INLEIDING WISKUNDIGE LOGICA

Woord vooraf

Deze tekst is een bewerking en uitbreiding van een syllabus die ik in 1983 geschreven heb voor een eerste semester-college aan de Rijksuniversiteit te Groningen. Hij verscheen destijds als wekelijks feuilleton. Mijn assistent, Frank de Boer, nam mij zoveel werk uit handen dat dat kon. Daar ben ik hem dankbaar voor.

Het bewerken en uitbreiden was trouwens ook een grotere klus dan ik had gedacht. In eerste instantie heb ik opnieuw gebruik moeten maken van het feuilletonsysteem. Deze keer was het Rogier Jacobsz dankzij wiens assistentie de studenten elke week de kennis in hun tas konden vermeerderen.

Bij nader inzien ligt een en ander toch niet zo eenvoudig als we in ons jeugdig optimisme suggereerden; en samen met de aangroei van extra onderwerpen waar ooit vraag naar was, heeft dat op de lange duur geleid tot een document waar te veel in staat om in een enkel eerstejaarssemester door te nemen. Men moet zich daar niet door af laten schrikken.

Een belangrijke kwaliteit van dit werk is dat het in de Nederlandse taal is geschreven. Er heerst dezer dagen een zekere druk om serieuze gedachten te verwoorden in het Euro-Engels. Meer mensen zouden er dan kennis van kunnen nemen. Het spreekt echter niet vanzelf dat men in het Engels kennis zou willen nemen van iets dat in het Nederlands een sonnet was. En a fortiori ligt het voor de hand dat bepaalde gedachten zich in de ene taal beter, of tenminste *anders*, uit laten drukken dan in de andere. Yourcenar [Y] was die mening toegedaan:

> 'Martin [een Keulse bankier], qui avait fait apprendre aux deux filles le parler français, si convenable aux femmes, s'en servait lui-même quand il lui arrivait d'avoir à exprimer des idées plus déliées ou plus relevées que celles des jours ouvrables'

— nuchtere ideeën, zoals die van de logica, formuleert men dus beter in het Rijnlands[1]. Bij sommige buitenlandse auteurs bespeurt men zelfs een zekere jaloezie. Zo schrijft Bell [DM] over het intuïtionisme:

> 'The primary revelations of the creed are veiled in the Dutch language. German and English expositions are available; but it is said by converts with expert knowledge of both the languages and the mathematics that only those who can think in Dutch can grasp the finer shades of meaning…'

Mijn behandeling van het onderwerp is, naar mijn inschatting, nauwgezet, maar niet formalistisch. Voor een inleiding in de wiskundige logica is ze nogal filosofisch. Ik heb me niet bijzonder ingespannen om indrukwekkende wiskundige toepassingen te presenteren — geen infinitesimaalrekening[2] of algebraï-

---

[1] In de oren van Y. vermoedelijk een variant van het Vlaams.

[2] Zie [K1].

sche meetkunde — maar ik heb wel geprobeerd om redeneervormen te behandelen die wiskundigen iets zeggen. In de laatste paragraaf wordt de beslisbaarheid van Presburger's Rekenkunde bewezen. Opmerkelijk is verder het bewijs van de volledigheid van de eerste orde-logica zonder Henkinconstanten.

De ervaring leert dat er lezers zouden kunnen zijn die hopen in het navolgende een rechtvaardiging van de wiskunde te vinden. Die moet ik teleurstellen. De wiskundige logica is een onderdeel van de wiskunde, en rechtvaardigt het geheel evenmin als de politieke logica de politiek. Ze kan voor de goede verstaander wel *aspecten* van de wiskunde rechtvaardigen, of verhelderen.[3]

Dit boekje is met grote zorg samengesteld, maar volmaaktheid is nauwelijks bereikbaar, en als u, lezer, een verschrijving opmerkt, of erger, dan hoor ik dat graag.

Leiden, september 2014, Piet Rodenburg

Inhoud

[3] Een beschouwing als die in [K2] is mogelijk interessant, maar niet per se verontrustend.

Aanwijzing voor het gebruik

Sommige opgaven en (onderdelen van) voorbeelden zijn gemerkt met een asterisk (*). Ze veronderstellen kennis die uit deze tekst niet verworven kan worden, of zijn anderszins moeilijk. Overigens heeft niet *elke* asterisk deze betekenis; en is van een deel van de opgaven de moeilijkheidsgraad niet uitvoerig vastgesteld. Paragrafen en subparagrafen waarvan de gedetailleerde inhoud, mijns inziens, niet nodig is om het vervolg te begrijpen, zijn gemerkt met een roos: ❀.

Sommige andere opgaven zijn een wezenlijk onderdeel van het betoog, en kunnen niet overgeslagen worden. Welke dat zijn, wordt op den duur vanzelf duidelijk.

Niet alle opgaven zijn gecontroleerd. Daar *moeten* dus haast wel ernstige fouten in voorkomen.

Het betoog is onderverdeeld in paragrafen (§); sommige daarvan zijn op hun beurt verdeeld in subparagrafen. Binnen §n wordt naar subparagraaf $n.m$ verwezen met #m; daarbuiten is het §$n.m$. Item (stelling, definitie, lemma, ...) m van §n wordt aangeduid met 'Item $n.m$', of, binnen §n, met 'Item m'. Item k van subparagraaf m van §n wordt aangeduid met 'Item $n.m.k$', of, binnen §n, met 'Item $.m.k$'.

Notatie en terminologie

Er bestaat enige variantie in de notatie en terminologie van de verzamelingsleer. Hieronder staan een aantal keuzen opgesomd die in deze tekst zijn gemaakt.

Het verschil van twee verzamelingen X en Y, de verzameling

$$\{x \in X \mid x \notin Y\},$$

noteren we als $X \setminus Y$. Twee verzamelingen heten *disjunct* als hun doorsnede leeg is.

We schrijven $X \subseteq Y$ of $Y \supseteq X$ voor 'X is een deelverzameling van Y', en $X \subset Y$ (of $Y \supset X$) als $X \subseteq Y$ en $X \neq Y$.

Een verzameling waarvan de elementen zelf ook verzamelingen zijn, noemen we soms een *collectie*. De machtsverzameling van een verzameling X, de collectie van alle deelverzamelingen van X, noteren we als $\mathcal{P}X$.

Als f een functie is met definitiegebied D, en $X \subseteq D$, dan is $f \upharpoonright X$ de beperking van f tot X, de functie met definitiegebied X die aan $x \in X$ de waarde $f(x)$ toekent.

Een n-plaatsige relatie op een verzameling X is een deelverzameling R van het n-voudig cartesisch product $X \times \ldots \times X$: een verzameling, dus, van rijtjes van n elementen van X. We schrijven dat product meestal als een macht, X^n. In plaats van $\langle x_1, \ldots, x_n \rangle \in R$ noteren we vaak $Rx_1 \ldots x_n$, en als $n = 2$ ook $x_1 R x_2$.

De inverse van een binaire relatie R is de relatie $R^{-1} := \{\langle y, x \rangle | xRy\}$.

Het beeld $\{f(x) | x \in X\}$ van een verzameling X onder een afbeelding f noteren we als $f[X]$.

Wanneer we een functie voorstellen als een relatie, een verzameling paren dus, dan schrijven we in die paren de waarde links, het argument rechts. Zo is functiecompositie een bijzonder geval van de samenstelling van binaire relaties:

$$R \circ S = \{\langle x, y \rangle | \text{er bestaat een } z \text{ zo dat } \langle x, z \rangle \in R \text{ en } \langle z, y \rangle \in S\}.$$

Een functie f is *injectief* als $f(x) = f(y)$ impliceert dat $x = y$. Een functie f van X naar Y (notatie: $f\colon X \longrightarrow Y$) is *surjectief* als $f[X] = Y$. Een functie is *bijectief* als ze zowel injectief als surjectief is.

Deel I. Propositielogica

Als wetenschap is de logica zo'n vierentwintig eeuwen oud, en dus bijna even oud als de meetkunde. Aan de wortel van het vak ligt enerzijds de meetkunde, en anderzijds het debat. Je zou kunnen zeggen dat de studie van de logica begint wanneer mensen zich realiseren dat stappen in een correcte redenering in bepaalde vormen gebracht kunnen worden, en wel zo dat *elke* redenering die bestaat uit stappen van die vorm correct is. Wanneer dat precies gebeurde, dat is voor een deel bekend, en voor een deel moeilijk te reconstrueren. Vermoedelijk werden logische problemen voor het eerst als zodanig besproken in de school van Megara, die rond 400 (v.C.) gesticht werd door Euclides — niet de beroemde meetkundige, maar een leerling van Socrates.

De logica bestudeert de conceptuele mechanismen die leiden tot geldige redeneringen. We kunnen die in meer of minder uitgebreide vorm, en tot op zekere hoogte onafhankelijk van elkaar, bestuderen. Vóór we daaraan beginnen, stellen we twee filosofische vragen die alle logische constructies in gelijke mate aangaan. Namelijk, ten eerste:

Wat is een geldige redenering?

Het antwoord geven we meteen, al legt het misschien niet alles uit en zullen we er later nog op variëren. Denk aan een niet al te simpel bewijs in een serieus wiskundevak. We zien: een geldige redenering is, op een paar details na, een zodanige reeks beweringen dat we van elk lid van de reeks zonder veel moeite begrijpen dat het *volgt uit* eerdere leden. Dat brengt ons bij de tweede vraag:

Wat betekent het dat een bewering A *volgt uit* beweringen $B_1,\ldots,B_n$?

Het antwoord daarop is: het betekent dat onder alle omstandigheden waaronder $B_1,\ldots,B_n$ waar zijn, A ook waar is.

Dit roept natuurlijk weer nieuwe vragen op, zoals: wat zijn *alle omstandigheden*? Welnu, dat hangt ervan af. Er zijn *feitelijke* omstandigheden; in de praktijk zijn die belangrijk, maar in theorie zouden we tenminste een deel onder woorden kunnen brengen en aan $B_1,\ldots,B_n$ toevoegen. Van groot belang is verder de *betekenis* van A, $B_1,\ldots,B_n$. We moeten diep genoeg op de omstandigheden ingaan om die, voorzover van belang, tot haar recht te laten komen.

Terminologie. Een frase van de vorm

$$B_1,\ldots,B_n, \text{ dus } A$$

noemen we een *gevolgtrekking*. Bewering A is de *conclusie*, en $B_1,\ldots,B_n$ zijn de *premissen*. We schrijven ook wel

$$\frac{B_1,\ldots,B_n}{A}$$

of $\{B_1,\ldots,B_n\} \models A$, of $B_1,\ldots,B_n \models A$.

