Universiteit Utrecht

Faculteit Geesteswetenschappen
Departement Filosofie en Religiewetenschap

De disjunctie-eigenschap in constructieve wiskunde

Bachelorscriptie

Quintijn Pit
4093011
BA Filosofie

Begeleider:

Prof. dr. Rosalie Iemhoff
Onderzoeksinstituut voor Filosofie en Religiewetenschap

19 juni 2020

Uittreksel

De gevolgtrekkingen in de constructieve wiskunde laten zich goed beschrijven door de intuïtionistische logica **I**. Deze logica heeft de zogeheten disjunctie-eigenschap: $\vdash A \vee B$ impliceert $\vdash A$ of $\vdash B$. Buss en Pudlák vonden een algoritme dat bewerkstelligt dat deze eigenschap ook voor de constructieve wiskunde geldt. Dat maakt gebruik van het bewijssysteem G1ip voor het propositionele deel van **I**, **Ip**. Voor de klasse Harrop-formules geldt zelfs een generalisatie van dit resultaat. Ik voltooi de bewijzen van deze resultaten en vertaal ze naar een ander **Ip**-bewijssysteem: G3ip.

Inhoudsopgave

> Den menschen is een vermogen eigen dat al hun wisselwerkingen met de natuur begeleidt, het vermogen n.l. tot wiskundig bekijken van hun leven, tot het zien in de wereld van herhalingen van volgreeksen, van causale systemen in den tijd.
>
> L.E.J. Brouwer
> *Over de grondslagen der wiskunde*

> In practice the intuitionistic point of view hasn't lead to a large scale and continuous rebuilding of mathematics. In fact, there is less of this kind of work going on now even than before. On the other hand, one might say that intuitionism describes a particular portion of mathematics, the constructive part, and that it has been described very adequately by now what the meaning of that constructive part is.
>
> D. de Jongh

1 Introductie

In deze scriptie onderzoek ik de disjunctie-eigenschap van de constructieve wiskunde aan de hand van het bewijssysteem G1ip voor de intuïtionistische logica. Ik zet eerst een korte filosofische achtergrond van het wiskundig constructivisme uiteen en beschrijf de verhouding tussen intuïtionistische logica en constructieve wiskunde, in het bijzonder met betrekking tot de disjunctie-eigenschap. Ik demonstreer dat deze eigenschap zich niet zonder meer laat vertalen in een stuk gereedschap voor de wiskundig constructivist, omdat dat een algemeen uitvoerbaar algoritme vereist dat uit een disjunctiebewijs een bewijs van een van de deelformules produceert. Dat doe ik in paragraaf 2. In de daaropvolgende paragraaf vertaal ik dit probleem naar de eis dat het algoritme te representeren is in een berekening die in polynomiale tijd uitvoerbaar is. Zo'n algoritme schets ik in paragraaf 4, waarna ik in paragrafen 5 en 6 de vereiste eigenschappen bewijs. Paragraaf 7 behandelt een generalisatie van het algoritme voor de klasse Harrop-formules, en ik besluit met een vertaling van deze resultaten naar een vergelijkbaar bewijssysteem, G3ip, in paragraaf 8.
Als voorkennis veronderstel ik bekendheid met basale eigenschappen van de wiskundige logica. Met 'disjunctie', 'conjunctie' en 'implicatie' zal ik zowel het voegteken aanduiden als een formule waarin dit het buitenste voegteken is.

2 Constructieve wiskunde, intuïtionistische logica en de disjunctie-eigenschap

In de klassieke wiskunde geldt een uitspraak als deze waar is. Neem bijvoorbeeld de bewering 'er zijn twee irrationale getallen a en b zodanig dat a^b rationaal is.' Een elegant bewijsje hiervoor neemt $a = \sqrt{2}, b = \sqrt{2}$ of, als $\sqrt{2}^{\sqrt{2}}$ rationaal blijkt, $a = \sqrt{2}^{\sqrt{2}}, b = \sqrt{2}$. Het bewijs berust op de tweeledigheid van waarheid: of er bestaat een breuk $\frac{p}{q}$ gelijk aan $\sqrt{2}^{\sqrt{2}}$, of niet. In beide gevallen is de initiële

uitspraak waar. Hoewel een dergelijke redenering voor een geoefend wiskundige een tweede natuur is, berust zij op een aantal onduidelijke aannames van metafysische aard. In de kern de aannames van het bestaan van onbekende wiskundige objecten, in casu $\frac{p}{q}$, en het toekennen van eigenschappen hieraan. Er wordt uitgegaan van een wiskundige werkelijkheid met absolute, mensonafhankelijke waarheden en eigenschappen, zij het in de vorm van een transcendentale platonische wereld of juist als systeem van conditionele formalismen, geregeerd door de logica. De waarheid van een bewering is hier onafhankelijk van onze kennis ervan, hetgeen de redeneertrant 'als φ niet onwaar is, moet het wel waar zijn, φ heeft immers een hoe dan ook een waarheidswaarde' rechtvaardigt.

Er is een vorm van wiskunde die een dergelijke epistemologische *leap of faith* verwerpt: de *constructieve wiskunde*. Voor een wiskundig constructivist geldt een uitspraak als er een constructie bestaat die de betekenisinhoud van die uitspraak aantoont. Het idee is dat de enige wiskunde die direct epistemisch toegankelijk is, bestaat in de constructies die zonder meer evident zijn als structuur in het menselijk denken, alsook in de constructies die hierop vervolgens weer voortbouwen. Dat impliceert dat gevolgtrekkingen van uitspraken in de constructieve wiskunde niet geschieden op grond van waarheid, maar op grond van constructieve bewijzen. Wanneer we de onderliggende gevolgtrekkingregels willen abstraheren en vervolgens formaliseren, blijkt dat deze nauwkeurig beschreven worden door de Brouwer-Heyting-Kolgomorovinterpretatie(BHK) van de gebruikelijke eersteordelogische symbolen:

- $\vee$: een bewijs voor $P \vee Q$ bestaat uit een bewijs voor P of een bewijs voor Q.
- $\wedge$: een bewijs voor $P \wedge Q$ bestaat uit een bewijs voor P en een bewijs voor Q.
- $\rightarrow$: een bewijs voor $P \rightarrow Q$ is een algoritme dat uit een bewijs voor P een bewijs voor Q kan produceren.
- $\exists$: een bewijs voor $\exists x \varphi(x)$ is een constructie van een object x een een bewijs voor $\varphi(x)$.
- $\forall$: een bewijs voor $\forall x \varphi(x)$ is een algoritme dat voor ieder object x in de onderhavige structuur een bewijs geeft van $\varphi(x)$.
- $\bot$: $\bot$ (het falsum) is onbewijsbaar.
- $\neg$: $\neg P$ is een afkorting voor $P \rightarrow \bot$.

Dit betekent dat hoewel in constructieve wiskunde afleidingen niet in laatste plaats op logica berusten — waar dat in de klassieke wiskunde wel het geval is — we wel een logica kunnen gebruiken om uitspraken te formaliseren en te bewijzen aan de hand van BHK. Deze logica heet de *intuïtionistische logica* **I**, naar de oudste stroming van het wiskundig constructivisme. We zien allereerst dat als de betekenisinhoud van een zin constructief bewijsbaar is, deze dan

ook zeker waar is, zodat **I** een deelsysteem is van de klassieke eersteordelogica. Verder is de beroemdste eigenschap van **I** het falen van de wet van de uitgesloten derde; die stelt dat voor iedere zin A ofwel A dan wel $\neg A$ geldt. In de klassieke logica wordt dit geïnterpreteerd als 'A is waar of A is onwaar' en is het een fundamenteel feit. Het stelt de classicus in staat om afleidingen te maken als $\neg\neg A \to A$ en $\neg(\neg A \wedge \neg B) \to (A \vee B)$. Voor de constructivist anderzijds zou deze wet betekenen dat voor iedere bewering er al een bewijs of een weerlegging is geconstrueerd, hetgeen duidelijk absurd is. Hoewel er talloze soorten en smaken van constructieve wiskunde bestaan — de vorm die ik hier schets ligt vrij dicht bij het oorspronkelijke intuïtionisme — delen deze allemaal de afwijzing van de wet van de uitgesloten derde.

