geval als gevolg hebben dat enkele stellingen bewezen kunnen worden onafhankelijk van het bestaan van $x^{\log(x)}$. De zojuist geformuleerde stelling zal verderop worden bewezen als Stelling 3.6. Voor dat bewijs hebben we echter enkele tussenresultaten nodig. De eerste daarvan is de volgende:

Stelling 3.3. *Stel dat $a^\gamma \in M$ en $F \in \Delta_0^M$ zodat $F : a^\gamma \rightarrowtail a$. Dan bestaat er een eindextensie K van M (aangegeven met $K \supseteq_e M$) zodat $K \models I\Delta_0$ en $a^{\gamma^2} \in K$.*
Bewijs. We mogen uiteraard aannemen dat $a^{\gamma^2} \notin M$.

We werken nu eerst als in Stelling 3.1 om op vergelijkbare manier een functie H te vinden zodat er een aftelling H_c bestaat voor $c < a$ zodat deze aftelling alle Δ_0^M afbeeldingen van 2^γ naar a aftelt. We gebruiken deze functies nu als volgt: we kunnen alle getallen kleiner dan a^{2^γ} omschrijven naar het grondtal a en daarvoor geldt dan dat er 2^γ coëfficienten zijn die allemaal kleiner zijn dan a. We kunnen dus de H_c zien als een vorm van coëfficientsfuncties en dus de c zelf indentificeren met het getal $\sum_{i<2^\gamma} H_c(i) \cdot a^i$. We kunnen nu dus ook een andere definitie van optellen en vermenigvuldigen

geven aan de hand van deze functies H_c. Deze definities zullen er als volgt uitzien:

$$\begin{aligned} c \oplus d = e \Leftrightarrow & \exists y < a \forall i < 2^\gamma : H_y(0) = 0 \\ & \wedge i + 1 < 2^\gamma \rightarrow H_y(i) + H_c(i) + H_d(i) = H_e(i) + a \cdot H_y(i+1) \\ & \wedge i + 1 = 2^\gamma \rightarrow H_y(i) + H_c(i) + H_d(i) = H_e(i) \end{aligned}$$

Deze definitie lijkt mogelijk verwarrend, maar feitelijk verschilt deze niet zoveel van optellen zoals we dat gewend zijn. De functie $H_y(i)$ die hier opduikt is een functie die in zekere zin het "één onthouden-principe weergeeft. Zodra $H_c(i) + H_d(i)$ groter wordt dan a, dan moet je als het ware één onthouden en die optellen bij het volgende a-tal. Bijvoorbeeld bij het berekenen van 15+16 in het 10-tallig stelsel. In zekere zin geldt nu dat 5+6=1+10·1. Deze 1 die we nu hebben onthouden komt weer terug als we de tientallen bij elkaar optellen: 1+1+1=3. Dus zo krijg je 15+16=31. Dit principe wordt hier formeel gedefinieerd voor andere grondtallen. Merk op dat de laatste regel in deze definitie noodzakelijk is om ervoor te zorgen dat $i = 2^\gamma$ niet nodig is.

Voordat we kijken naar de vervangende definitie van vermenigvuldigen, bekijken we eerst de volgende hulpdefinitie, die aangeeft dat e de som is van qa^j kopieën van c:

$$\begin{aligned} q_j^* c = e \Leftrightarrow & \exists y < a \forall i < 2^\gamma : i < j \rightarrow H_y(i) = H_e(i) = 0 \\ & \wedge j < i + 1 < 2^\gamma \rightarrow H_y(i) + q \cdot H_c(i - j) = H_e(i) + a \cdot H_y(i+1) \\ & \wedge j < i + 1 = 2^\gamma \rightarrow H_y(i) + q \cdot H_c(i - j) = H_e(i) \\ & \wedge 2^\gamma - j < i < 2^\gamma \rightarrow H_c(i) = 0 \wedge q = 0 \end{aligned}$$

Deze definitie heeft, niet geheel verrassend, iets weg van de definitie van $\oplus$. Merk vooral op dat de eerste regel aangeeft dat de expansie van e op minstens $j - 1$ nullen eindigt. De tweede en derde regel zijn vergelijkbaar met de definitie van optellen. De laatste regel zorgt ervoor dat het resultaat wederom niet te groot wordt.

Aan de hand van deze definitie kunnen we nu de vervangende definitie van vermenigvuldigen geven:

$$\begin{aligned} c \otimes d = e \Leftrightarrow & \exists y < a \forall i < 2^\gamma : H_y(0) = H_c(0)_0^* d \wedge e = H_y(2^\gamma - 1) \\ & \wedge i + 1 < 2^\gamma \rightarrow H_y(i+1) = H_y(i) \oplus H_c(i)_i^* d \end{aligned}$$

Wat er hier feitelijk gebeurt, dus dat er wordt gezegd dat $c \otimes d = \sum_{i<2^\gamma} H_c(i)_i^* d$.

We bekijken nu een verzamling I zodat $\gamma^2 \in I$, $I \subseteq_e 2^\gamma$ en zodat I gesloten is onder optelling. Gegeven zo'n I stellen we nu K gelijk aan:

$$\{c < a | \exists t \in I \forall i < 2^\gamma : (t < i \Rightarrow H_c(i) = 0)\}$$

Dan geldt dat K gesloten is onder $\oplus$ en $\otimes$. Zij bijvoorbeeld $c \in K$ en $d \in K$ gegeven en stel dat $c \oplus d = e$. Dan geldt dus dat

$$\exists t_1 \in I \exists t_2 \in I : \forall i < 2^\gamma (t_1 < i \Rightarrow H_c(i) = 0 \wedge t_2 < i \Rightarrow H_d(i) = 0)$$

Dan geldt dat $\max(t_1, t_2) < i \Rightarrow H_c(i) = H_d(i) = 0$. Wegens de definitie van $\oplus$ volgt nu dat voor $i > \max(t_1, t_2) + 1$ geldt dat[3] $H_e(i) = 0$. Dus daaruit volgt dat $e \in K$. Voor vermenigvuldigen geldt eenzelfde redenering.

Wat ook volgt uit de definitie van K en $\oplus$ is dat voor $d \in K$ geldt dat $c \trianglelefteq d \Rightarrow c \in K$ waarbij $c \trianglelefteq d \Leftrightarrow \exists e < a : c \oplus e = d$. Dit betekent dus dat we in K de reguliere symbolen $+, \cdot, \leq$ kunnen uitbreiden tot $\oplus, \otimes, \trianglelefteq$ en we kunnen stellen dat voor c en d in K geldt dat ze hetzelfde zijn als $H_c = H_d$. Door deze eenduidige interpretatie van de nieuwe symbolen volgt dat K in ieder geval voldoet aan de standaard axioma's van Peano, dat wil zeggen, de inductie-axioma's uitgezonderd. Ook geldt voor iedere $A \subset K$ die in Δ_0^K zit dat $A = K \cap B$ voor een $B \subset a$, $B \in \Delta_0^M$. Dit volgt uit het feit dat $\oplus, \otimes$ en $\trianglelefteq$ gedfinieerd zijn in Δ_0^M. Dus subsets van K zijn te identificeren met subsets van M, omdat iedere Δ_0-formule in K is opgebouwd met behulp van de nieuwe symbolen $\oplus, \otimes$ en $\trianglelefteq$. Met behulp van de volgende claim volgt nu dat $K \models I\Delta_0$:

Claim 2. *Zij een $a \in M$ gegeven en stel dat $\lessdot \in \Delta_0$ een partiële ordening is op a en zij een niet lege subset $X \subseteq a$ gegeven, zodat $X \in \Delta_0^M$. Dan geldt dat X een minimaal element heeft met betrekking tot $\lessdot$.*
Bewijs. We laten met inductie op $i \leq \log(a) + 1$ de volgende uitspraak zien:

$$\exists j < 2^i (\forall y \in X \exists x \in X (ja/2^i \leq x < (j+1)a/2^i \wedge x \lessdot y))$$

$$\wedge \neg (\forall y \in X \exists x \in X (x < ja/2^i \wedge x \lessdot y))$$

Met andere woorden, er is een j zodat voor alle elementen y van X er een element x te vinden is tussen twee grenswaarden zodat $x \lessdot y$, maar er is ook een element y van X zodat voor alle elementen onder de onderste grenswaarde geldt dat ze niet te vergelijken zijn met $\lessdot$.