Voegwoorden, of, zoals de logici zeggen, *connectieven*, gelden als het meest geschikte beginpunt voor een inleiding in de logica. Ze werden al vroeg in de geschiedenis bestudeerd: Chrysippus van Soli (Χρύσιππος ὁ Σολεύς, 280-207), geëerd als tweede oprichter van de Stoïsche school, heeft er uitgebreid over geschreven. Al zijn werken zijn verloren gegaan.

Voorbeelden van voegwoorden zijn: *of*, *en*, *maar*, *als … dan*, *want*, *niet*. In combinatie met één of twee beweringen, of, zoals de logici zeggen, *proposities*, leveren ze een nieuwe bewering op, en wat ons in het bijzonder interesseert is hoe de *waarheidswaarde* van de combinatie afhangt van de waarheidswaarden van de samenstellende delen.

§1 Rekenen met waarheidswaarden

1.1 We onderscheiden twee *waarheidswaarden*: 1, de *waarheid*, en haar tegendeel, 0 (de *onwaarheid*). Op de waarheidswaarden kunnen we operaties definieren, analoog aan, bijvoorbeeld, de operaties optelling en vermenigvuldiging op de gehele getallen. Men kan dan rekenen met waarheidswaarden — zoals met gehele getallen, alleen gemakkelijker. Op zichzelf is dat niet zo interessant. We kunnen de parallel echter verder doortrekken. We kunnen *variabelen* invoeren voor waarheidswaarden: letters p, q, r waarvan we in het midden laten voor welke waarheidswaarde ze staan. Zulke variabelen zijn te vergelijken met gewone proposities als 'het regent', die immers ook waar of onwaar zijn. Met deze 'propositieletters' vormen we samengestelde uitdrukkingen; en we zoeken naar betrekkingen tussen zulke uitdrukkingen, analoog aan $x \cdot (y + z) = x \cdot y + x \cdot z$ en $x - x = 0$. Wat we willen doen is een vorm van algebra, met waarheidswaarden in plaats van getallen.

1.2 Voorbeeld. Een reiziger in een vreemd land komt op een tweesprong. Het is laat en hij zoekt een herberg; maar hij weet niet of hij links of rechts moet, en de bewegwijzering laat te wensen over. Gelukkig zitten bij de tweesprong twee broers, wier faam hem tegemoet gesneld is: de ene (A) spreekt namelijk altijd de waarheid, en de andere (B) liegt altijd. Zij zijn inboorlingen en kennen uitstekend de weg. Helaas zijn ze een eeneiïge tweeling, en voor een buitenstaander onmogelijk van elkaar te onderscheiden. Hoe overwint de reiziger deze moeilijkheid?

Om dat uit te vinden analyseren we de situatie als volgt. Er zijn twee antwoorden mogelijk, afgekort l en r. Beide broers hebben het juiste antwoord in hun hoofd. We kunnen ze opvatten als operatoren op waarheidswaarden: A zegt wat hij gelooft, dus

$$\mathrm{A}(0) = 0, \mathrm{A}(1) = 1;$$

en B het tegenovergestelde, dus

$$\mathrm{B}(0) = 1, \mathrm{B}(1) = 0.$$

Stel eens dat l waar is. Als de reiziger aan A vraagt welke kant hij opmoet naar de herberg, dan krijgt hij het antwoord 'links', want $l = 1$, A weet dat, en $\mathrm{A}(1) = 1$. Maar B zou 'rechts' zeggen, en omdat de reiziger A en B niet kan onderscheiden heeft hij niets aan een antwoord op deze vraag. De reiziger moet een vraag stellen waarop A en B hetzelfde antwoord geven. De juiste vraag vinden we door de observatie dat $\mathrm{A}(\mathrm{B}(p)) = \mathrm{B}(\mathrm{A}(p))$ ($p = 1, 0$). Hij luidt: 'Wat zou je broer zeggen als ik hem vroeg welke kant ik op moet naar de herberg?'

1.3 De operator B verandert een waarheidswaarde in haar tegendeel. Die omkering noemen we *negatie*, en we voeren er een symbool, $\neg$, voor in. Als p waar is, dan is $\neg p$ onwaar; en als p onwaar is, dan is $\neg p$ waar. De negatie correspondeert met het Nederlandse woord *niet*. We kunnen haar ook kort definieren met de vergelijkingen

$$\neg 0 = 1, \neg 1 = 0;$$

of overzichtelijk in een *tabel*:

(1.3.1)

p	$\neg p$
1	0
0	1

We zullen nu meteen de overige veel voorkomende operaties invoeren. De negatie werkte op één argument (zo'n operatie noemen we éénplaatsig); deze daarentegen zijn tweeplaatsig, ze werken op twee argumenten, zoals de optelling bij de gehele getallen.

De *conjunctie* correspondeert met het voegwoord *en*; het symbool ervoor is $\wedge$. De werking is weergegeven in de onderstaande tabel.

(1.3.2)

p	q	$p \wedge q$
1	1	1
1	0	0
0	1	0
0	0	0

Dus $1 \wedge 1 = 1$; de overige combinaties van argumenten geven als uitkomst 0. De volgende tabel is een gecomprimeerde versie van (1.3.2):

(1.3.3)

$(p \wedge q)$

$p \backslash q$	1	0
1	1	0
0	0	0

De waarde van $p \wedge q$ staat in (1.3.3) op de kruising van de regel van p en de kolom van q.

De *disjunctie*, symbool $\vee$, correspondeert met het voegwoord *of*, in de zin van en/of. Definitie:

$(p \vee q)$

$p \backslash q$	1	0
1	1	1
0	1	0

Naast deze *inclusieve* disjunctie, *vel* in het Latijn, kennen we ook een *exclusieve* disjunctie, het Latijnse *aut*. Deze symboliseren we met +; de definiërende tabel is

(1.3.5)

$(p + q)$

$p \setminus q$	1	0
1	0	1
0	1	0

De (materiële) *implicatie*, symbool $\rightarrow$, lijkt het meest op *als… dan*. De definitie is vervat in:

(1.3.6)

$(p \rightarrow q)$

$p \setminus q$	1	0
1	1	0
0	1	1

De (materiële) *equivalentie*, symbool $\leftrightarrow$, lijkt op *dan en slechts dan als*. Definitie:

(1.3.7)

$(p \leftrightarrow q)$

$p \setminus q$	1	0
1	1	0
0	0	1

Merk op dat $\rightarrow$ de enige operatie is waarvoor de volgorde van de argumenten verschil maakt.

1.4 Voorbeeld. De buurman belt aan met de mededeling

Je houdt op met hameren of ik word boos en ik bel de politie.

Ik houd op met hameren; moeten we er nu rekening mee houden dat hij de politie *niet* belt? Dat hangt ervan af in welke volgorde we zijn uitspraak evalueren. In ons zojuist ingevoerd symbolisme zei hij:

$$h \vee b \wedge p \ .$$

Dat kunnen we op twee manieren opvatten. (1) $h = 1$; als minstens één argument van een disjunctie waar is, is de disjunctie waar; dus buurman heeft niet gezegd dat hij opbelt. (2) $1 \vee b = 1$; maar $1 \wedge 0 = 0$, dus p moet waar zijn, en buurman belt in elk geval de politie.

Om dit soort dubbelzinnigheden te voorkomen, zetten we haakjes. De eerste lezing was die van $h \vee (b \wedge p)$; de tweede die van $(h \vee b) \wedge p$.

De symbolen 0, 1 en + zijn ook in gebruik voor andere dingen dan waarheidswaarden, en soms is dat verwarrend (bijvoorbeeld in Deel III). In formules gebruiken we daarom meestal alternatieve symbolen: $\perp$, $\top$ (denk aan *truth*) en $\rightarrowtail\!\!\!\leftarrowtail$ (een $\leftrightarrow$ binnenstebuiten). We beschouwen $\perp$ en $\top$ als extra, *nulplaatsige*, connectieven.

Oefeningen bij §1:

1:1 Geef formules die corresponderen (als in Voorbeeld 4) met de volgende Nederlandse zinnen:

(i) Als de zon schijnt, dan regent of sneeuwt het niet.

(ii) Het regent of het regent niet.

(iii) Als $n = 2m$, en n is een kwadraat, dan is m deelbaar door 2, of ik eet mijn hoed op.
(iv)* Je houdt dan en alleen dan op met hameren als ik de politie bel, maar ik ben niet boos.

1:2 Reduceer tot $\perp$ of $\top$:

$(\perp \to \top) \wedge \perp$
$(\perp \vee \perp) \wedge \neg(\top \wedge \perp)$
$(\perp \leftrightarrow \perp) \to \perp$

1:3 Vereenvoudig:

$p \to \top$
$(\perp \to q) \vee p$
$(\perp \wedge q) \to p$
$\top \to (p \vee p)$
$(p \vee \top) \wedge (q \to \perp)$

§2 Het formalisme van de propositielogica

2.1 Om wiskundig te kunnen redeneren over formules hebben we een precieze definitie nodig. We definiëren formules als bepaalde rijtjes van *symbolen*. Er zijn drie groepen van symbolen:

— de propositievariabelen of *propositieletters*; daar hebben we er oneindig veel van, genummerd als $p_0, p_1, p_2, \ldots$
— de logische constanten of *connectieven*: $\top, \perp, \neg, \wedge, \vee, \to, \leftrightarrow, +$ (of $\rightarrowtail\!\!\!\leftarrowtail$)
— haakjes:), (.

Voor het ogenblik zien we geheel af van de betekenis van de symbolen. We komen daar pas op terug in §3. Eigenlijk doet het er zelfs niet toe wat de symbolen *zijn*, als we ze maar uit elkaar kunnen houden. In het bijzonder kunnen we in het midden laten of we de exclusieve disjunctie met + aanduiden of met $\rightarrowtail\!\!\!\leftarrowtail$.

(Een vergaande uitwerking van een dergelijke gedachtengang staat in *Through the Looking-glass* van Lewis Carroll, onder “It’s my own invention”:

‘Or else it doesn’t, you know. The name of the song is called “*Haddocks’ Eyes*.”’

‘Oh, that’s the name of the song, is it?’ Alice said, trying to feel interested.

‘No, you don’t understand,’ the Knight said, looking a little vexed. ‘That’s what the name is *called*. The name really *is* “*The Aged Aged Man*.”’

‘Then I ought to have said “That’s what the *song* is called”?’ Alice corrected herself.

‘No, you oughtn’t: that’s quite another thing! The *song* is called “*Ways and Means*”: but that’s only what it’s *called*, you know!’

‘Well, what *is* the song, then?’ said Alice, who was by this time completely bewildered.