Laten we door een constructivistische bril nog eens naar de uitspraak aan het begin van deze paragraaf kijken. Die luidt nu dat er voor twee getallen a en b constructies zijn gevonden die bewijzen dat ze irrationaal zijn, en een breuk die gelijk is aan a^b. We zien dat het klassieke bewijsje niet meer volstaat;[1] het berust namelijk op een toepassing van de wet van de uitgesloten derde: $\sqrt{2}^{\sqrt{2}}$ is rationaal of irrationaal. Om dezelfde disjunctie constructief te bewijzen, zouden we ofwel een breuk moeten vinden die evalueert op $\sqrt{2}^{\sqrt{2}}$, dan wel moeten laten zien dat de aanname van zo'n breuk tot een tegenspraak leidt.

Dit laat zich veralgemeniseren tot de *disjunctie-eigenschap* van **I**: als er een intuïtionistisch bewijs bestaat voor een disjunctie $A \vee B$, dan is ook een bewijs voor A of een bewijs voor B construeerbaar (we noemen A en B de *disjuncten*).[2] Met het oog op de interpretatie van de disjunctie in BHK is dit op eerste gezicht weinig verrassend; de betekenis van een disjunctie is simpelweg een verzwakking van een van de disjuncten, terwijl in het bewijs ervoor nog steeds blijkt welk van de disjuncten bewezen is en welk slechts dood gewicht meebrengt. Met de disjunctie-eigenschap heeft de disjunctie geen zelfstandige logische kracht, het is slechts een omkeerbare vertroebeling van het disjunct. Dit is anders in een formule als $\forall x A(x) \vee B(x)$, daar bevat de disjunctieve formule $A(x) \vee B(x)$ nog vrije variabelen en drukt disjunctie een gedeelde eigenchap uit over het gehele kwantorbereik. De disjunctie-eigenschap voltrekt zich daarom geheel op het propositionele deel van **I**, **Ip**, waarin we kwantorhoudende zinnen als atomair beschouwen en iedere formule dus een zin is. Ik zal de termen 'zin' en 'formule' verder uitwisselbaar gebruiken.

De disjunctie-eigenschap van **I** wordt vooral relevant wanneer we naar de bewijssystemen kijken. In deze scriptie behandel ik een Gentzensequentencalculus voor **Ip**: G1ip. De bouwstenen van een G1ip-bewijs zijn *sequenten*, dat zijn objecten van de vorm

$$\Gamma \Rightarrow B$$

[1] Een constructief bewijs is bijvoorbeeld $\sqrt{2}^{(\frac{\log(9)}{\log(2)})} = \sqrt{2^{(\frac{\log(9)}{\log(2)})}} = \sqrt{9} = 3$. Het bewijs van de irrationaliteit van $\frac{\log(9)}{\log(2)}$ niet veel moeilijker dan dat van de irrationaliteit van $\sqrt{2}$.

[2] Nick Bezhanishvili en Dick de Jongh. *Intuitionistic Logic*. Lecture Notes presented at the ESSLLI, Edinburgh, 2005. URL: `http://www.illc.uva.nl/Publications/ResearchReports/PP-2006-25.text.pdf`, p. 25.

waarin Γ een eindige multiverzameling van formules A_i is (een verzameling waarin elementen vaker kunnen voorkomen) en B hooguit één formule. We noemen Γ hier het *antecedent* en B het *succedent* van de sequent. Naar beide wordt verwezen als *cedent*. Verder is de *grootte* van Γ, $|\Gamma|$, de som van het aantal atomaire (deel)formules en het totale aantal voegtekens in Γ. De bovenstaande sequent is qua betekenis equivalent aan de formule

$$\bigwedge_{\Gamma} A_i \to B$$

met dien verstande dat de lege conjunctie altijd waar is en het lege succedent altijd onwaar.

We kunnen sequenten scheppen en manipuleren aan de hand van de volgende afleidingsregels. De gevolgtrekking is telkens van boven naar beneden; Latijnse hoofdletters staan voor hoogstens één willekeurige formule, Griekse hoofdletters voor een eindige multiverzameling formules.

Axioma's

$$A \Rightarrow A \ (A \ atomair) \qquad \bot \Rightarrow \quad L\bot$$

Structurele regels verzwakking (W) en samentrekking (C)

$$\frac{\Gamma \Rightarrow B}{A, \Gamma \Rightarrow B}\ LW \quad (A \ atomair) \qquad \frac{\Gamma \Rightarrow}{\Gamma \Rightarrow D}\ RW \quad (D \ atomair)$$

$$\frac{A, \Gamma \Rightarrow B}{A, A, \Gamma \Rightarrow B}\ LC$$

De snederegel

$$\frac{\Gamma \Rightarrow A \quad A, \Delta \Rightarrow B}{\Gamma, \Delta \Rightarrow B}$$

Propositionele regels

$$\frac{C, D, \Gamma \Rightarrow B}{C \wedge D, \Gamma \Rightarrow B}\ L\wedge \qquad \frac{\Gamma \Rightarrow C \quad \Delta \Rightarrow D}{\Gamma, \Delta \Rightarrow C \wedge D}\ R\wedge$$

$$\frac{C, \Gamma \Rightarrow B \quad D, \Delta \Rightarrow B}{C \vee D, \Gamma, \Delta \Rightarrow B}\ L\vee \qquad \frac{\Gamma \Rightarrow A_i}{\Gamma \Rightarrow A_0 \vee A_1}\ R\vee \quad (i = 0, 1)$$

$$\frac{\Gamma \Rightarrow C \quad D, \Delta \Rightarrow B}{C \to D, \Gamma, \Delta \Rightarrow B}\ L\to \qquad \frac{C, \Gamma \Rightarrow D}{\Gamma \Rightarrow C \to D}\ R\to$$

De sequent onder de streep heet het *consequent*, die boven de streep de *premisse(n)*. De formule die voor het eerst voorkomt in het consequent heet de *hoofdformule* van een afleiding, de rest zijn de *zijformules*(hierboven telkens weergegeven als Γ, Δ en B). De formule die wordt weergegeven als A in de snederegel is de *snedeformule*. We definiëren de *directe voorouders* van een

zijformule in een consequent als de corresponderende zijformule(s) in de premisse(n), en recursief als de directe voorouders van een directe voorouder. Een hoofdformule heeft geen directe voorouders.

In de gebruikelijke definitie van G1ip is de hoofdformule van een verzwakking niet per se atomair. Deze aanpassing zal echter de latere bewijzen een stuk eenvoudiger maken doordat iedere deelformule die in een bewijs voorkomt, ook als formule voorkomt. We zien dat een verzwakking met een complexe formule eenvoudig af te leiden is uit atomaire verzwakkingen en de nodige voegtekenintroducties. Zo'n afleiding waarin de facto met één of meerdere complexe formules wordt verzwakt, geef ik weer met een dubbele lijn, en zal ik ook als 'verzwakking' aanduiden.

Een G1ip-bewijs heeft de vorm van een eindige boom,[3] waarin de bovenste elementen axioma's zijn en de wortel, *de eindsequent*, de conclusie van het bewijs is. We definiëren de grootte van een bewijs P, $|P|$, als het aantal (niet noodzakelijkerwijs verschillende) sequenten in P. In een G1ip-bewijs van een **Ip**-formule A is de eindsequent

$$\Rightarrow A.$$

Dat is immers equivalent met

$$\top \to A \equiv A.$$

(Het verum $\top$ is de atomaire tautologie, hier een afkorting van $\neg\bot \equiv \bot \to \bot$.) Verder geldt dat als een sequent in een bewijs voorkomt, het bovenliggende deel van de boom deze sequent bewijst. We hebben het dan over een *deelbewijs*. Een andere term die nuttig zal blijken is het *conditionele bewijs*: dit is een bewijsboom waarvan de bovenste sequenten niet allemaal axioma's zijn. Het levert een volledig bewijs op op de voorwaarde dat deze beginsequenten zelf ook bewezen worden, in welk geval deze bewijzen aan de bovenkant van het oorspronkelijke bewijs kunnen worden toegevoegd.