We stellen eerst $i = 0$. Dan is de te bewijzen claim:

$$\exists j < 1 (\forall y \in X \exists x \in X (\min(a, ja) \leq x < \min(a, (j+1)a) \wedge x \lessdot y))$$

$$\wedge \neg (\forall y \in X \exists x \in X (x < \min(a, ja) \wedge x \lessdot y))$$

Het is duidelijk dat $j = 0$ hier voldoet. Vullen we immers $j = 0$ in dan staat er:

$$\forall y \in X \exists x \in X (0 \leq x < a \wedge x \lessdot y)$$
$$\wedge \neg (\forall y \in X \exists x \in X (x < 0 \wedge x \lessdot y))$$

Aangezien er geen elementen van X kleiner kunnen zijn dan 0, kunnen we voor alle y een x kiezen, namelijk $x = y$. Dus de basisstap volgt hieruit.

Stel nu dat de stelling is bewezen voor een $i < \log(a) + 1$. Dat betekent dus dat er een j is die voldoet aan de stelling. We moeten nu dus op zoek gaan naar een j' zodat de stelling ook voldoet voor $i + 1$. Het zal blijken dat $j' = 2j$ voldoet.

[3] Voor $i = \max(t_1, t_2)$ hoeft dit nog niet te gelden, aangezien $H_y(i)$ dan nog niet gelijk nul hoeft te zijn, dus $H_e(i)$ ook niet.

Omdat geldt dat $j < 2^i$, geldt dat $j' < 2^{i+1}$. Dus j' is klein genoeg. Als nu kijken naar de grenzen van het interval, dan kunnen we in ieder geval het volgende opmerken over de ondergrens: die blijft hetzelfde. Immers, $j'a/2^{i+1} = 2ja/2^{i+1} = ja/2^i$.

Als we kijken naar de bovengrens, dan zien we dat deze omlaag gaat. Simpel uitrekenen geeft namelijk dat $(j'+1)a/2^{i+1} = (j+1)a/2^i - a/2^{i+1}$. Dit betekent dat er sowieso punten uit het interval vallen. Dat houdt dan weer in dat er mogelijk punten y zijn waarvoor in het oude interval (dus met j en niet met j') nog gold dat er een punt y' in het interval was zodat $y' \lessdot y$, maar waarvoor in het nieuwe interval nu geldt dat y' er niet meer in zit. Als nu echter geldt dat er geen enkele x überhaupt is zodat $x < y'$, dan is aan de claim voldaan, want dan is y' immers een minimaal element van X. Dus als zo'n x bestaat, dan zit x ofwel in het nieuwe interval, ofwel we kunnen hetzelfde argument herhalen. Zo gaan we dus door tot er een element x' is gevonden zodat $x' \lessdot y'$ en x' in het nieuwe interval zit.

Dankzij de redeneringen over de grenzen, volgt nu eenvoudig dat $j' = 2j$ voldoet aan de voorwaardes van de claim voor $i+1$.

Kies nu $i = \log(a) + 1$. Dan wordt de uitspraak nu als volgt:

$$\exists j < 2^{\log(a)+1}(\forall y \in X \exists x \in X(j/2 \leq x < (j+1)/2 \wedge x \lessdot y))$$
$$\wedge \neg(\forall y \in X \exists x \in X(x < j/2 \wedge x \lessdot y))$$

Er kan nu maar een enkele x tussen $j/2$ en $(j+1)/2$ zitten, dus dat moet nu wel volgens de uitspraak een minimaal element zijn van X. Dit bewijst de claim. ❑

We kunnen nu ook bewijzen dat, op een isomorfisme na, geldt dat $M \subset_e K$. Bekijk nu een $q \in M$. We kunnen deze q omzetten naar grondtal a, waardoor het van de vorm $\sum_{j=0}^{m} q_j a^j$ wordt. We weten dat $a^{\gamma^2} \notin M$, dus er geldt dat $m < \gamma^2$. Aangezien we I hadden gekozen zodat $\gamma^2 \in I$ geldt dus dat $m \in I$, dus is er nu een $c < a$ te vinden zodat

$$H_c(i) = \begin{cases} q_i & \text{als } i < m \\ 0 & \text{als } m \leq i < 2^\gamma \end{cases}$$

We kunnen nu dus q identificeren met c, en deze c zit per definitie in K, want we kunnen in de definitie van K altijd $t = \gamma^2$ kiezen. Deze afbeelding geeft dus een inbedding van M in K.

Dan moet als laatste nu nog aangetoond worden dat $a^{\gamma^2} \in K$. Dit kunnen we doen als volgt: als $a^{\gamma^2} \notin K$, dan kunnen we de procedure van dit bewijs herhalen. Immers voldoet K aan de voorwaarden van de stelling. Zo kunnen we een K^2 construeren. Dit kunnen we overaftelbaar vaak herhalen zodat er uiteindelijk een K^{ω_1} ontstaat. Dit de kleinst mogelijke overaftelbare eindextensie van M; dat wil zeggen dat ieder beginsegment van K^{ω_1} aftelbaar is. Dan volgt hieruit dat

$$K^{\omega_1} \models I\Delta_0 + \{\forall x < y \exists z \theta(x,y,z) \rightarrow \exists t \forall x < y \exists z < t \theta(x,y,z) | \theta \in \Delta_0\}$$

Immers, de verzameling $\{x | x < y\}$ is hoogstens aftelbaar, en aangezien we voor iedere x een bijbehorende z kunnen kiezen, z_x, geldt dus dat de verzamling z_x ook hoogstens aftelbaar is. Aangezien K^{ω_1} zelf overaftelbaar is, volgt daaruit dat er een t is die een bovengrens vormt voor

alle z_x. Dus daaruit volgt dat $K^{\omega_1} \models I\Delta_0 + \{\forall x < y \exists z \theta(x,y,z) \to \exists t \forall x < y \exists z < t \theta(x,y,z)\}$. Uit eerder bekende resultaten, zie bijvoorbeeld [8], volgt nu dat $K^{\omega_1} \models$ Peano-axioma's, dus dan geldt dat $a^{\gamma^2} \in K^\alpha$ voor een $\alpha < \omega_1$. ❑

We hebben dus nu bewezen dat gegeven dat a^γ in een model M zit, dat er dan een eindextensie is waarin a^{γ^2} zit. Op eenzelfde manier hadden we kunnen laten zien dat dit ook geldt voor $a^{2\gamma}$. Dus er is een eindextensie waar $a^{\gamma+\gamma}$ in zit en een eindextensie waar $a^{\gamma\cdot\gamma}$ in zit. Zoals al in de inleiding is gezegd, kunnen we machtsverheffen omschrijven met behulp van $+$ en $\cdot$, dus als we maar vaak genoeg eindxtensies nemen, komen we bij het volgende gevolg uit:

Gevolg 3.4. *Stel dat $a^\gamma \in M$, en stel dat er een $F \in \Delta_0$ is zodat $F : a^\gamma \rightarrowtail a$. Dan is er een eindextensie K van M zodat $K \models I\Delta_0$ en de verzameling $\{\delta | a^\delta \in K\}$ gesloten is onder machtsverheffen.*

Voordat we de hoofdstelling van dit hoofdstuk kunnen gaan bewijzen, hebben we eerst nog het volgende lemma nodig. Dit lemma sluit aan op de vorige stelling, en dat zullen we gebruiken in het bewijs van de hoofdstelling.

Lemma 3.5. *Zij $M \subset_e K$ en $K \models I\Delta_0$. Dan geldt dat*

$$M \models \{\forall x < y \exists z \theta(x,y,z) \to \exists t \forall x < y \exists z < t \theta(x,y,z) | \theta \in \Sigma_1\}$$

Bewijs. Merk op dat dit schema een ander schema is dan in de vorige stelling is langsgekomen. Hier gebruiken we formules in Σ_1 en niet in Δ_0.

We zetten eerst y op een vaste waarde, zeg a. Stel nu dus dat $M \models \forall x < a \exists z \theta(x,z)$, met $\theta(x,z)$ dus van de vorm $\exists \vec{u} \phi(x,z,\vec{u})$ met $\phi \in \Delta_0$. Aangezien K een eindextensie is van M is er een $b \in K$ zodat $M < b$.