‘I was coming to that,’ the Knight said. ‘The song really *is* “*A-sitting On A Gate*”: and the tune’s my own invention.’

So saying, he stopped his horse and let the reins fall on its neck: then, slowly beating time with one hand, and with a faint smile lighting up his gentle foolish face, as if he enjoyed the music of his song, he began.)

Een rijtje symbolen noemen we ook kortweg een *uitdrukking*. Een *voorkomen* van een symbool s in een uitdrukking α is een plaats in α waar s staat, of eigenlijk de combinatie van s met die plaats: we zeggen bijvoorbeeld dat we *aababa* construeren uit *aabbba* door het tweede voorkomen van b te vervangen door (een voorkomen van) a. Algemener kunnen we spreken van voorkomens van een uitdrukking binnen een uitdrukking. Zo construeren we *aabbaba* uit *aabbba* door het tweede voorkomen van b te vervangen door (een voorkomen van) *ba*, of het derde door *ab*.

2.2 Definitie. De *formules* zijn de elementen van de kleinste verzameling X van uitdrukkingen die
(i) alle propositieletters, en
(ii), (iii) de constanten $\top$ en $\bot$ bevat, en waarvoor geldt
(iv) als $\varphi \in X$, dan ook $\neg\varphi \in X$, en
(v)-(ix) als $\varphi, \psi \in X$, dan behoren ook $(\varphi \wedge \psi)$, $(\varphi \vee \psi)$, $(\varphi \rightarrow \psi)$, $(\varphi \leftrightarrow \psi)$ en $(\varphi + \psi)$ tot X.

Merk op dat we uitdrukkingen bestaande uit één element identificeren met dat element. Dat wordt vaak gedaan, maar het spreekt niet vanzelf, en er zijn situaties denkbaar waarin het tot verwarring zou kunnen leiden.

2.3 Voorbeelden
(a) Uit de definitie volgt dat $(p_1 \rightarrow p_1)$ een formule is. Want, laat FP de verzameling van alle formules zijn als hierboven gedefinieerd. Volgens (i) behoort p_1 tot FP; dus volgt uit (vii) dat $(p_1 \rightarrow p_1) \in$ FP.
(b) Ook $(\top + (\neg p_2 \wedge p_3) \rightarrow p_1))$ is een formule. Want, volgens (i) behoort p_2 tot FP; dus volgt uit (iv) dat $\neg p_2 \in$ FP. Volgens (i), $p_3 \in$ FP; dus volgens (v), $(\neg p_2 \wedge p_3) \in$ FP. Volgens (i), $p_1 \in$ FP; dus volgens (vii),

$$((\neg p_2 \wedge p_3) \rightarrow p_1) \in \text{FP}.$$

En tenslotte, volgens (ii), $\top \in$ FP, dus volgens (ix),

$$(\top + ((\neg p_2 \wedge p_3) \rightarrow p_1)) \in \text{FP}.$$

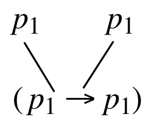
Hoe kun je nu zien dat iets *niet* een formule is? Eén criterium is gemakkelijk toe te passen: formules zijn uitdrukkingen, dus als iets geen rijtje symbolen is, is het geen formule. Maar hoe te bepalen dat een uitdrukking geen formule is?

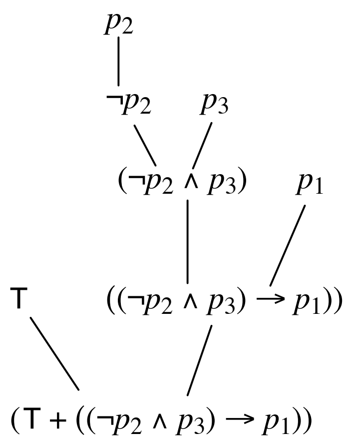
FP is gedefinieerd als de kleinste verzameling die de verzameling PROP der propositieletters omvat, $\top$ en $\bot$ bevat, en bepaalde *afsluitingseigenschappen* heeft. Op de verzameling W van alle niet-lege uitdrukkingen definiëren we de volgende operaties:
negatie; de negatie $F_\neg(\alpha)$ van een rijtje α is het rijtje $\neg\alpha$, bestaande uit het negatiesymbool gevolgd door de elementen van α, in volgorde.
conjunctie; de conjunctie $F_\wedge(\alpha, \beta)$ van twee rijtjes α en β is het rijtje $(\alpha \wedge \beta)$, bestaande uit het linkerhaakje gevolgd door de elementen van α, in volgorde, gevolgd door het conjunctiesymbool, gevolgd door de elementen van β, in volgorde, gevolgd door het rechterhaakje. (Er zitten ook spaties in, maar die zijn een toegift terwille van de leesbaarheid.)
inclusieve disjunctie; de (inclusieve) disjunctie $F_\vee(\alpha, \beta)$ is $(\alpha \vee \beta)$.
implicatie, $F_\rightarrow(\alpha, \beta) = (\alpha \rightarrow \beta)$.

bi-implicatie of *equivalentie*, $F_{\leftrightarrow}(\alpha, \beta) = (\alpha \leftrightarrow \beta)$.
exclusieve disjunctie, $F_{+}(\alpha, \beta) = (\alpha + \beta)$.
Een deelverzameling X van W is *gesloten onder negatie* als $F_{\neg}[X] \subseteq X$, dat wil zeggen, als voor alle $\alpha \in X$ ook $\neg\alpha \in X$; *gesloten onder conjunctie* als $F_{\wedge}[X \times X] \subseteq X$, i.e, voor alle $\alpha, \beta \in X$ ook $(\alpha \wedge \beta) \in X$; enzovoort. En FP is de kleinste PROP $\cup$ $\{\top, \bot\}$ omvattende verzameling die gesloten is onder $F_{\neg}$, $F_{\wedge}$, $F_{\vee}$, $F_{\rightarrow}$, $F_{\leftrightarrow}$ en F_{+}. Dus om te bewijzen dat een rijtje $\alpha \in W$ niet tot FP behoort, moeten we een verzameling $X \supseteq$ PROP $\cup$ $\{\top, \bot\}$ construeren die gesloten is onder $F_{\neg}$, $F_{\wedge}$, $F_{\vee}$, $F_{\rightarrow}$, $F_{\leftrightarrow}$ en F_{+}, en die α niet bevat. Omdat FP $\subseteq X$, volgt $\alpha \notin$ FP.
(c) $p_1 \wedge p_2$ is geen formule. Want, neem $X = W - \{p_1 \wedge p_2\}$. Dan bevat X de propositieletters en de constanten $\top$ en $\bot$; X is gesloten onder $F_{\neg}$, want alle rijtjes die beginnen met $\neg$ zitten in X; en X is gesloten onder de tweeplaatsige operaties, want alle rijtjes die beginnen met een haakje zitten erin. Maar $p_1 \wedge p_2 \notin X$; dus $p_1 \wedge p_2 \notin$ FP.
(d) (p_1) is geen formule. Want, neem $X = W \setminus \{(p_1)\}$. Dan bevat X de propositieletters en de constanten $\top$ en $\bot$; en X is gesloten onder de operaties, want alle rijtjes waar een connectief in voorkomt, zitten erin. Maar $(p_1) \notin X$; dus $(p_1) \notin$ FP.
(e) $((p_1 \leftrightarrow p_2) \rightarrow \bot))$ is geen formule: zie Lemma 6.

2.4 Constructiebomen

De redeneringen in 3(a) en (b), leidend tot de conclusie dat $(p_1 \rightarrow p_1)$ en $(\top + ((\neg p_2 \wedge p_3) \rightarrow p_1))$ formules zijn, kunnen we weergeven in boomvorm:





De bladeren van de boom worden bezet door propositieletters en logische constanten $\top$ en $\bot$. Op een knoop met één dochter staat de negatie van de dochterformule. Op een knoop met twee dochters staat een formule die geconstrueerd is uit de dochterformules met behulp van een tweeplaatsig connectief.

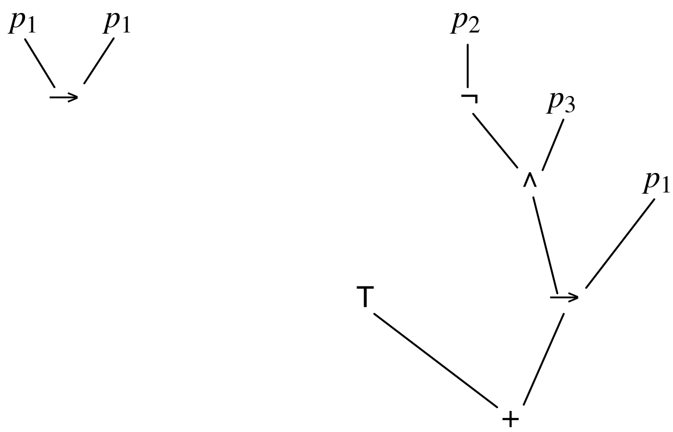
2:1 Oefening. Teken constructiebomen voor
(a) $(((p_1 \rightarrow p_2) \rightarrow p_1) \rightarrow p_1)$;
(b) $((p_1 \rightarrow p_2) \rightarrow (\neg p_2 \rightarrow (p_1 \rightarrow \bot)))$;
(c) $(\neg\neg\neg p_1 \rightarrow \neg p_1)$.

Definitie. De *subformules* van een formule φ zijn de formules die voorkomen in de constructieboom van φ.

De hoogte van de constructieboom is een maat voor de complexiteit van de geconstrueerde formule. Die hoogte is een natuurlijk getal — 1 voor

$(p_1 \to p_1)$, 4 voor $(\top + ((\neg p_2 \wedge p_3) \to p_1))$ — en daar kunnen we inductie over doen. We spreken dan van *inductie naar de complexiteit* van formules.

Terzijde. De constructieboom ligt vast zodra we weten waar we mee beginnen en wat we daarmee doen. We kunnen de bovenstaande bomen dus vereenvoudigen tot



Merk op dat we de vereenvoudigde bomen kunnen gebruiken als representanten van de formules. Haakjes zijn bij deze notatie niet nodig.

❀ 2.5 Unieke leesbaarheid

Nu we een precieze definitie van formules hebben, willen we terugkeren naar de vraag waar we mee begonnen, te weten, hoe de waarheidswaarde van een complexe formule afhangt van de waarheidswaarden van haar samenstellende delen. Er is echter een prealabele kwestie.

Voorbeeld 1.4 leidde tot de invoering van haakjes; zonder haakjes is de waarheidswaarde niet onder alle omstandigheden eenduidig bepaald. Het probleem is, dat $h \vee b \wedge p$ zowel de *disjunctie* van h en $b \wedge p$ kan zijn, als de *conjunctie* van $h \vee b$ en p. Met haakjes forceren we een keuze; we leggen de constructieboom vast. De kwestie is nu, of die oplossing altijd werkt: heeft *elke* formule maar één constructieboom? Het antwoord vult de rest van deze §.