We zien eenvoudig dat de afleidingsregels in G1ip de BHK-interpretatie gehoorzamen als we ze uitpakken. Neem bijvoorbeeld de regel $L \to$. Stel dat $\Gamma \Rightarrow C$ en $D, \Delta \Rightarrow B$ constructief gelden, wat erop neerkomt dat

$$\bigwedge_{\Gamma} A_i \to C \quad \text{en} \quad (D \wedge \bigwedge_{\Delta} D_i) \to B$$

constructief gelden. Dit betekent met BHK dat er algoritmes zijn die uit bewijzen van alle $A_i \in \Gamma$ een bewijs voor C vindt, respectievelijk uit bewijzen voor D en alle $D_i \in \Delta$ een bewijs voor B vindt. Als we dan een derde algoritme vinden dat uit een bewijs voor C een bewijs van D weet te construeren, zodat $C \to D$ geldt, kunnen we het eerste en derde algoritme samennemen om uit bewijzen voor de A_i een bewijs van D te verkrijgen, dat samen met de bewijzen voor de D_i door het tweede algoritme kan worden omgezet in een bewijs voor B. Oftewel

$$((C \to D) \wedge \bigwedge_{\Gamma} A_i \wedge \bigwedge_{\Delta} D_i) \to B \quad \equiv \quad C \to D, \Gamma, \Delta \Rightarrow B$$

[3] Preciezer gezegd: een neerwaarts monotone poset met een kleinste element.

geldt constructief. Voor de andere afleidingsregels volgt het analoge resultaat op een vergelijkbare manier. We zien dus dat een G1ip-bewijs van een **Ip**-formule volstaat als een constructie.

De disjunctie-eigenschap van **Ip** geeft daarom nu dat wanneer we een G1ip-bewijs hebben van een disjunctie $\Rightarrow B_0 \vee B_1$, er ook een G1ip-bewijs bestaat van $\Rightarrow B_i$ met $i = 0$ of 1. Bij snedevrije bewijzen (bewijzen waarin geen toepassing van de snederegel voorkomt) kunnen we zo'n bewijs eenvoudig vinden. Bij iedere niet-structurele gevolgtrekkingsstap neemt namelijk de complexiteit van de formules in de sequent toe, zodat we de bewijsboom simpelweg opwaarts kunnen doorlopen totdat we de afleiding vinden waar de disjunctie werd geïntroduceerd (RW). Het deelbewijs boven deze afleiding geeft precies een bewijs van één van de disjuncten. Algemeen geldt voor snedevrije bewijzen dat iedere formule die voorkomt in het bewijs, als deelformule in de eindsequent optreedt (de *deelformule-eigenschap*).

Voor snedehoudende disjunctiebewijzen is het lastiger om de disjunctie-eigenschap te realiseren. Eindigt zo'n bewijs bijvoorbeeld in de snede

$$\frac{\Rightarrow C \quad C \Rightarrow B_0 \vee B_1}{\Rightarrow B_0 \vee B_1}$$

dan zal in het algemeen er geen sequent $\Rightarrow B_i$ in het bewijs voorkomen. De snederegel is zelf af te leiden uit de andere G1ip-regels, wat betekent dat voor ieder snedehoudend bewijs van een sequent $\Gamma \Rightarrow B$, er een snedevrij bewijs van dezelfde eindsequent te vinden is. Bovendien zijn er algoritmes die deze snede-eliminatie kunnen uitvoeren. Het probleem hier is echter dat de grootte van een snedevrij bewijs exponentieel veel groter kan zijn dan die van het snedehoudende bewijs,[4] zodat voor dergelijke bewijzen dit algoritme — snedes elimineren en vervolgens het snedevrije bewijs opwaarts doorlopen — in sommige gevallen praktisch onuitvoerbaar is in termen van benodigde tijd, rekenkracht en geheugen. Het is daarom nog maar de vraag of de disjunctie-eigenschap van **I** te vertalen is naar een parallele eigenschap van de constructieve wiskunde.

Merk bovendien op dat de formulering van de disjunctie-eigenschap klassiek-wiskundig van aard is. Ik heb het over het *bestaan* van bepaalde constructieve bewijzen op een manier die niet afhangt van de kennis ervan, over *construeerbaarheid* zonder de daadwerkelijke constructie te geven. Zodoende heeft de constructivist de klassieke wiskunde nodig om de disjunctie-eigenschap van de constructieve wiskunde te kunnen formuleren. De constructieve wiskunde als zodanig wordt één van de vele onderzoeksvoorwerpen van de klassieke wiskunde, in plaats van een zelfstandig alternatief systeem dat naast de klassieke wiskunde staat.

Mijn doel in dit onderzoek is om de constructieve wiskunde in ieder geval deels uit deze houdgreep te bevrijden: ik zal een praktisch uitvoerbaar algoritme beschrijven dat gegeven een G1ip-bewijs van een disjunctie $\Rightarrow B_0 \vee B_1$, een G1ip-bewijs produceert van een disjunct $\Rightarrow B_i$. Zo geldt dan in ieder geval dat voor iedere wiskundige constructie die een disjunctie aantoont en zich laat

[4] 6, p. 12–14.

vertalen naar een G1ip-bewijs, de disjunctie-eigenschap constructief geldt. (Een ander klassiek-wiskundig resultaat is dat G1ip volledig is voor **Ip**, zodat voor iedere construeerbare **Ip**-formule een G1ip-bewijs bestaat. De daadwerkelijke constructies van deze bewijzen zijn echter niet algemeen gegeven, een algemeen recept om willekeurige constructieve bewijzen te vertalen in G1ip evenmin, dus geeft dit algoritme nog niet de constructieve disjunctie-eigenschap voor alle disjuncties.)

3 Construeerbaarheid als berekenbaarheid

Hoe kunnen we bepalen of een algoritme daadwerkelijk uitvoerbaar is? Dit hangt af van de speciefieke vorm van constructieve wiskunde die we omarmen. Zo neemt het intuïtionisme de wiskunde primair als persoonlijk mentaal construct, eventueel ondersteund door een 'extended mind' van kladpapier. Voor de intuïtionist zijn daarom sommige stellingen alleen al door de hoeveelheid informatie die ze bevatten onbereikbaar; geen mens kan bijvoorbeeld het tienduizenden pagina's tellende bewijs van de classificatiestelling van de eindige enkelboudige groepen geheel bevatten. Dit legt evenzo aan algoritmen strenge beperkingen op.

Meer van deze tijd is een vorm van constructivisme die alle positieve constructies toestaat, ook computerberekeningen. Het is deze vorm die ik verder zal aannemen. Dit heeft als groot voordeel dat we het instrumentarium van de informatica nu ook tot onze beschikking hebben, in het bijzonder de recursieleer en de complexiteitstheorie. Het kernbegrip hier is 'berekenbaarheid'. Het is net als Brouwers 'constructie' een informeel, primitief begrip. Toch bestaat er een algemeen aanvaard maar onbewijssbaar resultaat dat deze notie van berekenbaarheid min of meer vastlegt: de 'stelling' van Church-Turing. Deze zegt dat de berekeningen in deze intuïtieve zin (*calculations*) precies de berekeningen zijn die algoritmisch door een Turing-machine kunnen worden uitgevoerd (*computations*). Een Turing-machine is zogenaamd *model of computation*, een abstract wiskundig object dat, gegeven een invoer, mechanisch beschrijft hoe een uitvoer hieruit kan worden verkregen. Onze computers simuleren allemaal Turing-machines. Omdat we iedere berekening als een constructief bewijs kunnen aanvaarden, zien we met de Church-Turingstelling dat als we een Turingmachine vinden die praktisch altijd uit een intuïtionistisch disjunctiebewijs in een daadwerkelijk uitvoerbare berekening een bewijs van één van de disjuncten produceert — ook als het disjunctiebewijs veel groter wordt — dit dan de disjunctie-eigenschap voor constructieve wiskunde vaststelt.

De uitvoerbaarheid van het algoritme is dan te ontleden in termen van berekeningscomplexiteit. De heilige graal in complexiteitstheorie is *polynomialiteit* van een algoritme: dat houdtin dat de duur van het algoritme (uitgedrukt in het aantal berekeningen) is af te schatten met een veelterm die de grootte van de invoer van het algoritme als argument(en) neemt. Intuïtief betekent dit dat een algoritme altijd relatief snel de berekening voltooit, ook als de invoer veel groter wordt. Een polynomiaal algoritme biedt dus een altijd uitvoerbare constructie.

In de rest van deze scriptie geef ik aan de hand van een bewijsschets van Buss en Pudlak een algoritme dat de disjunctie-eigenschap voor **I** in polynomiale tijd verzilvert.