Uit datzelfde feit volgt dat $M \prec_{\Delta_0} K$; dat wil zeggen dat voor $\phi \in \Delta_0$ geldt dat $M \models \phi \Leftrightarrow K \models \phi$. Dit volgt uit het feit dat M een substructuur is van K, dus sowieso geldt dit voor kwantorvrije formules. Voor formules met begrensde kwantoren met bovengrenzen in M geldt dat deze bovengrenzen ook gelden in K, omdat K een eindextensie is van M. Voor een bovengrens in M geldt dat alle elementen die eronder liggen zich hetzelfde gedragen in K als in M. Dat laatste wil zeggen dat het voor een Δ_0-formule ϕ gedefinieerd op M niet uitmaakt of deze werkt op alleen M of op het beginsegment van K dat isomorf is met M. De relaties tussen de beginelementen verandert niet, en er komen ook geen nieuwe elementen bij in het beginsegment.

Dit wetende, kunnen we afleiden dat $K \models \forall x < a \exists z < b \exists \vec{u} < b \phi(x,z,\vec{u})$, want deze zin is zeker waar in M. Stel nu, door middel van $I\Delta_0$, dat b' de kleinste b is waarvoor geldt dat $K \models \forall x < a \exists z < b \exists \vec{u} < b \phi(x,z,\vec{u})$. Er moet nu gelden dat $b' \in M$. Stel immers van niet, dan zou $K \models \forall x < a \exists z < b \exists \vec{u} < b \phi(x,z,\vec{u})$ ook waar zijn voor $b'-1$, want $b'-1$ er zou nu ook gelden dat $b'-1 > M$. Dus dan hadden we niet b' gekozen als kleinste waarde voor b. Dus $b' \in M$, en uit $M \prec_{\Delta_0} K$ volgt daarna dat $M \models \forall x < a \exists z < b' \exists \vec{u} < b' \phi(x,z,\vec{u})$. Dus we kunnen concluderen dat:

$$M \models \forall x < a \exists z \theta(x,z) \to \exists t \forall x < a \exists z < t \theta(x,z)$$

Daarmee is het lemma bewezen. ❑

Nu kunnen we dan eindelijk het hoofdbewijs geven van dit hoofdstuk:

Stelling 3.6. *Stel dat $I\Delta_0$ te axiomatiseren is in eindig veel axioma's, dan geldt voor $F \in \Delta_0$ dat*

$$I\Delta_0 \vdash \neg(\exists x > 1 F : x^2 \rightarrowtail x)$$

Bewijs. Gegeven $M_0 \models I\Delta_0$, stel dat er een $a \in M_0$ is zodat $a > 1$ en $F : a^2 \rightarrowtail a$. We mogen ervan uitgaan dat $a^\gamma \in M_0$, waarbij γ hier een niet-standaard getal is van de vorm 2^λ voor een bepaalde λ. Dit kunnen we doen door een constructie genaamd ultramacht toe te passen. Dit hier uitleggen schiet het doel van deze scriptie voorbij. Ook mogen we aannemen dat F maar een enkele parameter heeft, c, en dat deze begrensd wordt door a^γ.

We bekijken nu de substructuur M van M_0 met als domein $\{x \in M_0 | x < a^{n\gamma}, n \in \mathbb{N}\}$. Het volgt eenvoudig dat $M \models I\Delta_0$ en dat F zowel domein als beeld in M heeft. In M bekijken we nu de volgende functie $G : a^\gamma \rightarrowtail a^\gamma$ die een getal $b < a^\gamma$ van basis a^2 omzet naar een getal van basis a. Preciezer gezegd: zij een $b < a^\gamma$ gegeven en schrijf b in basis a^2 als $\sum_{i<2^{\lambda-1}} b_i a^{2i}$. Dan stellen we nu

$$G(b) = \sum_{i<2^{\lambda-1}} F(b(i))a^i$$

Merk op dat $G(b) < a^{\gamma/2}$. We stellen nu $H = G^\lambda$. Dan volgt direct dat $H : a^\gamma \rightarrowtail a$ en $H \in \Delta_0^M$, aangzien het rijtje $b, G(b), G^2(b), \ldots, G^\lambda(b)$ gecodeerd kan worden door een getal $\leq a^{2\gamma}$.

We bekijken nu de verzameling axioma's van $I\Delta_0$, samen met de volgende uitspraken: $H : a^\gamma \rightarrowtail a$, $\neg\exists x(x = a^{\gamma^2})$ en a^γ is a tot de macht γ. We mogen stellen dat dit bij elkaar k formules zijn, en die kunnen we allemaal in prenex-normaalvorm schrijven. Deze formules worden dan van de vorm:

$$\forall y_0 \exists x_1 < t_1 \forall y_1 < s_1 \cdots \exists x_m < t_m \forall y_m < s_m \psi_j(\vec{x}, \vec{y}, a, \gamma, c, a^\gamma), \quad j < k$$

We bekijken nu de volgende functie $\Omega(q)$ die gedefinieerd is op de natuurlijke getallen. Deze functie maakt gebruik van de *code of sequences*, zoals die benoemd is in de inleiding.

Stel dat q geschreven kan worden in de volgende vorm:

$$q = \langle 0, \langle j, e, u_1, \ldots, u_m, w_0, \ldots, w_m \rangle \rangle$$

Hier geldt dat $j \leq k$ en $1 \leq e \leq m$. In dit geval stellen we $\Omega(q)$ gelijk aan de kleinste x_e zodat geldt dat:

$$x_e < t'_e \wedge \forall y_e < s'_e \exists x_{e+1} < t'_{e+1} \cdots \exists x_m < t'_m \forall y_m < s'_m : \psi'_j$$

als deze x_e bestaat, en 0 anders. Hier geldt dat de ψ'_j uitgeschreven moet worden als:

$$\psi_j(\Omega(u_1), \ldots, \Omega(u_{e-1}), x_e, \ldots, x_m, \Omega(w_0), \ldots, \Omega(w_{e-1}), y_e, \ldots, y_m, a, \gamma, c, a^\gamma)$$

Verder doen we het volgede: als

$$\begin{aligned}
&q = \langle 1, u\rangle && \text{zet } \Omega(q) = 0\\
&q = \langle 2, u\rangle && \text{zet } \Omega(q) = 1\\
&q = \langle 3, u\rangle && \text{zet } \Omega(q) = a\\
&q = \langle 4, u\rangle && \text{zet } \Omega(q) = \gamma\\
&q = \langle 5, u\rangle && \text{zet } \Omega(q) = c\\
&q = \langle 6, u\rangle && \text{zet } \Omega(q) = a^{\gamma}\\
&q = \langle 7, \langle u_1, u_2\rangle\rangle && \text{zet } \Omega(q) = \Omega(u_1)\cdot\Omega(u_2)\\
&q = \langle 8, \langle u_1, u_2\rangle\rangle && \text{zet } \Omega(q) = \Omega(u_1)+\Omega(u_2)
\end{aligned}$$

Mocht q aan geen van deze voorwaardes voldoen, dan stellen we dat $\Omega(q) = 0$.

We stellen nu $J = \Omega(\mathbb{N})$, dat wil zeggen, J is het beeld van de functie Ω. Dan is J een substructuur van M. Immers, $1^J = 1^M$ en $0^J = 0^M$. Ook geldt voor $x, y \in J$ dat $x <_J y \Leftrightarrow x < y$. Ook is J gesloten onder vermenigvuldigen en optellen.

In het bijzonder geldt dat J een elementaire substructuur is als je kijkt naar de k zinnen die we eerder hebben gedefinieerd. Formeler opgeschreven, betekent dit voor $j < k$:

$$J \models \theta_j \Leftrightarrow M \models \theta_j$$

Dit volgt uit de stap voor $q = \langle 0, \langle \ldots\rangle\rangle$. Zodra voor de zin $\theta_j = \forall y_0 \theta'_j(y_0)$ geldt dat $M \models \theta_j(d)$, voor een willekeurige $d \in M$, geldt dat er een x_e bestaat, zodat $\Omega(q) = x_e$, waarbij geldt dat $q = \langle 0, \langle j, 1, u_1, \ldots, u_m, d, w_1, \ldots, w_m\rangle\rangle$. Hier zijn de $u_1, \ldots, u_m$ en de $w_1, \ldots, w_m$ willekeurig, maar er geldt wel dat $w_0 = d$. Dit geeft aan dat x_e hier als het ware als getuige optreedt van het feit dat θ'_j ook waar is in J als je voor y_0 een waarde uit M invult. Dus zo volgt dat $J \models \theta'_j(d)$, maar d was willekeurig, dus geldt ook dat $J \models \forall y_0 \theta'_j$, dus $J \models \theta_j$.