2.6 Lemma. Elke formule bevat evenveel linker- als rechterhaakjes.

Bewijs. Laat X de verzameling zijn van alle uitdukkingen waar evenveel linker- als rechterhaakjes in voorkomen. Als een rijtje α bestaat uit één propositieletter, of uitsluitend het symbool $\top$ of $\bot$, dan $\alpha \in X$. Het is niet moeilijk na te rekenen dat X gesloten is onder de operaties $F_\neg$, $F_\wedge$, $F_\vee$, $F_\to$, $F_\leftrightarrow$ en F_+. Dus X bevat alle formules. ⊠

Een beginstuk van een rijtje dat niet het hele rijtje is, heet een *echt* beginstuk. Dus, bijvoorbeeld, het lege rijtje en a zijn echte beginstukken van ab.

2.7 Lemma. Als φ een formule is, dan bevat elk niet-leeg echt beginstuk van φ dat niet uitsluitend uit negatietekens bestaat meer linker- dan rechterhaakjes.

Bewijs. Laat X de verzameling zijn van alle formules waarvan elk niet-leeg echt beginstuk dat niet uitsluitend uit negatietekens bestaat meer linker- dan rechterhaakjes bevat.

Propositieletters hebben geen niet-lege echte beginstukken, en behoren daarom tot X. Hetzefde geldt voor $\top$ en $\bot$.

Als $\alpha \in X$, dan ook $\neg\alpha \in X$. Immers, een niet-leeg echt beginstuk van $\neg\alpha$ heeft de vorm $\neg\beta$, waarin β een echt beginstuk is van α. Dus als β niet geheel uit negatietekens bestaat, bevat β meer linker- dan rechterhaakjes; en hetzelfde geldt dan voor $\neg\beta$.

Als α en β tot X behoren, dan ook $(\alpha \wedge \beta) \in X$. Een niet-leeg echt beginstuk van $(\alpha \wedge \beta)$ heeft namelijk de vorm

$$(\gamma$$

— waarin γ een beginstuk is van α — of

$$(\alpha \wedge \delta$$

— met δ een beginstuk van β. In het eerste geval kan γ niet meer rechterhaakjes bevatten dan linker, dus $(\gamma$ bevat meer linker- dan rechterhaakjes. In het tweede geval bevatten zowel α als δ niet meer rechterhaakjes dan linker; en bevat $(\alpha \wedge \delta$ dus meer linker- dan rechterhaakjes.

Dezelfde redenering gaat op voor de andere tweeplaatsige connectieven. Dus X bevat alle formules. ⊠

2.8 Lemma. Een echt beginstuk van een formule is geen formule.

Bewijs. Volgens Lemma 7 is een echt beginstuk van een formule leeg, en dan is het geen formule; of het bestaat geheel uit negatietekens, en dan is het ook geen formule; of het bevat meer linker- dan rechterhaakjes, en dan is het volgens Lemma 6 geen formule. ⊠

2.9 Stelling (*unieke leesbaarheid*). Een formule heeft slechts één constructieboom.

Bewijs. Laat φ een formule zijn. We doen inductie naar de lengte van φ.

Als φ een propositieletter is, of $\perp$ of $\top$, dan is er geen twijfel mogelijk. Als φ begint met een negatieteken, zeg $\varphi = \neg\psi$, dan is een constructieboom voor φ noodzakelijkerwijs van de vorm

$$\begin{array}{c} B \\ | \\ \varphi \end{array}$$

met B een constructieboom voor ψ; B is uniek volgens inductieveronderstelling.

Als φ begint met een haakje, dan is φ van de vorm $(\psi \circ \chi)$, voor een of ander tweeplaatsig connectief $\circ$, en

$$\begin{tikzcd}[column sep=small] B_\psi \arrow[dr, dash] & & B_\chi \arrow[dl, dash] \\ & \varphi & \end{tikzcd}$$

met B_ψ en B_χ constructiebomen voor respectievelijk ψ en χ, een constructieboom voor φ. Volgens inductieveronderstelling zijn B_ψ en B_χ qua constructiebomen voor (respectievelijk) ψ en χ uniek. Een andere constructieboom vereist dus dat φ ook gezien kan worden als $(\psi' * \chi')$, met andere formules ψ' en χ', en een tweeplaatsig connectief $*$. Maar dat is onmogelijk; want dan moet ψ' een echt beginstuk zijn van ψ, of ψ een echt beginstuk van ψ'; en volgens Lemma 8 is één van beide dan geen formule. ☒

Verdere Oefeningen bij §2:

2:2 (substitutie) Laat α en β uitdukkingen zijn, en p een propositieletter. Dan is $[\alpha/p]\beta$ het resultaat van *substitutie van* α *voor* p *in* β, d.i., vervanging van *alle* voorkomens van p in β door voorkomens van α.[4] Dus, bijvoorbeeld,

$$[\,p_2)\wedge/p_0](\bot p_1\rightarrow p_0p_0))\vee\vee p_{23} = (\bot p_1\rightarrow p_2)\wedge p_2)\wedge))\vee\vee p_{23}$$

$$[(p_2 \wedge p_0)/p_2](\top \rightarrow (p_2 \vee p_1)) = (\top \rightarrow ((p_2 \wedge p_0) \vee p_1))$$

Bewijs: als φ en ψ formules zijn, dan is $[\varphi/p]\psi$ een formule. (Fixeer de formule φ en de propositieletter p. Laat zien dat

$$\{\psi \in \mathrm{F{\scriptstyle P}} \mid [\varphi/p]\psi \text{ is een formule}\} \supseteq \mathrm{F{\scriptstyle P}}.)$$

2:3 In de *Poolse notatie* representeert men formules ééndimensionaal (in tegenstelling tot de *tweedimensionale* boomnotatie gesuggereerd in §2.4), en toch zonder haakjes. Dat gaat als volgt: definieer de formules als de elementen van de kleinste verzameling X van uitdukkingen die
(i) alle propositieletters, en
(ii), (iii) de constanten $\top$ en $\bot$ bevat, en waarvoor geldt
(iv) als $\varphi \in X$, dan ook $\neg\varphi \in X$, en
(v)-(ix) als $\varphi, \psi \in X$, dan behoren ook $\wedge\varphi\psi$, $\vee\varphi\psi$, $\rightarrow\varphi\psi$, $\leftrightarrow\varphi\psi$ en $+\varphi\psi$ tot X.
a) Schrijf de formules op in Poolse notatie die corresponderen met

$$((p_1 \rightarrow p_2) \rightarrow (\neg p_2 \rightarrow (p_1 \rightarrow \bot)))$$

$$(((p_1 \wedge \top) \vee (p_1 \wedge p_1)) \leftrightarrow \neg p_4)$$

(Als je formules in bomen kunt omzetten, dan kun je als volgt verdergaan: laat een slak met de kop naar rechts over de boom wandelen, beginnend bij de wortel, dan omhoog langs de meest linkse tak, terug via de zijtakken, dan de rechtertak op dezelfde manier, steeds knopen leegetend zodra ze voor zijn mond komen. Als de wandeling gedaan is, zit de Poolse formule in het spijsverteringskanaal van de slak. De grootste boom van p.8 wordt op die manier omgezet in $+\top\rightarrow\wedge\neg p_2p_3p_1$.)
b) Onderzoek of de volgende uitdukkingen formules zijn in de Poolse notatie: $\neg\rightarrow p_1\neg p_2$; $\rightarrow\wedge\leftrightarrow p_1p_2\neg p_3p_1$; $\neg\rightarrow\top p_2\wedge\neg p_3$.

Definieer de gewichtsfunctie σ op uitdrukkingen als volgt:
(i) $\sigma(p) = -1$, voor propositieletters p; $\sigma(\top) = \sigma(\bot) = -1$;
(ii) zij ε het lege rijtje: $\sigma(\varepsilon) = \sigma(\neg) = 0$;
(iii) $\sigma(\wedge) = \sigma(\vee) = \sigma(\rightarrow) = \sigma(\leftrightarrow) = \sigma(+) = 1$;
(iv) als s een symbool is en α een uitdrukking, dan $\sigma(\alpha s) = \sigma(\alpha) + \sigma(s)$.
c) Bewijs dat voor alle uitdrukkingen α en β, $\sigma(\alpha\beta) = \sigma(\alpha) + \sigma(\beta)$.
d) Bewijs dat een uitdrukking α een formule is in Poolse notatie dan en slechts dan als (1°) voor elk echt beginstuk β van α, $\sigma(\beta) \geq 0$, en (2°) $\sigma(\alpha) = -1$.
[$\Rightarrow$: inductie over formules; $\Leftarrow$: inductie naar de lengte van de uitdrukking.]
e) Laat zien hoe uit (d) volgt dat formules in Poolse notatie uniek leesbaar zijn.

---

[4] Let op de omkering: α *substitueren voor* p is p *vervangen door* α.

§3 Semantiek van de propositielogica

We hebben ons in §1 al bezig gehouden met de betekenis van connectieven en het gebruik van propositieletters voor beweringen. Met de grammaticale algemeenheden van §2 in de rug gaan we dezelfde kwesties nu formeler, abstracter en algemener beschouwen.

3.1 Conventies. Eerst brengen we een aantal vereenvoudigingen aan in de notatie.

Het is vaak niet nodig om precies te weten welke propositieletters in een formule voorkomen. We gebruiken dan letters zonder subscripten, zoals in §1. — Ook in §2 gebruikten we trouwens "p" en "q" om willekeurige propositieletters aan te duiden.

Haakjes garanderen de leesbaarheid in theorie; de praktijk is anders. We laten ze soms (maar niet altijd) weg, in overeenstemming met de volgende afspraken:

(a) Buitenste haakjes kunnen we er altijd bijdenken, en hoeven we dus niet op te schrijven.