4 Een algoritme voor snedevrije disjunctiebewijzen

We zagen al dat in snedevrije disjunctiebewijzen eenvoudig de disjunctie-eigenschap kan worden gerealiseerd door het onderhavige bewijs omhoog te doorlopen tot aan afleidingsstap waarin de disjunctie wordt geïntroduceerd. Zo'n strategie laat zich echter moeilijk generaliseren tot snedehoudende bewijzen. In plaats daarvan werken we daarom met SLD-resolutiealgoritmes. Hoe deze er precies uitzien zal ik hier niet uitwerken; het belangrijke is dat ze zogenaamde Hornclausules snel kunnen manipuleren op een voorgeschreven manier, en dat we de sequenten van een intuïtionistisch bewijs kunnen interpreteren als zulke Hornclausules.[5] We hebben de volgende definitie nodig om dit precies te kunnen formuleren.

Definitie. Zij P een eindige multiverzameling van G1ip-sequenten of een bewijs. Dan is de **afsluiting van P**, **Cl(P)**, de kleinste verzameling sequenten die alle sequenten uit P bevat en gesloten is onder snedes en verzwakkingen.

In Schöning [11] wordt beschreven hoe SLD-algoritmes snel zo'n afsluiting kunnen construeren door met verzwakkingen en snedes telkens nieuwe sequenten te vinden:[6]

Bewering 1. *Gegeven een bewijs of een multiverzameling sequenten P, een multiverzameling sequenten Γ en een formule A, kan een SLD-resolutiealgoritme in polynomiale tijd in $|P|$ en $|\Gamma|$ de sequent $\Gamma \Rightarrow$ dan wel de sequent $\Gamma \Rightarrow A$ in $Cl(P)$ herkennen als deze inderdaad in de afsluiting voorkomt.*

We moeten dit voorstellen als een algoritme dat stapsgewijs $Cl(P)$ opbouwt door de sequenten die al in de afsluiting zijn gevonden te verzwakken en waar mogelijk te snijden. Zodoende heeft dit algoritme de volgende twee belangrijke eigenschappen:

(i.) Het algoritme kan gelijktijdig meerdere sequenten zoeken.

(ii.) Als het algoritme een sequent vindt in $Cl(P)$, vindt het een conditioneel bewijs van de sequent waarvan alle beginsequenten in P voorkomen en dat slechts uit verzwakkingen en snedes bestaat.

We zullen dit algoritme toepassen op bewijzen van disjuncties om de bewijzen van de losse disjuncten in de afsluiting te vinden. Daartoe hebben we nog een definitie nodig.

[5] Buss - An Introduction to Proof Theory, 25
[6] 11, p. 117–140.

Definitie. Zij P een bewijs. Dan is de **uitgebreide afsluiting van P**, $\mathbf{Cl^+(P)}$, gedefinieerd als $Cl(S_P)$, waar S_P de verzameling is van alle sequenten in P en de sequenten $A, B \Rightarrow A \wedge B$; $C \Rightarrow C \vee D$; $D \Rightarrow C \vee D$ en $F \Rightarrow E \rightarrow F$ respectievelijk voor de (deel)formules $A \wedge B, C \vee D$ en $E \rightarrow F$ die in P voorkomen.[7]

De extra sequenten die S_P toevoegt zijn allemaal eenvoudig bewijsbaar, zie appendix A.1-4 voor de bewijzen. Samen met de observatie dat de sequenten die in P voorkomen ook al bewezen zijn, geeft eigenschap (ii.) hierboven dat voor een sequent in $Cl^+(P)$ altijd een volledig bewijs bestaat. Merk bovendien op dat $|S_P|$ begrensd is door $3 \cdot |P|$, omdat per (deel)formule van P er maximaal twee nieuwe sequenten in S_P zitten en geen enkele afleidingsregel meer dan één nieuwe formule introduceert, en het aantal afleidingen in P strikt minder is dan het aantal sequenten. Concludeer hieruit dat bewering 1 ook opgaat voor de uitgebreide afsluiting.

We kunnen nu een orakel-Turingmachine construeren die met SLD-resolutiealgoritmes $Cl^+(P)$ doorzoekt en de volgende vijf regels volgt:

1. De machine begint met een bewijs P van een sequent $\Gamma \Rightarrow B_0 \vee B_1$. Aanvankelijk geldt $\Delta \equiv \Gamma$.

2. Als er een conjunctie $C \wedge D$ in Δ zit, vervangt de machine deze door de twee formules C, D.

3. Als Δ een implicatie $C \rightarrow D$ bevat en de machine $\Delta \Rightarrow C$ in $Cl^+(P)$ vindt, dan vervangt de machine $C \rightarrow D$ door D.

4. Als er een disjunctie $C \vee D$ in Δ zit, raadpleegt de machine het orakel, dat vervolgens één disjunct teruggeeft. De machine vervangt $C \vee D$ door het uitgekozen disjunct.

5. Als de machine $\Delta \Rightarrow B_0$ of $\Delta \Rightarrow B_1$ in $Cl^+(P)$ vindt, stopt het algoritme.

Een dergelijke Turing-machine noemen we een *Dp-machine*. Merk op dat het orakel hier een weinig mystieke rol vervult. Iedere keuze levert een werkbare Δ op, zo ook bijvoorbeeld de machine die altijd C kiest. Het orakel in de definitie veralgemeniseert deze arbitraire keuze in de formulering van regel 4.

We zien eenvoudig dat de Dp-machine altijd een regel kan toepassen als P snedevrij is.

Lemma 2 (BP, 2(a))**.** *Zij P een snedevrij bewijs van een sequent $\Delta \Rightarrow B_0 \vee B_1$ waarvoor geldt dat Δ slechts atomaire formules en implicaties bevat. Dan is minstens één van de volgende twee beweringen waar:*

(a) De sequent $\Delta \Rightarrow B_i$ zit in $Cl^+(P)$) voor $i = 0$ of 1.

[7] Deze definitie wijkt af van de definitie van Buss en Pudlák. Zij voegen voor dezelfde deelformules de sequenten $A \wedge B \Rightarrow A$, $A \wedge B \Rightarrow B$, $C \Rightarrow C \vee D$, $D \Rightarrow C \vee D$ en $E \Rightarrow F \rightarrow E$ toe aan de sequenten van P. In de afleidingen in appendix A.5-7 blijkt duidelijk dat alleen de huidige definitie volstaat om middels snedes te garanderen dat de nieuwe sequenten die het algoritme geeft nog in de uitgebreide afsluiting zitten.

(b) Er zit een implicatie $C \to D$ in Δ waarvoor geldt dat $\Delta \Rightarrow C$ in $Cl^+(P)$ zit.

Bewijs.

Beschouw de laatste afleiding van P die niet LW is. Uit de vorm van de eindsequent volgt dat dit een toepassing is van één van de volgende regels: RW, $R\vee$ of $L\to$. In het geval van RW of $R\vee$ volgt (a) direct. Als het een toepassing is van $L\to$ heeft de afleiding de volgende vorm:

$$\frac{\Sigma \;\Rightarrow\; C \qquad D, \Pi \;\Rightarrow\; B_0 \vee B_1}{C \to D, \Sigma, \Pi \;\Rightarrow\; B_0 \vee B_1}$$

De volgende (structurele) afleiding bewijst (b):

$$\frac{\Sigma \;\Rightarrow\; C}{\Delta \;\Rightarrow\; C}$$

■

Wanneer de Dp-machine regel 2, 3 of 4 toepast, blijft $\Delta \Rightarrow B_0 \vee B_1$ in de uitgebreide afsluiting van P (zie appendix A.5-7). We vinden daarom een bewijs Q van $\Delta \Rightarrow B_0 \vee B_1$ dat naast de sequenten uit S_P slechts snedes en verzwakkingen bevat, waaruit direct volgt dat $Cl^+(Q) \subseteq Cl^+(P)$. Het enige wat ons nu ervan weerhoudt dit proces te itereren, is de mogelijke aanwezigheid van snedes in P'. Als we in het algemeen de snedes uit een bewijs kunnen wegwerken zonder de uitgebreide afsluiting te vergroten, kunnen we bewijzen dat de Dp-machine altijd in polynomiale tijd stopt. Ik laat in de volgende paragraaf zien hoe we zo'n snede-eliminatie kunnen verwezenlijken.