Zo volgt dus dat:

$$J \models I\Delta_0 + H : a^{\gamma} \rightarrowtail a + \neg\exists x(x = a^{\gamma^2})$$

Dus J voldoet aan de voorwaardes voor Stelling 3.3, dus J heeft een strikte eindextensie K zodat $J \subset_e K$ en $K \models I\Delta_0$. Nu voldoen J en K aan de voorwaarden van Lemma 3.5, en daaruit volgt dat

$$J \models \{\forall x < y \exists z \theta(x, y, z) \rightarrow \exists t \forall x < y \exists z < t \theta(x, y, z) | \theta \in \Sigma_1\}$$

We laten zien dat dit tot een tegenspraak leidt. Allereerst merken we op dat er een formule in Σ_1 is die aangeeft dat $\Omega(n) = x$, voor een zekere $n \in \mathbb{N}$. Deze formule is te lang om uit te schrijven, maar dat deze in Σ_1 zit, volgt uit het feit dat deze formule afhangt van een rijtje, maar dat dit rijtje niet begrensd kan worden, zoals in eerdere gevallen. Dat zorgt ervoor dat er een enkele onberensde existentiële kwantor in de formule zit. Ook volgt duidelijkerwijs dat $J \models \Omega(n) = x \Leftrightarrow M \models \Omega(n) = x$; de functie Ω werkt immers niet anders in J dan in M. Samen met het feit dat $a^{\gamma} \in J$ en het feit dat J gesloten is onder vermenigvuldigen, volgt dat:

$$J \models \forall x < a \exists b \exists n(b = a^{n\gamma} \wedge \Omega(n) = x)$$

Aangezien we weten dat a niet-standaard groot is, zijn er oneindig veel elementen van M die kleiner zijn dan a. Dit heeft tot gevolg dat er ook oneindig veel $n \in \mathbb{N}$ nodig zijn om al deze x te bereiken. Dat zorgt er echter voor dat $a^{n\gamma}$ willekeurig groot kan worden, en dus b ook. Dus het is onmogelijk dat geldt dat $J \models \exists t \forall x < a \exists b < t \exists n (b = a^{n\gamma} \wedge \Omega(n) = x)$, maar deze zou wel moeten bestaan als $J \models \{\forall x < y \exists z \theta(x, y, z) \rightarrow \exists t \forall x < y \exists z < t \theta(x, y, z) | \theta \in \Sigma_1\}$. Dus hieruit volgt een tegenspraak. Dus de F die we helemaal in het begin hebben gedefinieerd, kan niet bestaan. ❑

4 De cofinaliteit van priemgetallen

In de vorige sectie is het duiventilprincipe uitvoerig behandeld, en de resultaten die daar behaald zijn zullen nu gebruikt worden om iets te zeggen over de oneindigheid en cofinaliteit van de priemgetallen. Voor deze bewijzen was er al het een en ander bekend over de cofinaliteit van de priemgetallen in $I\Delta_0$ en door middel van enkele nieuwe, verkorte bewijzen kunnen we dit op een vereenvoudigde manier laten zien.

Het idee van het bewijs is als volgt: we kunnen een aantal functies definiëren die recursief opgebouwd zijn, en daaruit kunnen we dan weer het bestaan van een functie afleiden op zo'n manier dat dit in tegenspraak is met Stelling 3.2. Hoewel er voor de constructie van de functies de voorwaarde $\forall x(x^{\log(x)}$ bestaat) niet nodig is, heb je die wel nodig om een tegenspraak te kunnen afleiden met Stelling 3.2.

We beginnen met het bewijzen van de volgende stelling:

Stelling 4.1. *Zij een $a \in M$ gegeven, samen met een standaard rationaal getal α, zodat $0 < \alpha < 1$. Zij daarnaast ook d en b gegeven zodat $d \leq \log(a)^k$ en $b < 2^{\log(a)^\alpha}$. Dan kan er uit iedere Δ_0^M-functie $G : M^2 \to M$ een functie F worden geconstrueerd zodat $F \in \Delta_0^M$, $F(0) = b$ en*

$$\forall i < d : F(i+1) = \min(G(F(i), i), 2^{\log(a)^\alpha})$$

Bewijs. Merk allereerst op dat $\log(a)^k \neq \log^k(a)$. De eerste term betekent $\log(a)$ tot de macht k, en de tweede betekent de functie log die k maal is toegepast op a.

We mogen zonder verlies van algemeenheid aannemen dat $G : M^2 \to 2^{\log(a)^\alpha}$. Immers, in de definitie van F maakt het niet uit als er een tupel (x, y) is zodat $G(x, y) \geq 2^{\log(a)^\alpha}$, want dan wordt door de aanwezigheid van de minimumfunctie in de definitie de functie vanzelf weer $2^{\log(a)^\alpha}$.

We zullen de stelling eerst bewijzen voor $k = (1 - \alpha)/2$. Dan is dit een definitie van F die voldoet aan de voorwaardes van de stelling:

$$F(i) = z \Leftrightarrow \exists \text{ rijtje } w_0, \ldots, w_i : w_0 = b \wedge w_i = z \wedge \forall j < i(w_{j+1} = G(w_j, j))$$

Dat dit voldoet aan de voorwaardes volgt vrij eenvoudig. Deze functie is ook Δ_0, aangezien het rijtje w_j gecodeerd kan worden in het grondtal $2^{\log(a)^\alpha}$, want alle termen zijn kleiner of gelijk aan $2^{\log(a)^\alpha}$. Aangzien dit rijtje in totaal $1 + \log(a)^k = 1 + \log(a)^{(1-\alpha)/2}$ termen heeft, kan het rijtje dus worden gecodeerd door een x zodat $x < \left(2^{\log(a)^\alpha}\right)^{2+\log(a)^{(1-\alpha)/2}} < \left(2^{\log(a)^\alpha}\right)^{\log(a)^{1/\alpha}} < a$. Dus zo wordt voldaan aan de voorwaardes.

Stel nu dat het resultaat is gegeen voor $k = \beta$. Dan laten we nu zien dat het resultaat ook geldt voor $\beta + (1 - \alpha)/2$. Dus zo volgt dan dat we k willekeurig groot kunnen maken, en daaruit volgt dan de stelling in zijn volledigheid.

Dus zij nu een functie G gegeven, en definieer aan de hand van G de functie $G_{y,w}(x, u) = G(x, y+u)$. Als we aannemen dat de stelling geldt voor $k = \beta$, dan bestaat er dus een functie $F_{f,w} \in \Delta_0^M$ waarvoor dus voor $u < \log(a^\beta)$ geldt dat $F_{y,w}(0) = w$ en $F_{y,w}(u + 1) = G_{y,w}(F_{y,w}(u), u)$. Dan

voldoet de volgende definitie aan de voorwaardes van de stelling:

$$\begin{aligned} F(i) = z \Leftrightarrow &\exists \text{ rijtjes } y_0, \ldots, y_j, w_0, \ldots, w_j : \\ &y_0 = 0 \wedge y_j = i \wedge \forall t < j : (0 \leq y_{t+1} - y_t \leq \log(a)^{\beta}) \\ &\wedge j \leq \log(a)^{(1-\alpha)/2} \wedge w_0 = b \wedge w_j = z \\ &\wedge \forall t < j : F_{y_t, w_t}(y_{t+1} - y_t) = w_{t+1} \end{aligned}$$

Dat deze funcite voldoet aan de voorwaardes is wat minder duidelijk. Als we kijken naar $F(0)$, dan kunnen we $j = 1$ kiezen, met als gevolg dat: $y_0 = 0, y_1 = 0, w_0 = b$ en $w_1 = F_{y_0,w_0}(y_1) = F_{0,b}(0) = b$. Dus we kunnen kiezen dat $w_j = b = z$. Dus $F(0) = b$.

Stel nu dat is gegeven dat $F(i) = z$. Dan moeten we laten zien dat $F(i+1) = G(z, i)$. We mogen hier aannemen dat $i < \log(a)^{\beta} \cdot \log(a)^{(1-\alpha)/2}$, aangezien anders de functie F voor $i + 1$ niet goed gedefinieerd kan worden.

We nemen nu ook aan dat $j < \log(a)^{(1-\alpha)/2}$. Het zou kunnen zijn dat er een gelijkheid geldt. Echter maakt dat het bewijs een stuk gecompliceerder, dus dit geval wordt hier buiten beschouwing gelaten, hoewel het bewijs dan zeker wel opgaat.