(b) Stel dat een formule φ is geconstrueerd door een aantal malen dezelfde clausule van Definitie 2.2 toe te passen, voor een of ander tweeplaatsig connectief $\circ$. Het resultaat, op de haakjes na, is dan van de vorm $\varphi_1 \circ \ldots \circ \varphi_n$. Daar kunnen op verschillende manieren haakjes in; de volgende komt veel voor:

$$\varphi_1 \circ (\varphi_2 \circ (\ldots\ldots \circ (\varphi_{n-1} \circ \varphi_n)\ldots)) \qquad (*)$$

(*associatie naar rechts*). We spreken af dat we met $\varphi_1 \circ \ldots \circ \varphi_n$ altijd (*) bedoelen. Dus

$$p \to q \to r \to s \quad \text{is} \quad p \to (q \to (r \to s)),$$
$$p \wedge q \wedge (r \vee \neg s) \quad \text{is} \quad p \wedge (q \wedge (r \vee \neg s)).$$

(c) In de rekenkunde bindt $\cdot$ sterker dan $+$. Zoiets kunnen wij ook:

$$\wedge \text{ en } \vee \text{ binden sterker dan } \to \text{ en } \leftrightarrow.$$

(We hadden al: $\neg$ bindt het sterkst van allemaal.) Dus

$$p \to q \vee p \quad \text{is} \quad p \to (q \vee p),$$
$$p \wedge q \leftrightarrow \neg q \quad \text{is} \quad (p \wedge q) \leftrightarrow \neg q.$$

3:1 Oefening. Vul de haakjes aan in

$(p \to q \to r) \to (p \to q) \to p \to r$

$\bot \vee r \vee s \leftrightarrow (\bot \to r) \wedge (\bot \to s)$

$p \wedge q \leftrightarrow \neg\neg p \wedge \neg\neg q \leftrightarrow \neg(\neg p \vee \neg q)$

3.2 Definitie. Een *valuatie* is een toekenning van waarheidswaarden aan propositieletters.

Als we van de propositieletters de waarheidswaarde kennen, dan kunnen we de waarheidswaarde van samengestelde formules berekenen. De connectieven staan immers voor operaties op waarheidswaarden, zoals uitgelegd in §1. De uitkomst van de berekening is 1 of 0.

❀ **3.3** Voor de zekerheid zullen we nagaan dat het echt *nooit* zo is dat beide uitkomsten op kunnen treden: gegeven een valuatie aan de propositieletters in φ, krijgt φ òf de waarde 1, òf de waarde 0.

Stelling. Laat V een valuatie zijn. Dan is er precies één uitbreiding V^* van V die aan alle formules een waarheidswaarde toekent en die voldoet aan
(i) $V^*(\top) = 1$, $V^*(\bot) = 0$;
(ii) voor elke formule φ, $V^*(\neg\varphi) = \neg V^*(\varphi)$;
(iii) voor alle formules φ en ψ, en ieder tweeplaatsig connectief $\circ$, $V^*(\varphi \circ \psi) = V^*(\varphi) \circ V^*(\psi)$.

Bewijs. Laat FP_n de verzameling zijn van alle formules van lengte hoogstens n. We zullen laten zien dat er voor elke $n \geq 1$ precies één functie

$$V_n\colon \mathrm{FP}_n \longrightarrow \{0, 1\}$$

bestaat die voldoet aan:
(1) $V_n \supseteq V$, $V_n(\top) = 1$, $V_n(\bot) = 0$;
(2) voor alle $\varphi \in \mathrm{FP}_n$: als $\varphi = \neg\psi$, dan $V_n(\varphi) = \neg V_n(\psi)$; als $\varphi = (\psi \circ \chi)$, voor een tweeplaatsig connectief $\circ$, dan $V_n(\varphi) = V_n(\psi) \circ V_n(\chi)$.

De formules van lengte 1 zijn $\top$, $\bot$, en de propositieletters. De enig mogelijke definitie van V_1 is: $V_1(\top) = 1$, $V_1(\bot) = 0$, en $V_1(p_i) = V(p_i)$, voor alle i.

Laat V_n gegeven zijn, $n \geq 1$; dan definiëren we V_{n+1} als volgt. Laat φ een formule zijn van lengte $k \leq n + 1$. Als $k \leq n$, dan nemen we $V_{n+1}(\varphi) = V_n(\varphi)$. Als $k = n + 1$, dan begint φ met een negatieteken of een linkerhaakje. In het eerste geval is er een formule $\psi \in \mathrm{FP}_n$ zo dat $\varphi = \neg\psi$. Dan definiëren we: $V_{n+1}(\varphi) = \neg V_n(\psi)$. In het tweede geval zijn er formules ψ en χ, en een tweeplaatsig connectief $\circ$, zo dat $\varphi = (\psi \circ \chi)$. De lengten van ψ en χ zijn kleiner dan n, dus $V_n(\psi)$ en $V_n(\chi)$ zijn gedefinieerd. We definiëren nu:

$$V_{n+1}(\varphi) = V_n(\psi) \circ V_n(\chi).$$

De aldus gedefinieerde toekenning van waarheidswaarden aan formules van lengte $\leq n + 1$ is de enige die voldoet aan (1) en (2) (met $n + 1$ gesubstitueerd voor n). Neem maar aan dat $W\colon \mathrm{FP}_{n+1} \longrightarrow \{0, 1\}$ voldoet aan
(1′) $W \supseteq V$, $W(\top) = 1$, $W(\bot) = 0$;
(2′) als φ een formule is van lengte hoogstens $n + 1$, dan, als $\varphi = \neg\psi$, $W(\varphi) = \neg W(\psi)$; als voor zeker tweeplaatsig connectief $\circ$, $\varphi = (\psi \circ \chi)$, dan $W(\varphi) = W(\psi) \circ W(\chi)$.
Omdat volgens inductieveronderstelling V_n uniek is, geldt zeker:

$$W \upharpoonright \mathrm{FP}_n = V_n.$$

Dus als $\varphi \in \mathrm{FP}_n$, dan $W(\varphi) = V_{n+1}(\varphi)$. Stel nu dat $\varphi \in \mathrm{FP}_{n+1} - \mathrm{FP}_n$. Als φ begint met een negatieteken, dan is er volgens de Unieke Leesbaarheidsstelling maar één formule ψ zo dat $\varphi = \neg\psi$; dus $W(\varphi) = \neg W(\psi) = \neg V_{n+1}(\psi) = V_{n+1}(\varphi)$. Als φ begint met een linkerhaakje, dan is er, weer volgens de Unieke Leesbaarheidsstelling, maar één constructie van φ uit formules ψ en χ en een tweeplaatsig connectief $\circ$; dan

$$W(\varphi) = W(\psi) \circ W(\chi) = V_{n+1}(\psi) \circ V_{n+1}(\chi) = V_{n+1}(\varphi).$$

Tenslotte verenigen we de functies V_n:

$$V^* = \bigcup_{n=1}^{\infty} V_n.$$

Het is gemakkelijk in te zien dat V^* een functie is, dat V^* een uitbreiding is van V, en dat (i)-(iii) gelden. Om in te zien dat V^* uniek is, beschouwen we een willekeurige uitbreiding U van V met domein FP die voldoet aan (i)-(iii). Laat φ een formule zijn; zij k de lengte van φ. De functie U voldoet aan (1) en (2), voor alle n; wegens de uniciteit van V_k geldt dan in het bijzonder

$$U \restriction \mathrm{FP}_k = V_k .$$

Dus $U(\varphi) = (U \restriction \mathrm{FP}_k)(\varphi) = V_k(\varphi) = V^*(\varphi)$. Omdat φ willekeurig was, volgt: $U = V^*$. ☒

Verwarring tussen een valuatie V en de uitbreiding V^* is nauwelijks mogelijk; daarom schrijven we in het vervolg bijna altijd V in plaats van V^*.

3.4* Uitweiding. In het Lemma beschouwen we enerzijds een verzameling uitdrukkingen, de formules, met bijzondere elementen, ‘constanten’, ⊤ en ⊥, en operaties $F_\neg$, $F_\wedge$, $F_\to$,…, en anderzijds de verzameling {0, 1} met verwante constanten en operaties 1, 0, ∧, →,…; en we laten zien dat elke functie van PROP naar {0, 1} een unieke voortzetting f op FP heeft die *de operaties respecteert*, dat wil zeggen, zo dat $f(\top) = 1, f(\bot) = 0, f(F_\neg(\alpha)) = \neg f(\alpha), f(F_\wedge(\alpha, \beta)) = f(\alpha) \wedge f(\beta)$, enzovoort. Een dergelijke situatie doet zich vaak voor in de algebra. Bijvoorbeeld, iedere keuze van een element x van een groep G bepaalt een uniek homomorfisme f van de abelse groep **Z** naar G dat 1 op x afbeeldt; iedere toekenning van ringelementen aan variabelen bepaalt een uniek homomorfisme van de polynoomring $R[x_1 \ldots x_n]$ op R.

3.5 Waarheidstafels

Er zijn oneindig veel valuaties; maar dikwijls zijn bijna alle verschillen tussen valuaties irrelevant.

3.5.1 Eindigheidslemma. Laat φ een formule zijn, en V_1 en V_2 valuaties die aan alle propositieletters die in φ voorkomen dezelfde waarde toekennen. Dan $V_1(\varphi) = V_2(\varphi)$.

Bewijs. Met inductie naar de lengte van φ.

Als φ lengte 1 heeft, dan is φ een propositieletter, en dan is $V_1(\varphi) = V_2(\varphi)$ gegeven; of φ is een logische constante, ⊤ of ⊥, waaraan alle valuaties dezelfde waarde toekennen.

Als de lengte van φ groter is dan 1, dan is φ geconstrueerd uit kortere formules: het is een negatie, zeg $\varphi = \neg\psi$, of er zijn formules ψ_1 en ψ_2 en een tweeplaatsig connectief ∘ zo dat $\varphi = \psi_1 \circ \psi_2$. In het eerste geval

$$V_1(\varphi) = \neg V_1(\psi) = \neg V_2(\psi) = V_2(\varphi),$$

want $V_1(\psi) = V_2(\psi)$ volgens inductieveronderstelling. In het tweede geval

$$V_1(\varphi) = V_1(\psi_1) \circ V_1(\psi_2) = V_2(\psi_1) \circ V_2(\psi_2) = V_2(\varphi)$$

omdat $V_1(\psi_1) = V_2(\psi_1)$ en $V_1(\psi_2) = V_2(\psi_2)$ volgens inductieveronderstelling. ☒

Voor de evaluatie van een formule φ zijn verschillen tussen valuaties dus alleen van belang als ze de waardering betreffen van propositieletters die in φ voorkomen. Dus als φ n propositieletters bevat, zijn er wat φ betreft slechts 2^n

verschillende valuaties. Die kun je uitschrijven in een tabel, een *waarheidstafel*.