5 Snede-eliminatie

Stelling 3 (BP, 1)**.** *Zij P een* G1ip*-bewijs van $\Gamma \Rightarrow A$. Dan bestaat er een snedevrij bewijs P' van $\Gamma \Rightarrow A$ zodanig dat $Cl^+(P') \subseteq Cl^+(P)$.*

Bewijs. Merk ten eerste op dat het volstaat een snedevrij bewijs P' van $\Gamma \Rightarrow A$ te vinden waarvan iedere sequent in $Cl(P)$ zit. Iedere (deel)formule in P' is immers al deelformule van $\Gamma \Rightarrow A$ (de deelformule-eigenschap) en dus een deelformule in P. Bovendien geldt voor zo'n P' dat $Cl(P') \subseteq Cl(P)$.

We construeren het nieuwe bewijs door alle snedes in P weg te werken middels inductie op de complexiteit van de snedeformule. Snedes op complexe formules worden naar boven verplaatst in het bewijs, waardoor de snedeformule eenvoudiger wordt; snedes op atomaire formules zijn elegant te elimineren.

Neem een deelbewijs van P dat eindigt in de snede

$$\frac{\begin{array}{cc} Q & R \\ \vdots & \vdots \\ \Gamma_1 \;\Rightarrow\; A & A, \Gamma_2 \;\Rightarrow\; C \end{array}}{\Gamma_1, \Gamma_2 \;\Rightarrow\; C}$$

We noemen de sequenten van Q die een directe voorouder van A in het succedent bevatten het *onderste deel van* Q, en de sequenten van R die een directe voorouder van A in het antecedent bevatten het *onderste deel van* R. De bovengrens van het onderste deel van een deelbewijs bestaat uit alle afleidingen waarin de snedeformule wordt geïntroduceerd. Wanneer zo'n afleiding een verzwakkingsafleiding is, is deze zonder meer te vervangen door een verzwakking die een willekeurige andere cedent introduceert. Daardoor zullen in de rest van dit bewijs deze gevallen triviaal blijken. Een bijzonder geval is nog dat de snedeformule $\bot$ is; succedentintroductie is dan altijd een verzwakking, zodat een bewijs Q' te verkijgen is uit Q door iedere sequent $\Pi \Rightarrow \ \bot$ waarin $\bot$ een directe voorouder van de snedeformule is, te vervangen door $\Pi \Rightarrow C$. Het nieuwe bewijs wordt

$$\dfrac{\begin{array}{c} Q' \\ \Gamma_1 \ \Rightarrow \ C \end{array}}{\Gamma_1, \Gamma_2 \ \Rightarrow \ C}$$

We kunnen in het vervolg zonder verlies van algemeenheid aannemen dat de snedeformule niet in een verzwakking wordt geïntroduceerd.

Inductiestart: A is atomair. De snede kan als volgt worden geëlimineerd: vervang iedere sequent $\Pi \Rightarrow A$ in Q waarin A als directe voorouder van de snedeformule voorkomt door $\Pi, \Gamma_2 \Rightarrow C$. Als deze sequent een axioma van Q was (en dus $\Pi \equiv A$), vervang deze dan als volgt door een kopie van R:

$$\begin{array}{c} R \\ A, \Gamma_2 \ \Rightarrow \ C \\ Q' \\ \Gamma_1, \Gamma_2 \ \Rightarrow \ C \end{array}$$

Alle nieuwe sequenten $\Pi, \Gamma_2 \Rightarrow C$ in het bewijs komen voor in $Cl(P)$, als gevolg van de snede

$$\dfrac{\Pi \ \Rightarrow \ A \qquad A, \Gamma_2 \ \Rightarrow \ C}{\Pi, \Gamma_2 \ \Rightarrow \ C}$$

Inductiestap. Neem als inductiehypothese telkens aan dat snedes op een snedeformule B of D kunnen worden geëlimineerd binnen de afsluiting van P.

Geval 1: A is een conjunctie $B \wedge D$. De bovengrens van het onderste deel van Q bestaat uit k afleidingen met een directe voorouder van de snedeformule als hoofdformule:

$$\dfrac{\begin{array}{c} Q^i_B \\ \Pi_i \ \Rightarrow \ B \end{array} \qquad \begin{array}{c} Q^i_D \\ \Pi'_i \ \Rightarrow \ D \end{array}}{\Pi_i, \Pi'_i \ \Rightarrow \ B \wedge D}$$

voor $i = 1, ..., k$.
Vergelijkbaar zijn er m deelbewijzen R_j van R met een directe voorouder van de snedeformule als hoofdformule:

$$\dfrac{\begin{array}{c}\vdots \\ X_j, \Delta_j \ \Rightarrow \ F_j\end{array}}{B \wedge D, \Delta_j \ \Rightarrow \ F_j}$$

voor $j = 1, ..., m$ en waar X_j gelijk is aan B of D.
Voor iedere $i = 1, ..., k$ kan nu een bewijs R^i als volgt uit R worden verkregen. Vervang eerst de laatste afleiding van iedere R_j door een snede en verzwakkingen:

$$\dfrac{\dfrac{\begin{array}{c}Q^i_{X_j} \\ \vdots \\ \Pi_i^{(\prime)} \ \Rightarrow \ X_j\end{array} \qquad \begin{array}{c}\vdots \\ X_j, \Delta_j \ \Rightarrow \ F_j\end{array}}{\Pi_i^{(\prime)}, \Delta_j \ \Rightarrow \ F_j}}{\Pi_i, \Pi_i', \Delta_j \ \Rightarrow \ F_j}$$

Vervang vervolgens in de rest van het onderste deel van R de directe voorouders van de snedeformule elk door de cedent Π_i, Π_i', om zodoende een bewijs R^i van $\Pi_i, \Pi_i', \Gamma_2 \Rightarrow C$ te krijgen.
Als we nu ieder deelbewijs Q^i van P door R^i vervangen en iedere sequent $\Pi \Rightarrow B \wedge D$ in het onderste deel van Q door $\Pi, \Gamma_2 \Rightarrow C$, geeft dit een bewijs van $\Gamma_1, \Gamma_2 \Rightarrow C$ waaruit de snede op $B \wedge D$ is geëlimineerd.
De nieuwe sequenten $\Pi_i, \Pi_i', \Delta \Rightarrow F$ uit R^i zijn in $Cl(P)$ terug te vinden door de snede

$$\dfrac{\Pi_i, \Pi_i' \ \Rightarrow \ B \wedge D \qquad B \wedge D, \Delta \ \Rightarrow \ F}{\Pi_i, \Pi_i', \Delta \ \Rightarrow \ F}$$

De nieuwe sequenten van de vorm $\Pi, \Gamma_2 \Rightarrow C$ zitten in de afsluiting van P door

$$\dfrac{\Pi \ \Rightarrow \ B \wedge D \qquad B \wedge D, \Gamma_2 \ \Rightarrow \ C}{\Pi, \Gamma_2 \ \Rightarrow \ C}$$

Geval 2: A is een disjunctie $B \vee D$. We kijken wederom naar de bovengrens van het onderste deel van Q, ditmaal bestaande uit k afleidingen met een directe voorouder van de snedeformule als hoofdformule:

$$\dfrac{\begin{array}{c}Q^i \\ \vdots \\ \Pi_i \ \Rightarrow \ X_i\end{array}}{\Pi_i \ \Rightarrow \ B \vee D}$$

voor $i = 1, ..., k$ en X_j is gelijk aan B of D.
De bovengrens van het onderste deel van R bestaat uit de eindsequenten van deelbewijzen R_j die een directe voorouder van de snedeformule als hoofdformule hebben:

$$\frac{\begin{array}{cc} \vdots & \vdots \\ B, \Delta_j \Rightarrow F_j & D, \Delta'_j \Rightarrow F_j \end{array}}{B \vee D, \Delta_j, \Delta'_j \Rightarrow F_j}$$

voor $j = 1, ..., m$.
Voor iedere $i = 1, ..., k$ is een bewijs R^i uit R als volgt te verkrijgen. Vervang eerst de laatste afleiding van elke R_j door een snede en verzwakkingen:

$$\dfrac{\dfrac{\begin{array}{cc} Q^i & \\ \vdots & \\ \Pi_i \Rightarrow X_i & \end{array} \qquad \begin{array}{cc} \vdots & \\ X_i, \Delta_j^{(\prime)} \Rightarrow F_j & \end{array}}{\Pi_i, \Delta_j^{(\prime)} \Rightarrow F_j}}{\Pi_i, \Delta_j, \Delta'_j \Rightarrow F_j}$$