Uit het feit dat $F(i) = z$ volgt dat er rijtjes y_i en w_i bestaan zodat deze voldoen aan de voorwaardes. Voor $F(i+1)$ moeten die rijtjes aangevuld worden. De nieuwe rijtjes y'_i en w'_i zijn hetzelfde als y_i en w_i voor de eerste j termen. De toegevoegde termen zijn $y'_{j+1} = y'_j + 1$ en $w'_{j+1} = G(z, i)$.

Voor alle t kleiner dan j gold sowieso al dat $F_{y_t,w_t}(y_{t+1}) = w_{t+1}$, en door de toevoeging van de nieuwe termen is daar niks aan veranderd. Bekijken we nu $t = j$, dan krijgen we:

$$F_{y_j,w_j}(y'_{j+1} - y_j) = F_{i,z}(1) = G_{i,z}(F_{i,z}(0), 0) = G_{i,z}(z, 0) = G(z, i) = w'_{j+1}$$

Dus zo volgt dat $F(i+1) = w'_{j+1} = G(z, i) = G(F(i), i)$. Dus deze F voldoet inderdaad aan de voorwaardes van de stelling.

Ook is deze definitie van F Δ_0, aangezien beide rijtjes kunnen worden gecodeerd door een getal kleiner dan a, namelijk de getallen $\left(1 + \log(a)^{\beta+(1-\alpha)/2}\right)^{1+\log(a)^{(1-\alpha)/2}}$ en $\left(1 + 2^{\log(a)^{\alpha}}\right)^{2+\log(a)^{(1-\alpha)/2}}$ voor respectievelijk de y_j en de w_j. Daarmee is de stelling bewezen ❑

In dit volgende bewijs bouwen we voort op wat we zojuist hebben bewezen. Aan de hand van de vorige stelling en de functies die daar zijn gedefinieerd kunnen we bewijzen dat er weer een andere recursief gedefinieerde functie bestaat die bepaalde fijne eigenschappen heeft. Precies geformuleerd, ziet dat er zo uit:

Stelling 4.2. *Stel $a, b \in M$, en zij $d < \log(a)^k$ gegeven. Dan bestaat er voor iedere Δ_0^M-functie $G : d \to b$ een functie $F \in \Delta_0^M$ zodat $F(0) = G(0)$ en $\forall i < d : F(i+1) = F(i) + G(i+1)$.*

Bewijs. Hoewel dit mogelijk niet meteen duidelijk is uit de stelling, heeft de functie F de eigenschap dat $F(i) = \sum_{q=0}^{i} G(q)$. In het vervolg van dit bewijs zal dit dan ook gebruikt worden in de plaats van $F(i)$.

Allereerst dient opgemerkt te worden dat dit resultaat al volgt uit de vorige stelling wanneer $b \leq d$. Er geldt namelijk $b \leq d \leq \log(a)^k < a$, en er is altijd een α zodat $2^{\log(a)^\alpha} > \log(a)^k$ voor een gegeven k. Dus $G(0) < b < 2^{\log(a)^\alpha}$. We kunnen nu de functie $H : M^2 \to M$ bekijken:

$$H(x, y) = x + G(y)$$

Aangezien nu aan alle voorwaardes voldaan wordt, volgt uit de vorige stelling dat er functie F bestaat zodat $F(0) = G(0)$ en $F(i+1) = H(F(i), i) = F(i) + G(i+1)$. En dat is precies de functie die gevraagd werd in deze stelling.

We kunnen nu iedere term $G(i)$ schrijven in binaire vorm; dit wordt dus $\sum_{s \leq \log(b)} G_s(i) \cdot 2^i$. Het idee van het bewijs is als volgt: we willen de $F(i)$ schrijven als som van twee functies die beide Δ_0 zijn.

We definiëren eerst de volgende functie voor $0 \leq j \leq d$:

$$H_0(j) = \sum_{i \leq j} G_0(i)$$

$$H_{t+1}(j) = \lfloor H_t(j)/2 \rfloor + \sum_{i \leq j} G_{t+1}(i)$$

We kunnen met behulp van de vorige stelling de volgende claim bewijzen:

Claim 3. $\forall t \leq \log(b) : H_t \in \Delta_0^M$.
Bewijs. We bekijken eerst H_0. Om te bewijzen dat $H_0 \in \Delta_0^M$, bekijken we eerst de functie $P_0 : M^2 \to M$, zodat $P_0(x, y) = x + G_0(y)$. Als we vervolgens kiezen dat $H_0(0) = G_0(0)$, wat niet in strijd is met de voorwaardes van de vorige stelling, dan volgt daaruit dat $P(H_0(1), 1) = H_0(0) + G_0(1) = G_0(0) + G_0(1) = \sum_{i \leq 1} G_0(i)$. Zo kan dit eenvoudigerwijs uitgebreid worden voor alle j.

Stel nu dat H_t ook op eenzelfde manier Δ_0-recursief gedefinieerd is. Dus $H_t(j+1) = P_t(H_t(j), j)$. Dan kunnen we voor H_{t+1} de volgende functie bekijken: $P_{t+1} : M^2 \to M$ zodat $P_{t+1}(x, y) = \lfloor P_t(x, y)/2 \rfloor + G_{t+1}(y)$. Dan kunnen we op eenzelfde manier als bij de inductiehypothese laten zien dat $H_{t+1}(j+1) = P_{t+1}(H_{t+1}(j), j)$. Dus zo volgt de claim. ❑

Verder definiëren we de volgende functie voor $j \leq d$ en $t \leq \log(b)$:

$$p_t(j) = \text{bin}_{H_t(j)}(0)$$

Nu volgt duidelijk uit de definitie van H en p dat $p_t(0) = G_t(0)$, want G_t is altijd 0 of 1, en daardoor is $\lfloor G_t(0)/2 \rfloor$ altijd 0. Verder geldt de volgende claim:

Claim 4.

$$2^t H_t(j) + \sum_{s<t} p_s(j) 2^s + \sum_{s \leq t} G_s(j+1) 2^s = 2^t H_t(j+1) + \sum_{s<t} p_s(j+1) 2^s$$

Bewijs. We gebruiken inductie op $t \leq \log(b)$.

Bekijk eerst $t = 0$. Dan wordt de linkerzijde van de claim $H_0(j) + G_0(j+1)$. Uit de definitie van H_0 en de vorige claim volgt dat $H_0(j+1) = H_0(j) + G_0(j+1)$, en de rechterzijde van de claim is precies $H_0(j+1)$. Dus dit bewijst de claim voor $t = 0$

Stel nu dat de claim gegeven is voor een $t < \log(b)$. We nemen nu eerst aan dat $H_t(j)$ en $H_t(j+1)$ even zijn. Dit maakt het bewijs iets overzichtelijker en eenvoudiger, anders moeten er een paar extra gevallen nagegaan worden, die redelijk identiek zijn aan dit geval.

We bekijken nu de rechterkant van de claim voor $t+1$, dan staat er: $2^{t+1}H_{t+1}(j+1) + \sum_{s\leq t} p_s(j+1)2^s$. Aangezien $H_t(j+1)$ even is, geldt dat $p_t(j+1) = 0$, dus de rechterzijde is ook gelijk aan $2^{t+1}H_{t+1}(j+1) + \sum_{s<t} p_s(j+1)2^s$. We weten ook uit de definitie van H dat de functie $2^{t+1}H_{t+1}(j+1)$ gelijk is aan $2^{t+1}(H_t(j)/2 + \sum_{i\leq j+1} G_{t+1}(i) = 2^t H_t(j+1) + 2^{t+1}\left(\sum_{i\leq j} G_{t+1}(i)\right) + 2^{t+1}G_{t+1}(j+1)$. Wegens de inductiehypothese geldt nu dus dat de rechterkant gelijk is aan

$$2^t H_t(j) + \sum_{s<t} p_s(j)2^s + \sum_{s\leq t} G_s(j+1)2^s + 2^{t+1}\left(\sum_{i\leq j} G_{t+1}(i)\right) + 2^{t+1}G_{t+1}(j+1)$$

Aangezien $H_t(j)$ even is en dus $p_t(j) = 0$, en uit de definitie van H_t, kunnen we deze laatste regel omschrijven tot:

$$2^{t+1}\left(H_t(j)/2 + \sum_{i\leq j} G_{t+1}(i)\right) + \sum_{s\leq t} p_s(j)2^s + \sum_{s\leq t+1} G_s(j+1)2^s$$

En dit is per definitie weer gelijk aan:

$$2^{t+1}H_{t+1} + \sum_{s\leq t} p_s(j)2^s + \sum_{s\leq t+1} G_s(j+1)2^s$$

Dit is gelijk aan de linkerzijde van de claim met $t+1$, dus hiermee is de inductiestap voltooid en is de claim bewezen. ❑

We gebruiken nu de rechterzijde van de claim voor $t = \log(b)$. Dit geeft de volgende uniforme Δ_0^M-functie:

$$F(j) = 2^{\log(b)}H_{\log(b)}(j) + \sum_{s<\log(b)} p_s(j)2^s$$

Het is geen toeval dat deze functie $F(j)$ wordt genoemd, want deze functie blijkt de eigenschappen te hebben die we verwachtten in deze stelling te krijgen.