3.5.2 Voorbeeld. $\varphi = (p_0 \to p_1) \vee (\neg p_0 \to p_2) \to p_2$

p_0	p_1	p_2	$p_0 \to p_1$	$\neg p_0$	$\neg p_0 \to p_2$	$(p_0 \to p_1) \vee (\neg p_0 \to p_2)$	φ
1	1	1	1	0	1	1	1
1	1	0	1	0	1	1	0
1	0	1	0	0	1	1	1
1	0	0	0	0	1	1	0
0	1	1	1	1	1	1	1
0	1	0	1	1	0	1	0
0	0	1	1	1	1	1	1
0	0	0	1	1	0	1	0

3.6 Formules zoals φ in het bovenstaande voorbeeld, die afhankelijk van de valuatie zowel waar als onwaar kunnen zijn, heten *contingent*. Een formule die onder elke valuatie onwaar is, heet een *contradictie* of *tegenspraak*. De bekendste is $p \wedge \neg p$:

p	$\neg p$	$p \wedge \neg p$
1	0	0
0	1	0

Een formule die onder elke valuatie waar is, heet een *tautologie*. Voorbeelden zijn $p \vee \neg p$ (de *Wet van de Uitgesloten Derde*) en $\neg(p \wedge \neg p)$ (de *Wet van de Noncontradictie*). Een korte notatie voor "φ is een tautologie" is $\models \varphi$. De uitspraak "φ is *geen* tautologie" wordt $\not\models \varphi$.

3:2 Oefening. (a) Ga na dat $p \vee \neg p$ en $\neg(p \wedge \neg p)$ inderdaad tautologieën zijn.
(b) Volgt uit de tabel in 3.6 dat elke formule van de vorm $\varphi \wedge \neg\varphi$ een contradictie is?
(c) En uit de tabel in 3.5.2, dat elke formule van de vorm

$$(\varphi \to \psi) \vee (\neg\varphi \to \chi) \to \chi$$

contingent is?

3:3 Oefening. (a) Ga voor elk van de onderstaande formules na of ze tautologisch, contingent of contradictoir is:

(i) $p \to q \to p$ (iv) $\neg((p \to q) \to \neg q \to \neg p)$
(ii) $(p \to q) \to p$ (v) $\neg(p \vee q) \to (p \to q)$
(iii) $\neg(p \wedge q) \to \neg q$

(b) Zij V een valuatie, q een propositieletter, en φ een formule. Definieer de valuatie W door

$$W(p) = \begin{cases} V(p) \text{ als } p \neq q, \\ V(\varphi) \text{ als } p = q. \end{cases}$$

Bewijs dat voor elke formule ψ, $V([\varphi/q]\psi) = W(\psi)$.

3.7 Als $\models \varphi \leftrightarrow \psi$ dan heten φ en ψ (*logisch*) *equivalent*. We noteren dit als $\varphi \mathrel{\models\!\!\!\dashv} \psi$. Gezien de waarheidstafel voor $\leftrightarrow$ (1.3.7) bestaat deze relatie tussen φ en ψ precies dan als $V(\varphi) = V(\psi)$ voor elke valuatie V; dat is, volgens 3.5, als φ en ψ op elke regel van hun waarheidstafel dezelfde waarde hebben. Zo toont de tabel in 3.5.2 aan dat $(p_0 \to p_1) \vee (\neg p_0 \to p_2) \to p_2$ equivalent is met p_2.

3.7.1 *Dubbele Negatie-Wet*. Voor elke formule φ is $\neg\neg\varphi$ equivalent met φ. Men kan dat bewijzen met een waarheidstafel. Bij een gegeven valuatie V zijn er voor φ hoogstens twee mogelijkheden: φ is waar, of φ is onwaar. Die zetten we uit in de tabel:

φ	$\neg\varphi$	$\neg\neg\varphi$
1	0	1
0	1	0

We zien dat op beide soorten regels, die waar φ waar wordt en die waar φ onwaar wordt, φ en $\neg\neg\varphi$ dezelfde waarde hebben.

3.7.2 *Commutatieve en Associatieve Wetten*. Het is gemakkelijk in te zien dat

$$(\varphi \wedge \psi) \mathrel{\models\!\!\!\dashv} (\psi \wedge \varphi), \qquad (\varphi \vee \psi) \mathrel{\models\!\!\!\dashv} (\psi \vee \varphi)$$

(Commutatieve Wetten) en

$$((\varphi \wedge \psi) \wedge \chi) \mathrel{\models\!\!\!\dashv} (\varphi \wedge (\psi \wedge \chi)), \quad ((\varphi \vee \psi) \vee \chi) \mathrel{\models\!\!\!\dashv} (\varphi \vee (\psi \vee \chi))$$

(Associatieve Wetten).

3.7.3 *Distributieve Wetten*. Beschouw de onderstaande tabel:

φ	ψ	χ	$\psi \vee \chi$	$\varphi \wedge (\psi \vee \chi)$	$\varphi \wedge \psi$	$\varphi \wedge \chi$	$(\varphi \wedge \psi) \vee (\varphi \wedge \chi)$
1	1	1	1	1	1	1	1
1	1	0	1	1	1	0	1
1	0	1	1	1	0	1	1
1	0	0	0	0	0	0	0
0	1	1	1	0	0	0	0
0	1	0	1	0	0	0	0
0	0	1	1	0	0	0	0
0	0	0	0	0	0	0	0

Bij elke mogelijke combinatie van waarheidswaarden van φ, ψ en χ blijkt voor $\varphi \wedge (\psi \vee \chi)$ en $(\varphi \wedge \psi) \vee (\varphi \wedge \chi)$ dezelfde waarheidswaarde te resulteren. Dus

$$(\varphi \wedge (\psi \vee \chi)) \mathrel{\models\!\!\!\dashv} ((\varphi \wedge \psi) \vee (\varphi \wedge \chi)),$$

conjunctie distribueert over disjunctie. Een sterk verwante tabel bewijst

$$(\varphi \vee (\psi \wedge \chi)) \mathrel{\models\!\!\!\dashv} ((\varphi \vee \psi) \wedge (\varphi \vee \chi)),$$

disjunctie distribueert over conjunctie.

3.7.4 *Wetten van De Morgan*. Beschouw de onderstaande tabel:

φ	ψ	$\neg\varphi$	$\neg\psi$	$\varphi \wedge \psi$	$\neg(\varphi \wedge \psi)$	$\neg\varphi \vee \neg\psi$	$\varphi \vee \psi$	$\neg(\varphi \vee \psi)$	$\neg\varphi \wedge \neg\psi$
1	1	0	0	1	0	0	1	0	0
1	0	0	1	0	1	1	1	0	0
0	1	1	0	0	1	1	1	0	0
0	0	1	1	0	1	1	0	1	1

Er blijkt uit dat $\neg(\varphi \wedge \psi)$ logisch equivalent is met $\neg\varphi \vee \neg\psi$, en $\neg(\varphi \vee \psi)$ met $\neg\varphi \wedge \neg\psi$.

3.7.5 *Implicatie en Equivalentie*. Op dezelfde manier kun je bewijzen dat $\varphi \rightarrow \psi$ logisch equivalent is met $\neg\varphi \vee \psi$ en met $\neg(\varphi \wedge \neg\psi)$, en $\varphi \leftrightarrow \psi$ met $(\varphi \rightarrow \psi) \wedge (\psi \rightarrow \varphi)$.

3:4 Oefening. (a) Controleer de beweringen in 3.7.5.
(b) Als φ logisch equivalent is met ψ, en ψ is logisch equivalent met χ, moet het dan zo zijn dat φ logisch equivalent is met χ? En als

$$\models \varphi \leftrightarrow \psi \leftrightarrow \chi,$$

geldt dan $\models \varphi \leftrightarrow \chi$?
(c) Laat V een valuatie zijn, en φ een formule waarin, naast propositieletters en eventuele haakjes, hoogstens één, binair, connectief voorkomt. Bewijs:
1° Als het connectief $\wedge$ is, dan $V(\varphi) = 1$ dan en slechts dan als $V(p) = 1$ voor elke propositieletter p die in φ voorkomt.
2° Als het connectief $\vee$ is, dan $V(\varphi) = 1$ dan en slechts dan als $V(p) = 1$ voor minstens één propositieletter p die in φ voorkomt.
3° Als het connectief $\leftrightarrow$ is, dan $V(\varphi) = 1$ dan en slechts dan als het aantal voorkomens in φ van propositieletters q waarvoor $V(q) = 0$ even is.
(d) Een binair connectief $\circ$ heet *associatief* als $(p_0 \circ p_1) \circ p_2$ logisch equivalent is met $p_0 \circ (p_1 \circ p_2)$. Is $\rightarrow$ associatief?
(e) Bewijs dat elke formule waarin geen andere connectieven voorkomen dan $\wedge$ en $\vee$ contingent is.
(f) Vind zo veel mogelijk logisch niet-equivalente formules die zijn geconstrueerd met uitsluitend haakjes, $\rightarrow$, en de propositieletters p_0 en p_1.

3.8 Notatie. De eigenschappen van $\wedge$ en $\vee$ die worden beschreven in (c) van bovenstaande oefening motiveren bijzondere notaties voor herhaalde conjunctie en disjunctie:

$$\bigwedge_{i \leq n} \varphi_i = \varphi_0 \wedge \ldots \wedge \varphi_n,$$

$$\bigvee_{i \leq n} \varphi_i = \varphi_0 \vee \ldots \vee \varphi_n.$$

3:5 Oefening. (a) Bewijs de *Idempotentiewetten*

$$\varphi \vee \varphi \mathrel{\models\!\!\!\dashv} \varphi \qquad \text{en} \qquad \varphi \wedge \varphi \mathrel{\models\!\!\!\dashv} \varphi.$$

(b) Bewijs de *Absorptiewetten*

$$\varphi \vee (\varphi \wedge \psi) \mathrel{\models\!\!\!\dashv} \varphi \qquad \text{en} \qquad \varphi \wedge (\varphi \vee \psi) \mathrel{\models\!\!\!\dashv} \varphi.$$

(c) Bewijs de Noncontradictiewet en de Wet van de Uitgesloten Derde in de vorm

$$\varphi \wedge \neg\varphi \mathrel{\models\!\!\!\dashv} \bot \qquad \text{en} \qquad \varphi \vee \neg\varphi \mathrel{\models\!\!\!\dashv} \top.$$

§4 Modellen en Geldigheid

Hier is een eenvoudig voorbeeld van een redenering waarvan de geldigheid berust op de betekenis van connectieven:

(4.1) Als de zon schijnt, dan regent of sneeuwt het niet. Het regent. Dus de zon schijnt niet.

De premissen zijn 'Als de zon schijnt, dan regent of sneeuwt het niet' en 'Het regent'; de conclusie is 'de zon schijnt niet'. Volgens de inleiding van dit Deel betekent *geldigheid* van (4.1) dat de conclusie waar is onder alle omstandigheden waarin de premissen waar zijn. We kunnen nu precies uitleggen om wat voor omstandigheden het gaat.

4.1 Definitie. Een valuatie V is een *model* van een verzameling Φ van formules als $V(\varphi) = 1$ voor alle $\varphi \in \Phi$. Notatie: $V \models \Phi$.