Vervang vervolgens in de rest van het onderste deel van R de directe voorouders van de snedeformule elk door de cedent Π_i, om zodoende een bewijs R^i van $\Pi_i, \Gamma_2 \Rightarrow C$ te krijgen.
Als we nu ieder deelbewijs Q^i van P door R^i vervangen en iedere sequent $\Pi \Rightarrow B \vee D$ in het onderste deel van Q door $\Pi, \Gamma_2 \Rightarrow C$, geeft dit een bewijs van $\Gamma_1, \Gamma_2 \Rightarrow C$ waaruit de snede op $B \vee D$ is geëlimineerd.
De nieuwe sequenten $\Pi_i, \Delta \Rightarrow F$ uit R^i zijn in $Cl(P)$ terug te vinden door de snede

$$\frac{\Pi_i \Rightarrow B \vee D \qquad B \vee D, \Delta \Rightarrow F}{\Pi_i, \Delta \Rightarrow F}$$

De nieuwe sequenten van de vorm $\Pi, \Gamma_2 \Rightarrow C$ zitten in de afsluiting van P door

$$\frac{\Pi \Rightarrow B \vee D \qquad B \vee D, \Gamma_2 \Rightarrow C}{\Pi, \Gamma_2 \Rightarrow C}$$

Geval 3: A is een implicatie $B \to D$. De bovengrens van het onderste deel van Q bestaat nu uit k afleidingen met een directe voorouder van de snedeformule als hoofdformule van de vorm

$$\frac{\begin{array}{cc} Q^i & \\ \vdots & \\ \Pi_i, B \Rightarrow D & \end{array}}{\Pi_i \Rightarrow B \to D}$$

voor $i = 1, ..., k$.
De bovengrens van het onderste deel van R bestaat uit de eindsequenten van deelbewijzen R_j die een directe voorouder van de snedeformule als hoofdformule hebben:

$$\dfrac{\begin{array}{cc}\vdots & \vdots \\ \Delta_j \Rightarrow B & D, \Delta'_j \Rightarrow F_j\end{array}}{B \to D, \Delta_j, \Delta'_j \Rightarrow F_j}$$

voor $j = 1, ..., m$.
Voor iedere $i = 1, ..., k$ kan nu een bewijs R^i als volgt uit R worden verkregen. Vervang ten eerste de laatste afleiding van iedere R_j door twee snedes:

$$\dfrac{\dfrac{\begin{array}{cc}\vdots & \overset{Q^i}{\vdots} \\ \Delta_j \Rightarrow B & \Pi_i, B \Rightarrow D\end{array}}{\Pi_i, \Delta_j \Rightarrow D} \qquad \begin{array}{c}\vdots \\ D, \Delta'_j \Rightarrow F_j\end{array}}{\Pi_i, \Delta_j, \Delta'_j \Rightarrow F_j}$$

Vervang vervolgens in de rest van het onderste deel van R de directe voorouders van de snedeformule elk door de cedent Π_i, om zodoende een bewijs R^i van $\Pi_i, \Gamma_2 \Rightarrow C$ te krijgen.
Als we nu ieder deelbewijs Q^i van P door R^i vervangen en iedere sequent $\Pi \Rightarrow B \to D$ in het onderste deel van Q door $\Pi, \Gamma_2 \Rightarrow C$, geeft dit een bewijs van $\Gamma_1, \Gamma_2 \Rightarrow C$ waaruit de snede op $B \to D$ is geëlimineerd.
De nieuwe sequenten $\Pi_i, \Delta \Rightarrow F$ uit R^i zijn in $Cl(P)$ terug te vinden door de snede

$$\dfrac{\Pi_i \Rightarrow B \to D \qquad B \to D, \Delta \Rightarrow F}{\Pi_i, \Delta \Rightarrow F}$$

De nieuwe sequenten van de vorm $\Pi, \Gamma_2 \Rightarrow C$ zitten in de afsluiting van P door

$$\dfrac{\Pi \Rightarrow B \to D \qquad B \to D, \Gamma_2 \Rightarrow C}{\Pi, \Gamma_2 \Rightarrow C}$$

■

Hiermee volgt direct de veralgemenisering van lemma 2.

Corollarium 4. *Zij P een snedehoudend bewijs van een sequent $\Delta \Rightarrow B_0 \vee B_1$ waarvoor geldt dat Δ slechts atomaire formules en implicaties bevat. Ook dan is minstens één van de volgende twee beweringen waar:*

(a) De sequent $\Delta \Rightarrow B_i$ zit in $Cl^+(P))$ voor $i = 0$ of 1.

(b) Er zit een implicatie $C \to D$ in Δ waarvoor geldt dat $De \Rightarrow C$ in $Cl^+(P)$ zit.

Bewijs. Stelling 1 geeft een snedevrij bewijs P' van $\Delta \Rightarrow B_0 \vee B_1$ met $Cl^+(P') \subseteq Cl^+(P)$. Een toepassing van lemma 2 op P' geeft vervolgens dit resultaat.

■

6 Het disjunctie-eigenschapalgoritme

We kunnen nu bewijzen dat een Dp-machine voor elk disjunctiebewijs in polynomiale tijd stopt.

Stelling 5. *Zij P een bewijs van $\Gamma \Rightarrow B_0 \vee B_1$. Dan geeft een Dp-machine in polynomiale tijd in $|P|$ en $|\Gamma|$ een bewijs voor $\Delta \Rightarrow B_0$ of voor $\Delta \Rightarrow B_1$.*

Bewijs.

- We zagen al in paragraaf 4 dat als de machine regel 2, 3 of 4 toepast de sequent $\Delta \Rightarrow B_0 \vee B_1$ in $Cl^+(P)$ blijft, en dat er dan ook meteen een bewijs P' van $\Delta \Rightarrow B_0 \vee B_1$ bekend is met $Cl^+(P') \subseteq Cl^+(P)$.
- Er kan altijd minstens één van de regels worden toegepast: als er geen conjuncties en disjuncties (meer) in Δ zitten, garanderen lemma 2 en corollarium 4 (met betrekking tot de P' die met de onderhavige Δ correspondeert) dat ofwel regel 3, dan wel regel 5 toepasbaar is.
- $|\Delta|$ neemt bij elke toepassing van regel 2, 3 en 4 af, dus het aantal regeltoepassingen voordat de machine stopt, i.e. regel 5 toepast, is begrensd door $|\Gamma|$.
- Elke regeltoepassing geschiedt in polynomiale tijd in $|P|$ en $|\Gamma|$, zo snel kan immers een sequent in $Cl^+(P)$ herkend worden.

Dit voltooit het bewijs.

■

Corollarium 6. *De disjunctie-eigenschap van **I** is in polynomiale tijd in* G1ip *te realiseren.*

Bewijs. Zij P een bewijs van een sequent $\Rightarrow B_0 \vee B_1$. Dit is een bijzonder geval van stelling 5 met $\Gamma \equiv \varnothing$. Regels 2, 3 en 4 zijn daarom niet toepasbaar, zodat regel 5 toepassing vindt: de Dp-machine vindt in polynomiale tijd een bewijs voor $\Rightarrow B_i$ met $i = 0$ of 1.

■

7 De gegeneraliseerde disjunctie-eigenschap

Het resultaat van stelling 5 is een stuk sterker dan slechts de constructieve verwezenlijking van de intuïtionistische disjunctie-eigenschap. We kunnen namelijk vrij veel zeggen over de Δ die de machine produceert uit een niet-lege Γ. De toepassingen van regels 2 en 3 zijn namelijk onmiddelijk omkeerbaar met de regels $L\wedge$ en $L\rightarrow$ respectievelijk. Regel 4 daarentegen niet. Door één van disjuncten te kiezen kan Δ sterker zijn dan Γ. Neem bijvoorbeeld het volgende simpele disjunctiebewijs:

Voorbeeld 1.

$$\dfrac{\dfrac{B \Rightarrow B}{B \Rightarrow B \vee C} \qquad \dfrac{C \Rightarrow C}{C \Rightarrow B \vee C}}{B \vee C \Rightarrow B \vee C}$$

Stap 1: $\Delta \equiv B \vee C$
Stap 2: toepassing van regel 4. Het orakel kiest B. $\Delta \equiv B$.
Stap 3: toepassing van regel 5. De machine vindt $B \Rightarrow B$ *in* $Cl^+(P)$.