Immers wisten we al dat $\forall t < \log(b) : p_t(0) = G_t(0)$, en uit de definitie van $H_{\log(b)}$ volgt dat $H_{\log(b)}(0) = G_{\log(b)}(0)$, dus bij elkaar geeft dat dat $F(0) = 2^{\log(b)}G_{\log(b)}(0) + \sum_{s<\log(b)} G_t(0)2^s = \sum_{s\leq\log(b)} G_t(0)2^s = G(0)$.

Ook volgt eenvoudig uit de claim dat $F(j+1) = F(j) + \sum_{s\leq\log(b)} G_s(j+1)2^s = F(j) + G(j+1)$.

Dus hiermee is de stelling bewezen. ❑

We kunnen nu het hoofdbewijs van deze sectie bekijken. Vanuit dit bewijs volgt via een klein lemma wat we willen bewijzen over de cofinaliteit van de priemgetallen.

Stelling 4.3. *Stel dat er voor een $a \in M$ geldt dat er geen priemgetal zit tussen a en a^{11}. Dan bestaat er een functie $H \in \Delta_0^M$ zodat:*

$$H : a\log(a^{10}) \rightarrowtail (1 + \lfloor a/2 \rfloor)\log(a^{10}) + 2a\log(a)$$

Bewijs. Allereerst merken we op dat we in Δ_0 kunnen spreken over het aantal priemgetallen dat een bepaald getal x deelt. Dit getal zal in het vervolg van het bewijs aangeduid worden met $v(y)$. Ook kunnen we op eenzelfde manier spreken over het i'de priemgetal wat x deelt.

Ook kunnen we laten zien dat $v(y) \leq \log(y)$. Dit volgt als volgt: kies een $y \in M$ en bekijk $y' = \prod_{j<v(y)} p_j$. Dan geldt dat $v(y') = v(y)$ en $\log(y') \leq \log(y)$. Dus we hoeven dit alleen maar voor y' te laten zien. Bekijk nu $2^{v(y')}$. Omdat voor alle $j < v(y')$ geldt dat $p_j \geq 2$, geldt dat $2^{v(y')} = \prod_{j<v(y')} 2 \leq \prod_{j<v(y')} p_j = y'$. Dus $2^{v(y')} \leq y'$ en daaruit volgt dat $v(y') \leq \log(y')$.

Zij nu dus een $x < a\log(a^10)$ gegeven. Er geldt nu dat er een unieke $i \leq a$ is zodat $(i-1)\log(a^{10}) \leq x < i\log(a^{10})$. Bekijk nu voor deze i het getal $a^{10} + i$. Dit getal zullen we in het vervolg schrijven als $\prod_{j<v} p_j^{e_j}$, waarbij v hier dan uiteraard $v(a^{10} + i)$ is.

We bekijken nu eerst een apart geval, waarvoor de claim makkelijker te bewijzen is.

Stel dat het volgende geldt:

$$(*) \quad \exists j < v(\forall t \leq a : p_j^{e_j+1} \nmid a^{10} + t \wedge (\exists r \leq i : p_j^{e_j} | a^{10} + r) \Rightarrow i = r)$$

Dan kiezen we de kleinste j waarvoor dit geldt en dan definiëren we de functie H als volgt:

$$H(x) = \lfloor (1 + p_j)/2 \rfloor \log(a^{10}) + x - (i-1)\log(a^{10})$$

Hierbij moet opgemerkt worden dat aangezien geldt dat $p_j < a^1 0 + t < a^1 1$, want a is groot, weten we uit de aanname dat $p_j \leq a$, dus $\lfloor (1 + p_j)/2 \rfloor < \lfloor a/2 \rfloor + 1$.

Stel nu dat $(*)$ niet geldt.

We kunnen sowieso voor $y \in M$ de priemontbinding bekijken: $\prod_{j<v(y)} q_i^{b_i}$. Dan geldt dat:

$$\log(y) = \log\left(\prod_{i<v(y)} q_i^{b_i}\right) = \sum_{i<v(y)} b_i \log(q_i) \leq \sum_{i<v(y)} b_i(1 + \log(q_i))$$

.

Er geldt echter ook dat:

$$2^{\sum_{i<v(y)} b_i(1+\log(q_i))} \leq \prod_{i<v(y)} 2^{b_i} \cdot 2^{\log(q_i)} = \prod_{i<v(y)} 2^{b_i} \cdot q_i \leq \prod_{i<v(y)} q_i^{b_i} \cdot q_i \leq \prod_{i<v(y)} q_i^{b_i} \cdot q_i^{b_i} = y^2$$

Ofwel, anders gezegd: $\sum_{i<v(y)} b_i(1+\log(q_i)) \leq 2\log(y)$.

Dus de conclusie hiervan is:

$$(**) \qquad \log(y) \leq \sum_{i<v(y)} b_i(1+\log(q_i)) \leq 2\log(y)$$

Met behulp van $(**)$ kunnen we het interval waar x in ligt verscherpen. We kunnen nu namelijk $j < v$ en $k < e_j$ kiezen zodat:

$$d_0 = (i-1)\log(a^{10}) + \sum_{m<j} e_m(1+\log(p_m)) + k(1+\log(p_j)) \leq x <$$

$$(i-1)\log(a^{10}) + \sum_{m<j} e_m(1+\log(p_m)) + (k+1)(1+\log(p_j)) = d_1$$

We kiezen nu een $s \leq a$ zodat voor een bepaalde b geldt dat $a^{10}+s$ voldoet aan $(*)$ als je e_j vervangt door b. Dat wil zeggen dat de volgende uitspraken allemaal gelden: $p_j^b | a^{10}+s$, $\forall t \leq a : p_j^{b+1} \nmid a^{10}+t$ en $\forall t < s : p_j^b \nmid a^{10}+t$. Als zou gelden dat $s = i$, dan zou aan de voorwaarden voor $(*)$ voldaan zijn, en we hadden aangenomen dat dat niet het geval was.

Stel dus dat $s < i$. Merk allereerst op dat $e_j \leq b$. We hadden immers aangenomen dat $\forall t \leq a : p_j^{b+1} \nmid a^{10}+t$ en er gold dat $p_j^{e_j} | a^{10}+i$. Aangezien we ook hadden aangenomen dat $p_j^b | a^{10}+s$, kunnen we daaruit concluderen dat $p_j^{e_j} | a^{10}+i-(a^{10}+s) = i-s > 0$. We kunnen nu dus kijken naar de priemontbinding van $i-s$: $\prod_{m<v(i-s)} q_m^{c_m}$. Aangezien $p_j | i-s$, moet p_j wel gelijk zijn aan een van de termen in dit product. Dus stel dat $q_r = p_j$. Dan weten we dankzij $(**)$ dat:

$$2(i-s-1)\log(a) + \sum_{m<r} c_m(1+\log(q_m)) + (k+1)(1+\log(q_r)) \leq$$

$$2(i-s-1)\log(a) + \sum_{m\leq r} c_m(1+\log(q_m)) \leq 2(i-s-1)\log(a) + \sum_{m<v(i-s)} c_m(1+\log(q_m)) \leq$$

$$2(i-s-1)\log(a) + \log(i-s) < 2(i-s-1)\log(a) + \log(a) = 2(i-s)\log(a) < 2a\log(a)$$

Dus we kunnen nu de functie H het interval $[d_0, d_1)$ af laten beelden op het interval:

$$[2(i-s-1)\log(a) + \sum_{m<r} c_m(1+\log(q_m)) + k(1+\log(q_r)),$$

$$2(i-s-1)\log(a) + \sum_{m<r} c_m(1+\log(q_m)) + (k+1)(1+\log(q_r)))$$

Deze functie is duidelijk injectief, en aangezien je voor iedere parameter voor dit interval een bovengrens kan vinden, geldt dat de functie H ook Δ_0^M is. Dus dit bewijst de stelling als $s < i$

In het geval dat $s > i$ kunnen we op een vrijwel identieke manier te werk gaan. We hoeven alleen

iedere keer dat de term $i - s$ voorkomt in het vorige geval dit te vervangen door:

$$s - i + \lfloor (a - s)/p_j^k \rfloor p_j^k$$

De term $\lfloor (a - s)/p_j^k \rfloor p_j^k$ komt mogelijk als een verrassing. Deze term is echter nodig om ervoor te zorgen dat daadwerkelijk alle mogelijke gevallen van i worden beschouwd. De grootste i waarvoor het vorige geval geldt was namelijk $s + \lfloor (a - s)/p_j^k \rfloor p_j^k$, want $\lfloor (a - s)/p_j^k \rfloor p_j^k < a$. Dus nu moeten we bij die term beginnen en daarna afwerken naar beneden, zodat echt alle gevallen behandeld worden. Voor de rest is het bewijs identiek.