We zeggen ook wel dat Φ *vervuld* wordt door V. In plaats van 'model voor $\{\varphi\}$' en '$V \models \{\varphi\}$' schrijven we: model van φ, en $V \models \varphi$. Als V een model is van φ, dan zeggen we ook dat V *voldoet aan* φ.

4.2 Definitie. Laat $\Phi \cup \{\psi\}$ een verzameling formules zijn. We schrijven

$$\Phi \models \psi$$

als ieder model van Φ ook een model is van ψ.

Als Φ eindig is, zeg $\Phi = \{\varphi_1, \ldots, \varphi_n\}$, dan noteren we ook wel

$$\varphi_1, \ldots, \varphi_n \models \varphi.$$

We korten '$\emptyset \models \varphi$' af tot $\models \varphi$. Dat stemt overeen met §3: *iedere* valuatie is een model voor $\emptyset$, dus $\emptyset \models \varphi$ juist als φ een tautologie is.

Redenering (4.1) is geldig omdat

(4.2) de zon schijnt $\to$ ¬(het regent ∨ het sneeuwt), het regent $\models$ ¬ de zon schijnt

We gaan dat na met een waarheidstafel, waarin we de propositie-atomen afkorten tot respectievelijk z, r en s.

z	r	s	$r \vee s$	$\neg(r \vee s)$	$z \to \neg(r \vee s)$	$\neg z$
1	1	1	1	0	0	0
1	1	0	1	0	0	0
1	0	1	1	0	0	0
1	0	0	0	1	1	0
0	1	1	1	0	1	1
0	1	0	1	0	1	1
0	0	1	1	0	1	1
0	0	0	0	1	1	1

Op de twee, omkaderde, regels van de tabel die de valuaties representeren waaronder beide premissen waar zijn, is de conclusie waar. Dat betekent dat inderdaad

(4.3) $$z \to \neg(r \vee s), r \models \neg z\ ,$$

wat de drie propositieletters ook betekenen.

Er zijn ook *ongeldige* redeneringen. Het volgende toont een veelgemaakte fout:

(4.4) Als het regent, schijnt de zon niet. De zon schijnt niet. Dus het regent.

Een waarheidstafel levert nu een *tegenvoorbeeld*: een situatie waarin de premissen waar zijn en de conclusie onwaar is.

r	z	$r \to \neg z$	$\neg z$
1	1	0	0
1	0	1	1
0	1	1	0
0	0	1	1

Elke valuatie V waarvoor $V(r) = V(z) = 0$ is een model van de premissen, maar niet van de conclusie. We noteren: $r \to \neg z, \neg z \not\models r$.

4:1 Oefening. (a) Construeer modellen, zo mogelijk, voor
(i) $\{p, q, \neg r\}$ (iii) $\{p \to q \to r, p \vee q, p \to q, \neg r\}$
(ii) $\{p \to \neg p, q \to p, q\}$
(b) Ga na of (i) $\neg\neg(p \to q) \models q \to p$
(ii) $\neg p \models (p \to q) \vee p$
(c) Laat zien dat
(i) $\varphi_0, \ldots, \varphi_n \models \psi$ dan en slechts dan als $\varphi_0, \ldots, \varphi_{n-1} \models \varphi_n \to \psi$;
(ii) $\varphi, \psi \models \chi$ dan en slechts dan als $\models \varphi \wedge \psi \to \chi$
dan en slechts dan als $\models \varphi \to \psi \to \chi$.

4.3 Voorbeelden

Een enkel tegenvoorbeeld volstaat om te bewijzen dat een redeneerschema ongeldig is. Er is dus iets voor te zeggen om te proberen, in plaats van een complete waarheidstafel, één regel te construeren die een tegenvoorbeeld weergeeft.
(a) Is $(\neg p \to \neg q) \to (p \leftrightarrow q)$ een tautologie? We zoeken naar een tegenvoorbeeld V. Uit de definitie van $\to$ volgt dat $V(\neg p \to \neg q) = 1$ moet zijn en $V(p \leftrightarrow q) = 0$. Het laatste impliceert dat $V(p) \neq V(q)$, dus $V(\neg p) \neq V(\neg q)$, wat bij $V(\neg p \to \neg q) = 1$ betekent dat $V(p) = 1$ en $V(q) = 0$.
(b) Is $p \wedge (q \vee r) \,/\, (p \wedge q) \vee r$ een geldige gevolgtrekking? Voor een tegenvoorbeeld V zou moeten gelden: $V(p \wedge (q \vee r)) = 1$ en $V((p \wedge q) \vee r) = 0$. Het laatste impliceert direct dat $V(r) = 0$; $V(p \wedge (q \vee r)) = 1$ vereist dus dat $V(q) = 1$. Bovendien is nodig dat $V(p) = 1$, waardoor $V(p \wedge q) = 1$, en $V((p \wedge q) \vee r) \neq 0$.
Een tegenvoorbeeld is dus onmogelijk, en de gevolgtrekking is geldig.

4.4 Beslisbaarheid en complexiteit. Een geldigheidsprobleem is een probleem van de vorm

(4.5) is $\varphi_1, \ldots, \varphi_n \,/\, \psi$ een geldige gevolgtrekking?

We kunnen (4.5) ook formuleren als een *vervulbaarheidsprobleem*, een probleem van de vorm

(4.6) heeft $\{\psi_1, \ldots, \psi_k\}$ een model?

— want $\varphi_0, \ldots, \varphi_n \models \psi$ dan en slechts dan als $\{\varphi_0, \ldots, \varphi_n, \neg\psi\}$ *niet* vervulbaar is.

De constructie van waarheidstafels is een onfeilbare methode om zulke problemen op te lossen. Het is echter wel een bewerkelijke methode: als het probleem n propositieletters bevat, heeft de waarheidstafel 2^n regels. Anders gezegd: als probleem P maar één propositieletter meer bevat dan probleem Q, kost de oplossing van P tweemaal zo veel moeite als die van Q. Zulke problemen worden in de informatica *exponentieel* genoemd, en ze gelden als praktisch onoplosbaar.

Anderzijds, verifiëren dat een gegeven valuatie een tegenvoorbeeld is, is goed te doen: het is ongeveer even moeilijk als het opschrijven van het probleem. Dit probleemtype heet *lineair*. De lineaire problemen vormen een deelklasse van de *polynomiale* problemen. Een gelukkige gok maakt het vervulbaarheidsprobleem polynomiaal; zulke problemen heten *nondeterministisch polynomiaal*. Van geen enkel probleem van dit type is nog bewezen dat het echt niet polynomiaal is.

Oefeningen

4:2 Zoek tegenvoorbeelden voor

(i) $p \to q \to r \,/\, q \to p \to r$

(ii) $p \wedge q \to r \,/\, (p \to q) \to r$

4:3 Onderzoek de gevolgtrekking $p \to q \,/\, (\neg p \to \neg q) \to \bot$ op geldigheid.

4:4 Ga na dat onderstaande gevolgtrekkingsregels geldig zijn:

(a) $\varphi, \varphi \to \psi \,/\, \psi$ (modus ponens)

(b) $\neg\psi, \varphi \to \psi \,/\, \neg\varphi$ (modus tollens)

(c) $\neg\psi \to \neg\varphi \,/\, \varphi \to \psi$ (contrapositie)

(d) $\psi \to \chi, \varphi \to \chi, \varphi \vee \psi \,/\, \chi$

4:5 *Het busvertragingsprobleem*. Gegeven zijn de volgende premissen:

(i) Als Wim de bus neemt, dan mist hij zijn afspraak als de bus te laat is.

(ii) Wim moet niet naar huis gaan als hij zijn afspraak mist en terneergeslagen is.

(ii) Als Wim de baan niet krijgt, dan is hij terneergeslagen en moet hij niet naar huis gaan.

Welke van de volgende beweringen volgen daar *niet* uit? Geef tegenvoorbeelden.

(1) Als Wim de bus neemt, dan krijgt hij de baan, als de bus te laat is.

(2) Wim krijgt de baan als hij zijn afspraak mist en naar huis moet gaan.

(3) Als de bus te laat is, dan neemt Wim niet de bus; of Wim mist zijn afspraak niet als hij de baan niet krijgt.

(4) Wim neemt niet de bus als de bus te laat is en hij de baan niet krijgt.

(5) Als Wim zijn afspraak niet mist, dan moet hij niet naar huis gaan en krijgt hij de baan niet.

(6) Wim is terneergeslagen als de bus te laat is of hij zijn afspraak mist.

(7) Als Wim de baan krijgt, dan is hij niet terneergeslagen, of moet hij niet naar huis gaan.

(8) Als Wim naar huis moet gaan, en de bus neemt, dan is hij niet terneergeslagen als de bus te laat is.

4:6* *De Cantorruimte*. Beschouw de verzamelingen 2^ω van alle functies van de verzameling ω der natuurlijke getallen naar de verzameling $\{0, 1\}$ (= 2) en $2^{<\omega}$ van eindige rijtjes nullen en enen — beginsegmenten van de elementen van 2^ω. Voor $\sigma \in 2^{<\omega}$ definieert men

$$B_\sigma = \{f \in 2^\omega \,|\, \text{als } n \in \operatorname{Dom}\sigma, \text{ dan } f(n) = \sigma(n)\},$$

de *boom op* σ.

(a) Bewijs: de collectie $\mathcal{B} := \{B_\sigma | \sigma \in 2^{<\omega}\}$ is de basis van een topologie op 2^ω.

De verzameling 2^ω met de topologie bepaald door $\mathcal{B}$ heet de *Cantorruimte*. De punten in deze ruimte corresponderen één op één met de valuaties: f correspondeert met de valuatie V_f gedefinieerd door $V_f(p_n) = f(n)$.
(b) Bewijs: de elementen van $\mathcal{B}$ zijn gesloten in de Cantorruimte.

Laten we een verzameling $X \subseteq 2^\omega$ *propositioneel* noemen als er een formule φ bestaat zo dat $X = \{f \in 2^\omega | V_f(\varphi) = 1\}$.
(c) Bewijs: de propositionele verzamelingen zijn zowel open als gesloten.
(d) Bewijs dat de Cantorruimte compact is. (Gebruik König's Lemma om te bewijzen dat als $X = \bigcup\{B_\sigma | \sigma \in \Sigma\}$ uitsluitend voor oneindige Σ, er een punt buiten X moet bestaan.)
(e) Bewijs: als een verzameling zowel open als gesloten is, is ze propositioneel.