We zien dat niet algemeen kan gelden dat er ook een bewijs $\Gamma \Rightarrow B_i$ uit een disjunctiebewijs $\Gamma \Rightarrow B_0 \vee B_1$. In dit voorbeeld zou dat een bewijs opleveren van $B \vee C \Rightarrow B$, wat zeker niet altijd geldt!

Harrop (citeer) toonde echter aan dat voor een belangrijke categorie formules deze algemenere versie van de disjunctie-eigenschap wel geldt: als een sequent $\Gamma \Rightarrow A \vee B$ bewijsbaar is, met Γ een multiverzameling van zogenaamde *Harrop-formules*, dan is $\Gamma \Rightarrow A$ of $\Gamma \Rightarrow B$ ook bewijsbaar. Ik geef de definitie.

Definitie. 1. iedere atomaire formule is Harrop, waaronder $\perp$;

2. als A en B Harrop-formules zijn, is $A \wedge B$ ook Harrop;

3. als B Harrop is, is $A \rightarrow B$ ook Harrop voor willekeurige A;

4. geen andere formule is Harrop.

We kunnen ook deze gegeneraliseerde disjunctie-eigenschap constructief verwezenlijken met behulp van stelling 5.

Stelling 7. *Er is een algoritme dat gegeven een* G1ip*-bewijs van* P *van een sequent*

$$A_1, ..., A_n \Rightarrow B_1 \vee ... \vee B_m,$$

met de A_k *Harrop-formules, in polynomiale tijd in* $|P|$ *en* $|\{A_1, ..., A_n\}|$ *een bewijs* P' *vindt van*

$$A_1, ..., A_n \Rightarrow B_i$$

voor een $1 \leq i \leq m$.

Bewijs. We zien dat het bewijs voor lemma 2 onveranderd ook de generalisatie met $\Gamma \Rightarrow B_1 \vee ...ovB_m$ aantoont, en corollarium 4 volgt ook op precies dezelfde manier. Als we regels 1 en 5 voor de Dp-machine vervolgens aanpassen om m disjuncten in het succedent te faciliteren, kunnen we wederom een Turing-machine vinden die de regels volgt en met SLD-resolutiealgoritmes $Cl^+(P)$ doorzoekt: de *gDp-machine*. We zien dat als Δ slechts Harrop-formules bevat, na toepassing van regel 2 of 3 dit voor de nieuwe Δ nog steeds geldt, en dus dat regel 4 nooit wordt toegepast. Precies als in stelling 5 vindt deze machine in polynomiale tijd een bewijs voor $\Delta \Rightarrow B_i$, waarna zoals opgemerkt uit Δ weer Γ kan worden bewezen door in omgekeerde volgorde van de toepassingen van regels 2 en 3 respectievelijk de afleidingen $L\wedge$ en $L\rightarrow$ te maken op de corresponderende formules.

■

Harrop-formules worden veelvuldig gebruikt in de informatica en de constructieve wiskunde, wat dit tot een aardig resultaat maakt.

8 G3ip

Er is een andere Gentzensequentencalculus voor intuïtionistische propositielogica waarin alle structurele regels zijn geabsorbeerd: G3ip. Dit is een zeer nuttige eigenschap wanneer je 'opwaarts' een bewijs wilt vinden, dat wil zeggen door bij de eindsequent te beginnen en de complexiteit van de formules die voorkomen stap voor stap te ontleden. De definities zijn als volgt.
Axioma's

$$A, \Gamma \Rightarrow A \ (A \ atomair) \qquad \bot, \Gamma \Rightarrow A \quad L\bot$$

De snederegel

$$\frac{\Gamma \Rightarrow A \quad A, \Delta \Rightarrow B}{\Gamma, \Delta \Rightarrow B}$$

Propositionele regels

$$\frac{C, D, \Gamma \Rightarrow B}{C \wedge D, \Gamma \Rightarrow B} \ L\wedge \qquad \frac{\Gamma \Rightarrow C \quad \Delta \Rightarrow D}{\Gamma, \Delta \Rightarrow C \wedge D} \ R\wedge$$

$$\frac{C, \Gamma \Rightarrow B \quad D, \Delta \Rightarrow B}{C \vee D, \Gamma, \Delta \Rightarrow B} \ L\vee \qquad \frac{\Gamma \Rightarrow A_i}{\Gamma \Rightarrow A_0 \vee A_1} \ R\vee \quad (i = 0, 1)$$

$$\frac{C \rightarrow D, \Gamma \Rightarrow C \quad D, \Delta \Rightarrow B}{C \rightarrow D, \Gamma, \Delta \Rightarrow B} \ L\rightarrow \qquad \frac{C, \Gamma \Rightarrow D}{\Gamma \Rightarrow C \rightarrow D} \ R\rightarrow$$

Het is daarom de moeite waard om na te gaan of het resultaat van de constructieve realisatie van de disjunctie-eigenschap ook voor G3ip opgaat. Dat blijkt het geval.

Om dit te bewijzen, laat ik eerst zien hoe G3ip verzwakkingen heeft ingelijfd. Neem daartoe een G3ip-bewijs van een sequent $\Gamma \Rightarrow A$, die we links willen verzwakken met Δ. In plaats van een extra afleiding onder het bewijs aan te voegen, transformeert een verzwakking in G3ip het hele bewijs. Voeg simpelweg de Δ toe aan het succedent van de eindsequent en van iedere bovenliggende sequent, tot en met de axioma's, die in G3ip deze zijformules toestaan. Het nieuwe, verzwakte bewijs heeft nu dezelfde lengte. De rechtsverzwakking gaat geheel analoog.

De definitie van de grootte van een bewijs zullen we ook wat moeten aanpassen in G3ip, omdat verzwakkinngsformules hier niet meer atomair hoeven te zijn: $|P|$ is in dit geval de som van het aantal sequenten in P en de groottes van alle zijformules in de beginsequenten van P.

Stelling 8. *Stelling 5, corollarium 6 en stelling 7 gelden ook voor* G3ip.

Bewijs. Omdat G3ip geen verzwakkingen maar verzwakkingstransformaties kent, is de strategie van paragrafen 4, 5 en 6 in dit geval niet te reproduceren. In plaats daarvan zullen we al het rekenwerk in G1ip uitvoeren, om het gevonden bewijs vervolgens om te zetten in een G3ip-bewijs.

Zij P een G3ip-bewijs van een sequent $\Gamma \Rightarrow B_0 \vee B_1$. Dan is P ook een conditioneel G1ip-bewijs: alle afleidingsregels in P zijn ook geldig in G1ip als we $L \rightarrow_{\mathsf{G3ip}}$ interpreteren als $L \rightarrow_{\mathsf{G1ip}}$ gevolgd door een samentrekking. We passen stelling 5 toe en krijgen in polynomiale tijd in $|P|$ en $|\Gamma|$ een (conditioneel) G1ip-bewijs P' van $\Gamma \Rightarrow B_i$, dat slechts sequenten uit S_P en snedes en verzwakkingen bevat. Als we deze verzwakkingen vervolgens wegtransformeren op de bovenbeschreven wijze, vinden we een bewijs P'' dat slechts verzwakte sequenten uit P en snedes bevat. P'' is dus een geldig G3ip-bewijs van $\Gamma \Rightarrow B_i$. Dan hoeven we alleen nog aan te tonen dat de verzwakkingstransformaties zich in polynomiale tijd voltrekken. Er zijn strikt meer sequenten dan afleidingen in een bewijs, zodat het aantal verzwakkingen kleiner is dan $|P'|$, en per verzwakking is het aantal bovenliggende sequenten duidelijk ook minder dan $|P'|$, zodat het aantal sequenttransformaties dat P' in P'' omzet is af te schatten op $|P'|^2$. Verder werd P' in polynomiale tijd gevonden, en is dus in het bijzonder niet van bovenpolynomiale grootte. Dus P'' is ook in polynomiale tijd in $|P|$ en $|\Gamma|$ te vinden.

Het equivalent van corollarium 6 volgt wederom direct: neem simpelweg $\Gamma \equiv \varnothing$.

Het equivalent van stelling 7 volgt door overal in het bovenbeschreven bewijs een sequent $A_1, ..., A_n \Rightarrow B_1 \vee ... \vee B_m$ (met de A_k Harrop-formules) te nemen in plaats van $\Gamma \Rightarrow B_0 \vee B_1$ en stelling 7 in te roepen in plaats van stelling 5.