De functie H die we hebben geconstrueerd is nu dus duidelijk injectief en Δ_0^M, dus zo is de stelling bewezen. ❑

Nu we dit bewijs hebben afgerond, is de stap naar het hoofdresultaat van deze sectie niet groot meer. Wat we zullen bewijzen is dat uit de functie H uit de vorige stelling omgeschreven kan worden, zodat er een tegenspraak met Stelling 3.2 optreedt. Daaruit volgt dan weer dat uit het duiventilprincipe voor x^2 en x kan worden afgeleid dat er een priemgetal groter dan x moet bestaan.

Gevolg 4.4.

$$I\Delta_0 \vdash \forall a(a^{\log(a)} \textit{ bestaat } \Rightarrow \exists y > a : y \textit{ is priem})$$

Bewijs. Stel dat er een $a \in M$ bestaat zodat er geen priemgetal is dat groter is. Dan zit er in het bijzonder geen priemgetal tussen a en a^{11}. Uit de vorige stelling volgt nu dat er een functie H is zodat:

$$H : a\log(a^{10}) \rightarrowtail (1 + \lfloor a/2 \rfloor)\log(a^{10}) + 2a\log(a)$$

Dit kunnen we echter omschrijven zodat:

$$H : 10a\log(a) \rightarrowtail 10(1 + \lfloor a/2 \rfloor)\log(a) + 2a\log(a)$$

We nemen nu zonder verlies van algemeenheid aan dat a deelbaar is door twee; mocht dat niet zo zijn, dan geldt een vergelijkbaar verhaal.

Dit geeft, samen met het feit dat a groot is, dat:

$$H : 10a\log(a) \rightarrowtail 10(1 + a/2)\log(a) + 2a\log(a)$$

$$H : 10a\log(a) \rightarrowtail 10\log(a) + 5a\log(a) + 2a\log(a)$$

$$H : 10a\log(a) \rightarrowtail a\log(a) + 5a\log(a) + 2a\log(a)$$

$$H : 10a\log(a) \rightarrowtail 8a\log(a)$$

Als we nu aannemen dat $a^{\log(a)}$ bestaat kunnen we Stelling 3.2 gebruiken met $x = 8a\log(a)$ en $\epsilon = 1/4$. Daaruit volgt dat het onmogelijk is dat er een H bestaat zodat $H : 10a\log(a) \rightarrowtail 8a\log(a)$. Dit leidt dus tot een tegespraak met het feit dat we aannamen dat er geen priemgetal was groter dan a. ❑

5 Verbeteringen en nieuwe bevindingen

In deze sectie zullen we zien dat het onderzoek naar de bewijsbaarheid van bepaalde stellingen niet heeft stilgezeten sinds de hoofdbevindingen van deze scriptie zijn geformuleerd. In de tussentijd is de relatie tussen $I\Delta_0$ en computationele complexiteitstheorie flink uitgediept. Ook zijn bepaalde voorwaardes die in het hoofdgedeelte van deze scriptie zijn gesteld afgezwakt. In deze sectie volgt dus een kleine uitweiding over deze resultaten.

5.1 Een zwakkere aanname

In Stelling 3.1 gebruikten we de aanname dat in het geval dat $x^{\log^k(x)}$ bestaat, dat dan het duiventilprincipe voor x^2 en x kon worden afgeleid. Dit gebruikten we vervolgens om via een gevolg aan te tonen dat voor een zekere x er een priemgetal bestaat wat groter is, mits $x^{\log(x)}$ bestond.

In 2001 is echter bewezen in [9] dat deze laatste voorwaarde flink verzwakt kan worden. De hoofdstelling die in dat artikel bewezen werd, is de volgende:

Stelling 5.1. *Voor iedere $k \in \mathbb{N}, k > 0$ geldt dat:*

$$I\Delta_0 \vdash \forall x(\exists y : x^{(\log(x))^{1/k}} \text{ bestaat } \Rightarrow \neg(F : 2x \rightarrowtail x))$$

Merk op dat de notatie $(\log(x))^{1/k}$ hier betekent dat de $1/k$'de macht wordt genomen, en niet dat de functie in zichzelf wordt samengesteld.

Deze vergelijkbare voorwaarde geeft dus een aanmerkelijk sterker resultaat, en dit sterkere resultaat kan worden gebruikt om een sterker bewijs te geven met betrekking tot de cofinaliteit van de priemgetallen. Dat wordt hieronder getoond.

Stelling 5.2.

$$I\Delta_0 \vdash \forall x(\exists y : x^{(\log(x))^{1/k}} \text{ bestaat } \Rightarrow \exists u > x \wedge u \text{ priem})$$

Bovendien geldt dat dit een strikte verbetering is, aangezien er een model M van $I\Delta_0$ bestaat waarin $a^{(\log(a))^{1/k}}$ bestaat, maar $a^{\log(a)}$ niet.

Bewijs. Stel dat $a^{(\log(a))^{1/k}}$ bestaat in M zodat $M \models I\Delta_0$. Stel nu $b = a^2$ en merk op dat $b^{(\log(b))^{1/k}} = a^{(\log(a))^{1/k}} \cdot a^{(\log(a))^{1/k}}$ bestaat in M, want M is gesloten onder vermenigvuldiging. We gebruiken nu Stelling 5.1, waaruit dus volgt dat er geen afbeelding F bestaat zodat $F : b^2 \rightarrowtail b$. Hieruit volgt ook dat er geen afbeelding F kan zijn waarvoor geldt dat $F : \frac{9}{8}b \rightarrowtail b$. Als deze namelijk wel bestond, dan hadden we hem een aantal keer kunnen samenvoegen, zodat er uiteindelijk een afbeelding $F^k : 2b \rightarrowtail b$ zou ontstaan, vergelijkbaar met de situatie in Stelling 3.2. Uit dit laatste feit mogen we nu ook concluderen dat er geen afbeelding F is zodat $F' : 9a\log(a) \rightarrowtail 8a\log(a)$. Zou deze laatste functie wel bestaan, dan geldt de volgende redenering: We kunnen $\frac{9}{8}b$ en b opbreken in $a/8\log(a)$ gelijke stukjes van respectievelijke grootte $9a\log(a)$ en $8a\log(a)$. Op ieder van deze stukjes zou je dan de functie F' kunnen toepassen, maar dat levert een functie F, waarvoor geldt dat $F : 2b \rightarrowtail b$. Dit is in tegenstelling met wat we net hebben beredeneerd. De redenering gaat nu verder zoals in het einde van Gevolg 4.4.

Om de verbetering te laten zien, bekijken we nu het volgende model van $I\Delta_0$: zij N een niet standaard model van de rekenkunde met een niet-standaard element a en stel dat $M = \{x \in N | \exists n \in \mathbb{N} : N \models x < a^{n(\log(a))^{1/k}}\}$. Het is nu duidelijk dat M een snede is van N die gesloten is onder optellen en vermenigvuldigen, dus zoals al in de inleiding behandeld is, betekent dit dat $M \models I\Delta_0$. Het gevraagde volgt nu, door op te merken dat $a^{n(\log(a))^{1/k}}$ nog steeds in M zit, en dat $a^{\log(a)} > a^{n(\log(a))^{1/k}}$ voor iedere $n \in \mathbb{N}$. ❑

5.2 De eindige axiomatisering van $I\Delta_0$

In de Stelling 3.6 is er bewezen dat de eindige axiomatisering van $I\Delta_0$ impliceert dat het duiventil-principe voor x^2 en x onmiddelijk kan worden aangenomen zonder verdere voorwaarden. Het blijkt dat deze eindige axiomatisering nauw samenhangt met de computationele complexiteitstheorie. Dit is onder andere beschreven in [10] en [2]. Voor een kleine uitleg van de gebruikte termen uit de complexiteitstheorie, zie de Appendix.

Het belangrijkste resultaat is als volgt:

Stelling 5.3. *Als de Polynominale Hiërarchie niet instort, dan is $I\Delta_0$ niet eindig axiomatiseerbaar.*

De omgekeerde uitspraak is niet per se waar. Het beste resultaat dat tot nu toe behaald is, is het volgende:

Stelling 5.4. *Als in $I\Delta_0$ bewezen kan worden dat de Polynominale Hiërarchie instort, dan is $I\Delta_0$ eindig axiomatiseerbaar.*

Deze laatste voorwaarde is erg sterk. Het is nog een onbekend of überhaupt bewezen kan worden dat de Polynominale Hiërarchie instort, laat staan in $I\Delta_0$. De kans dat via deze stelling bewezen wordt dat $I\Delta_0$ eindig axiomatiseerbaar is, lijkt dan ook bijzonder klein.

Verder is er weinig te vinden over dit probleem. Het lijkt erop alsof de eindige axiomatiseerbaarheid op een dusdanige manier in relatie staat tot de computationele complexiteitstheorie, dat resultaten in dat vakgebied haast noodzakelijk zijn om op dit punt vooruitgang te boeken.

A Appendix: Een kleine inleiding tot computationele complexiteitstheorie

In deze appendix zullen we een beetje ingaan op de theorie van computationele complextiteitstheorie. Dit materiaal is onder andere terug te vinden in [2] en daarin staan nog meer verwijzingen naar andere bronnen.

Computationele complextiteitstheorie is het vakgebied binnen de theoretische informatica dat zich focust op het indelen van berekeningsproblemen in klasses van moeilijkheid en de relaties tussen deze klasses bestudeert. Een probleem wordt als (inherent) moeilijk beschouwd wanneer er veel tijd of veel geheugen is om het op te lossen, onafhankelijk van het algoritme dat gebruikt wordt. In deze appendix zullen we ons alleen focussen op het tijdsaspect en de problemen die we behandelen zullen deterministisch zijn, dat wil zeggen, problemen die van de input een bepaalde eigenschap moeten controleren en dan een ja-nee-antwoord teruggeven.

Enkele klasses waarin deze problemen worden gerangschikt zijn de volgende:

P

De klasse P is de klasse van alle problemen die in polynominale tijd op te lossen zijn. Dit betekent dat de berekeningstijd van algoritmes van dit probleem polynominaal afhangt van de input. Deze problemen worden intuïtief gezien als "redelijk", waarmee bedoeld wordt dat het probleem in een redelijke tijd op te lossen valt. Enkele voorbeelden van problemen in P zijn "Gegeven twee getallen x en y, is x een deler van y?", of, zoals recent is bewezen in [11], het probleem "Gegeven x, is x priem?".

NP

Deze klasse bestaat uit al die problemen waarvan een positieve oplossing in polynominale tijd te controleren is. Het is duidelijk dat alle problemen die in P zitten ook in NP zitten; een algoritme om het antwoord te controleren is bijvoorbeeld om het algoritme om de oplossing te vinden, dat is in P zit, te herhalen. Het is onbekend of de inclusie P$\subseteq$ NP een strikte is. Dit vraagstuk staat ook wel bekend als het P=NP-probleem en is een van de zeven milleniumproblemen. Een voorbeeld van een probleem dat in NP is, maar waarvan het onbekend is of het in P zit, is het volgende: "Gegeven een verzameling gehele getallen, is er een niet-lege deelverzameling zodat de som van de getallen in deze deelverzameling 0 is?". Als het algoritme een positief antwoord geeft, dan is het voor deze deelverzameling niet moeilijk om te controleren of deze voldoet; het enige wat hoeft te gebeuren is dat de getallen opgeteld moeten worden. Er is echter nog geen algoritme bekend wat dit probleem in polynominale tijd oplost.

coNP

De klasse coNP is, zoals de naam al enigszins suggereert, de klasse die bestaat uit al die problemen waarvan een negatieve oplossing in polynominale tijd te controleren is. Dit wordt dan ook wel eens

gezien als het "complement"van NP. Een voorbeeld van een probleem in coNP is het probleem "Gegeven een verzameling gehele getallen, is er geen niet-lege deelverzameling zodat de som van de getallen in deze deelverzameling 0 is?". Merk op dat dit probleem vrijwel hetzelfde is als het voorbeeld dat hierboven is genoemd. De ontkenning zorgt er echter voor dat in dit geval het nee-antwoord makkelijker te controleren is. Van dit probleem is het ook onbekend of het ja-antwoord in polynominale tijd te bepalen is, ofwel anders gezegd, het is onbekend of het ook in NP zit. Dit hangt weer samen met de vraag of NP=coNP, een ander belangrijk vraagstuk.

$\mathbf{P^{NP}}$

Deze klasse is, intuïtief gezien, de klasse waarvan de problemen in polynominale tijd op te lossen zijn, mits je van een NP-probleem de oplossing in een enkele stap kan berekenen. Deze klasse leent zich minder makkelijk om een voorbeeld bij te geven. Wel is duidelijk dat geldt dat NP$\subseteq$ P^{NP} en coNP$\subseteq$ P^{NP}. Ook van deze inclusie is nog niet bekend of deze strikt is.

De Polynominale Hiërarchie

Zoals de klasse P^{NP} is gedefinieerd kunnen er nog meer klasses gedefinieerd worden. Zo is er ook de klasse NP^{NP}, waarvoor geldt dat NP$\subseteq$ P^{NP}. Op dezelfde manier is er ook de klasse $coNP^{NP}$, waarvoor geldt dat coNP$\subseteq$ $coNP^{NP}$. Er bestaat zo ook zelfs de klasse $P^{NP^{NP}}$ en zo kunnen deze klasses tot in het oneindige door worden gedefineerd. De vereniging van al deze klasses wordt de *Polynominale Hiërarchie* genoemd. De eerder genoemde inclusies kunnen ook worden uitgebreid tot deze hogere niveaus. Van geen enkele van deze inclusies is echter bekend of ze strikt zijn of niet. Als blijkt dat een van deze inclusies strikt is, dan wordt ook wel gezegd dat de Polynominale Hiërarchie *instort*. In het bijzonder is dit het geval als P=NP of NP=coNP.

Referenties

[1] J. Paris, A. Wilkie, en A. Woods: *Provability of the pigeonhole principle and the existence of infinitely many primes.* The Journal of Symbolic Logic, 53(4):1235–1244, 1988.

[2] P. Hájek en P. Pudlák: *Metamathematics of First-Order Arithmetic.* Perspectives in Mathematical Logic. Springer, 1e uitgave, 1993.

[3] A. Macintyre en D. Marker: *Primes and their residue rings in models of open induction.* Annals of Pure and Applied Logic, 43:57–77, 1989.

[4] J. Kraíček: *Bounded arithmetic, propositional logic, and complexity theory.* Cambridge University Press, 1995.

[5] H. Gaifman en C. Dimitracopoulos: *Fragments of Peano's arithmetic and the MRDP theorem.* Logic and algorithmic, Monographie No. 30 de L'Enseignement Mathématique, pagina's 187–206, 1982.

[6] J. van Oosten: *Gödel's Incompleteness Theorems.* Niet gepubliceerd. Dictaat.

[7] A. Woods: *Some problems in logic and number theory.* proefschrift, University of Manchester, 1981.

[8] J. Paris en L. Kirby: Σ_n*-collection schemes in arithmetic.* In A. Macintyre en L. Pacholski (redactie): *Logic Colloquim '77*, pagina's 199–209, Amsterdam, 1978. North–Holland.

[9] A. Atserias: *Improved bounds on the weak pigeonhole principle and infinitely many primes from weaker axioms.* In J. Sgall, A. Pultr, en P. Kolman (redactie): *Mathematical Foundations of Computer Science 2001*, volume 2136 van *Lecture Notes in Computer Science*, pagina's 148–158. Springer, Heidelberg, 2001.

[10] J. Kraíček, P. Pudlák, en G. Takeuti: *Bounded arithmetic and the polynomial hierarchy.* Annals of Pure and Applied Logic, 52(1-2):143–153, 1991.

[11] M. Agragwal, N. Kayal, en N. Saxena: *PRIMES is in P.* Annals of Mathematics, 160(2):781–793, 2004.