■

9 Conclusie

Uit de disjunctie-eigenschap van **I** volgt dat een disjunctie in **Ip** geen zelfstandige logische status heeft; deze bestaat slechts in de omkeerbare verhulling van

een van zijn deelformules. Omdat **I** de gevolgtrekkingsstructuur van de constructieve wiskunde beschrijft, geldt daar een equivalente bewering: als een een disjunctie $A \vee B$ constructief bewijsbaar is, dan bestaat er ook een constructief bewijs van A of van B. De vaststelling van deze eigenschap is zelf een klassiek-wiskundige uitspraak, het bewijs voor het disjunct 'bestaat' zonder dat het daadwerkelijk gevonden is, of dat er algoritmische instructies zijn voor een constructie. Want hoewel het gezien de BHK-interpretatie onaannemelijk lijkt, zagen we dat er constructieve disjunctiebewijzen van $A \vee B$ zijn die niet al een bewijs van A of van B als zodanig omvatten. Deze hebben de vorm van snedehoudende G1ip-bewijzen. De disjunctie-eigenschap garandeert hier de mogelijkheid een constructief bewijs te vinden van een disjunct, maar biedt geen constructie. Voor de constructivist is dit dus ontoegankelijk: hij heeft de klassieke wiskunde nodig om de disjunctie-eigenschap van de constructieve wiskunde te formuleren. Een constructieve versie (de constructivistische disjunctie-eigenschap van de constructieve wiskunde) vereist daarom een manier om uit zo'n constructief disjunctiebewijs altijd een bewijs van een van de disjuncten te verkrijgen. Die heb ik gegeven met de Dp-machine van paragraaf 4. De constructieve wiskunde wordt daarmee in dit opzicht een zelfkennend systeem: het is mogelijk om *binnen* de constructieve wiskunde de disjunctie-eigenschap uit te drukken. Voor een vorm van wiskundig constructivisme die de klassieke wiskunde afwijst, is dit van groot belang. Het is immers moeilijk de zelfstandigheid van het constructieve systeem vol te houden als het voor een ontleding van elementaire feiten als de significantie van een disjunctie is aangewezen op de klassieke wiskunde.

Maar een kanttekening is hier op zijn plaats. Het bewijs dat het gevonden algoritme inderdaad altijd een disjunctbewijs vindt, uiteengezet in paragraaf 5 en 6, is weer klassiek-wiskundig van aard. Het berust weliswaar op een inductief gegeven constructie van een snedevrij bewijs, het probleem is echter dat het aantal manipulaties in deze snede-eliminatie exponentieel is in de grootte van het oorspronkelijke bewijs. Dat betekent dat er grote disjunctiebewijzen zijn waarvan de snede-eliminatie op de manier van stelling 3 praktisch onuitvoerbaar is. Corollarium 4 is daarom een klassiek-wiskundig resultaat: voor ieder bewijs 'is er' een snedevrij bewijs in dezelfde afsluiting dat de gezochte sequenten geeft, ook als dit bewijs in feite onconstrueerbaar is. De constructief wiskundige weet dus niet dat zijn Dp-algoritme inderdaad altijd volstaat.

Een daadwerkelijk onafhankelijke constructieve wiskunde is daarom nog niet in beeld.

A Appendix

1.

$$\dfrac{\dfrac{A \Rightarrow A}{A, B \Rightarrow A} \qquad \dfrac{B \Rightarrow B}{A, B \Rightarrow B}}{A, B \Rightarrow A \wedge B}$$

2.

$$\dfrac{C \Rightarrow C}{C \Rightarrow C \vee D}$$

3.

$$\dfrac{D \Rightarrow D}{D \Rightarrow C \vee D}$$

4.

$$\dfrac{\dfrac{F \Rightarrow F}{E, F \Rightarrow F}}{F \Rightarrow E \to F}$$

5. Regel 2

$$\dfrac{C, D \Rightarrow C \wedge D \qquad C \wedge D, \Sigma \Rightarrow B_0 \vee B_1}{C, D, \Sigma \Rightarrow B_0 \vee B_1}$$

6. Regel 3

$$\dfrac{D \Rightarrow C \to D \qquad C \to D, \Sigma \Rightarrow B_0 \vee B_1}{D, \Sigma \Rightarrow B_0 \vee B_1}$$

7. Regel 4

$$\dfrac{C \Rightarrow C \vee D \qquad C \vee D, \Sigma \Rightarrow B_0 \vee B_1}{C, \Sigma \Rightarrow B_0 \vee B_1}$$

8.

$$\dfrac{\dfrac{A \Rightarrow A}{\Rightarrow A \to A} \qquad \dfrac{\dfrac{B \Rightarrow B}{B \Rightarrow B \vee C} \qquad \dfrac{C \Rightarrow C}{C \Rightarrow B \vee C}}{B \vee C \Rightarrow B \vee C}}{(A \to A) \to (B \vee C) \Rightarrow B \vee C}$$

Stap 1: $\Delta \equiv (A \to A) \to (B \vee C)$.

Stap 2: toepassing van regel 3. De machine vindt $(A \to A) \to (B \vee C) \Rightarrow A \to A$ in $Cl^+(P)$:

$$\dfrac{\dfrac{A \Rightarrow A}{\Rightarrow A \to A}}{(A \to A) \to (B \vee C) \Rightarrow A \to A}$$

$\Delta \equiv B \vee C$.

Stap 3: toepassing van regel 4. Het orakel kiest B. $\Delta \equiv B$.

Stap 4: toepassing van regel 5. De machine vindt $B \Rightarrow B$ in $Cl^+(P)$.

Verantwoording

Het beeld van de constructieve wiskunde dat ik schets is hoofdzakelijk geïnspireerd door Brouwer [4] en Heyting [9], met moderner vergelijkingsmateriaal uit Bridges en Palmgren [3], Bauer [1] en Bishop [2]. Het bewijs van het hoofdresultaat van dit onderzoek (§4-6) en de generalisatie (§7) komt goeddeels uit Buss en Pudlák [10]. Ik heb het waar nodig zelf aangevuld en verbeterd. Het bewijs van stelling 8 is van eigen hand.

De definities van G1ip en G3ip komen uit Troelstra en Swichtenberg [8], met dien verstande dat bij hen deze systemen geen snederegel kennen en verzwakkingsformules niet slechts atomair zijn. Talloze andere definities zijn rechtstreeks ontleend aan Buss [5] of kleine aanpassingen daarvan.

Referenties

[1] Andrej Bauer. "Five Stages of Accepting Constructive Mathematics". In: *Bulletin of the American Mathematical Society* 3 (2017), p. 481–498.

[2] Errett Bishop. "The Crisis in Contemporary Mathematics". In: *Historia Mathematica* 2 (1975), p. 507–517.

[3] Erik Bridges Douglas en Palmgren. "Constructive Mathematics". In: *Stanford Encyclopedia of Philosophy* (Summer 2018). URL: `https://plato.stanford.edu/archives/sum2018/entries/mathematics-constructive/`.

[4] L.E.J. Brouwer. *Over de grondslagen der wiskunde*. Amsterdam: Maas Van Suchtelen, 1907.

[5] Samuel R. Buss. "Chapter I: An Introduction to Proof Theory". In: *Handbook of Proof Theory*. Red. door S.R. Buss. Elsevier Science, 1998.

[6] A. Carbone. "Duplication of directed graphs and exponential blow up of proofs". In: *Annals of Pure and Applied Logic* 100 (1999), p. 1–67.

[7] Nick Bezhanishvili en Dick de Jongh. *Intuitionistic Logic*. Lecture Notes presented at the ESSLLI, Edinburgh, 2005. URL: `http://www.illc.uva.nl/Publications/ResearchReports/PP-2006-25.text.pdf`.

[8] A.S. Troelstra en H. Swichtenberg. *Basic Proof Theory*. Cambridge: Cambridge University Press, 1996.

[9] A. Heyting. *Intuitionism: an Introduction*. Amsterdam: North Holland Publishing Company, 1971.

[10] Samuel R. Buss en Pavel Pudlák. "On the computational content of intuitionistic propositional proofs". In: *Annals of Pure and Applied Logic* 109.1-2 (2001), p. 49–64.

[11] Uwe Schöning. *Logic for Computer Scientists*. Boston: Birkhäuser, 1989.