§5 Waarheidsfuncties en normaalvormen

In het voorafgaande hebben we een aantal operaties op de verzameling $\{0, 1\}$ der waarheidswaarden ingevoerd: connectieven als ¬ (eenplaatsig), ∧ (tweeplaatsig), enzovoort. Er zijn echter veel meer van zulke operaties mogelijk. In het bijzonder kunnen we een formule waar hoogstens de propositieletters $p_0, \ldots, p_{k-1}$ in voorkomen, opvatten als een k-plaatsige operatie op waarheidswaarden. Neem de formule $\varphi = (p_0 \to p_1) \vee (\neg p_0 \to p_2) \to p_2$ uit 3.5.2: de waarheidstafel in dat voorbeeld associeert met elk invoerdrietal $\langle p_0, p_1, p_2 \rangle$ van nullen en enen een uitvoerwaarde, die we kunnen schrijven als $\varphi[p_0, p_1, p_2]$. Bijvoorbeeld, $\varphi[0, 1, 1] = 1$.

5.1 Definitie. Een *n-plaatsige waarheidsfunctie* is een functie van $\{0, 1\}^n$ naar $\{0, 1\}$.

Er is precies één functie met leeg domein, dus $\{0, 1\}^0$ heeft precies één element. Een functie waarvan het domein maar één element heeft, is constant. In het bijzonder corresponderen de nulplaatsige waarheidsfuncties met de formules ⊥ (constant 0) en ⊤ (constant 1).

Om aan te geven dat we een formule ψ bedoelen als n-plaatsige waarheidsfunctie, schrijven we $\psi^{(n)}$. Dus in het geval van φ hierboven:

$$\varphi^{(3)}[0, 1, 1] = 1.$$

We spreken af dat n altijd minstens één groter is dan de hoogste propositieletter-index die in de formule voorkomt. We mogen φ dus ook vierplaatsig maken: $\varphi^{(4)}[p_0, p_1, p_2, p_3] = \varphi^{(3)}[p_0, p_1, p_2]$, bijvoorbeeld $\varphi^{(4)}[0, 1, 1, 0] = 1$.

5.2 Definitie. Zij φ een formule die geen andere propositieletters bevat dan $p_0, \ldots, p_{n-1}$. Dan is $\varphi^{(n)}$ de functie f van $\{0, 1\}^n$ naar $\{0, 1\}$ met de eigenschap dat voor elke valuatie V,

$$f(V(p_0), \ldots, V(p_{n-1})) = V(\varphi).$$

Deze definitie is toelaatbaar op grond van het Eindigheidslemma (3.5.1).

We hebben zo voor elk paar van een formule en een geschikte (niet te kleine) plaatsigheid een waarheidsfunctie bepaald. Nu keren we het probleem om:

kunnen we bij een gegeven n-plaatsige waarheidsfunctie f een formule φ vinden zo dat $\varphi^{(n)} = f$?

5.3 Stelling. Zij f: $\{0, 1\}^n \longrightarrow \{0, 1\}$ een waarheidsfunctie. Dan is er een formule φ zo dat $\varphi^{(n)} = f$.

Bewijs. Als $n = 0$, dan kies je $\bot$ of $\top$ als φ.

Laat anders W de verzameling zijn van alle rijtjes $\bar{x} = \langle x_0,\ldots, x_{n-1}\rangle \in \{0, 1\}^n$ waarvoor $f(\bar{x}) = 1$. Neem $\varphi = \bot$ als $W = \emptyset$. Definieer anders voor alle $\bar{x} \in W$:

$$\varphi_{\bar{x}} = \bigwedge_{i<n} \alpha_i, \qquad \text{waar } \alpha_i = \begin{cases} p_i \text{ als } x_i = 1, \\ \neg p_i \text{ als } x_i = 0. \end{cases}$$

Laat $\varphi = \bigvee_{\bar{x} \in W} \varphi_{\bar{x}}$. Dan is gemakkelijk in te zien (cf. 3:4(c)) dat $\varphi^{(n)} = f$. ⊠

De bijzondere gevallen $n = 0$ en $W = \emptyset$ kunnen vermeden worden door af te spreken dat $\bigwedge\emptyset = \top$ en $\bigvee\emptyset = \bot$. Dat doen we bij dezen.

5.4 Gevolg (Disjunctieve Normaalvormstelling). Elke formule is logisch equivalent met een disjunctie van conjuncties van propositieletters en negaties van propositieletters.

Bewijs. Zij ψ een formule; neem n groter dan de hoogste propositieletterindex die voorkomt in ψ. Construeer voor $f = \psi^{(n)}$ een formule φ als in de voorgaande stelling. Dan $\varphi^{(n)} = \psi^{(n)}$, dus φ en ψ zijn logisch equivalent. ⊠

Een formule α die een conjunctie is van conjuncties van propositieletters en negaties van propositieletters heet een *disjunctieve normaalvorm*; een *volle* disjunctieve normaalvorm in het bijzondere geval dat elke propositieletter die in α voorkomt in ieder disjunct van α precies éénmaal voorkomt. Een (volle) disjunctieve normaalvorm α die logisch equivalent is met een gegeven formule β noemen we een (volle) *disjunctieve normaalvorm van* β. De formule $\varphi^{(n)}$ in het bewijs van 5.4 is een volle disjunctieve normaalvorm van ψ.

5.5 Voorbeelden. De constructie van een disjunctieve normaalvorm φ van een formule ψ zoals hierboven beschreven komt er in feite op neer dat je disjuncten van φ afleest van een waarheidstafel voor ψ.

(i) $\psi = (p \to q) \to r$; we behandelen p als p_0, q als p_1, r als p_2.

p	q	r	$p \to q$	$(p \to q) \to r$	
1	1	1	1	1	$\alpha_{111} = p \wedge q \wedge r$
1	1	0	1	0	
1	0	1	0	1	$\alpha_{101} = p \wedge \neg q \wedge r$
1	0	0	0	1	$\alpha_{100} = p \wedge \neg q \wedge \neg r$
0	1	1	1	1	$\alpha_{011} = \neg p \wedge q \wedge r$
0	1	0	1	0	
0	0	1	1	1	$\alpha_{001} = \neg p \wedge \neg q \wedge r$
0	0	0	1	0	

Resultaat: $\varphi = \alpha_{111} \vee \alpha_{101} \vee \alpha_{100} \vee \alpha_{011} \vee \alpha_{001} =$

$$(p \wedge q \wedge r) \vee (p \wedge \neg q \wedge r) \vee (p \wedge \neg q \wedge \neg r) \vee (\neg p \wedge q \wedge r) \vee (\neg p \wedge \neg q \wedge r).$$

We hadden ψ ook kunnen zien als een *vier*waardige waarheidsfunctie; de normaalvorm was dan ruim twee keer zo lang geworden.
(ii) $\psi = (p \to \neg p) \wedge p$.

p	$\neg p$	$p \to \neg p$	$(p \to \neg p) \wedge p$
1	0	0	0
0	1	1	0

Er zijn geen regels in de tabel die iets opleveren, dus $\varphi = \bot$.
(iii) Een andere — dikwijls minder bewerkelijke — manier om normaalvormen te construeren is *algebraïsch*, door gebruik te maken van bekende logische equivalenties. We berekenen:

$(p \to q) \to r \mathrel{\models\!\!\!\dashv} \neg(\neg p \vee q) \vee r$ volgens 3.7.5,
$\mathrel{\models\!\!\!\dashv} (\neg\neg p \wedge \neg q) \vee r$ volgens De Morgan,
$\mathrel{\models\!\!\!\dashv} (p \wedge \neg q) \vee r$ volgens de dubbele negatiewet;
en $(p \to \neg p) \wedge p \mathrel{\models\!\!\!\dashv} (\neg p \vee \neg p) \wedge p$ volgens 3.7.5,
$\mathrel{\models\!\!\!\dashv} \neg p \wedge p$ wegens idempotentie (3:5a)
$\mathrel{\models\!\!\!\dashv} \bot$ volgens noncontradictie (3:5c).

5:1 Oefening. Geef disjunctieve normaalvormen voor de volgende formules:
(i) $\neg(p \to q)$ (iii) $p \leftrightarrow q$
(ii) $(p \to q) \to p$ (iv) $\neg(q \wedge (p \to \neg p))$

5.6 Functionele volledigheid

Als het doel van de formules van de propositielogica is: waarheidsfuncties uit te drukken — daar is iets voor te zeggen — dan leert Stelling 3 ons dat ze daarin slagen. Omgekeerd kunnen we ons nu weer afvragen of die formules niet zuiniger kunnen. Zijn alle symbolen die we hebben ingevoerd in §2 wel nodig?

Dat haakjes niet nodig zijn, weten we uit Oefening 2:3 (Poolse notatie). We hebben wel echt oneindig veel propositieletters nodig: de projectie van rijtjes van n waarheidswaarden op de j-de coördinaat ($1 \leq j \leq n$), d.i. de toekenning

$$\langle q_0, \ldots, q_{n-1} \rangle \mapsto q_{j-1}$$

is een waarheidsfunctie, en p_{j-1} representeert haar.

5:2 Oefening. Bewijs dat een formule waar p_{j-1} niet in voorkomt niet logisch equivalent is met p_{j-1}.

Nemen we nu de haakjes en propositieletters als gegeven aan, dan is de les van Stelling 3 dat we voldoende connectieven hebben. Sterker: we hebben genoeg aan $\vee$, $\wedge$, $\neg$, $\top$ en $\bot$.

Van de nulplaatsige connectieven kunnen we er nog één weglaten, want $\top = \neg\bot$ en $\bot = \neg\top$. Sterker: als we de nulplaatsige waarheidsfuncties, die we natuurlijk nooit kunnen uitdrukken als we niet beschikken over minstens één nulplaatsig connectief, buiten beschouwing laten, dan kunnen we $\top$ en $\bot$ allebei laten vallen. Want $\top$ is logisch equivalent met $p \vee \neg p$.

Het woord *connectief* is in het voorafgaande tamelijk informeel gebruikt. Voor de volgende discussie definiëren we het precies, als: *symbool van het logisch formalisme dat een bepaalde waarheidsfunctie uitdrukt*. Tot nog toe hebben we nul-, één- en tweeplaatsige connectieven gezien, maar een connectief zou ook drie argumenten kunnen hebben, of zelfs nog meer. Het resultaat van toepassing van een n-plaatsig connectief F op formules $\varphi_1,\dots, \varphi_n$ noteren we algemeen als $F(\varphi_1,\dots, \varphi_n)$, zonder daarmee uit te sluiten dat de formule in het echt anders genoteerd wordt, bijvoorbeeld als $\varphi_1 \wedge \varphi_2$. We gaan er wel van uit dat unieke leesbaarheid op één of andere manier gegarandeerd is. We evalueren $F(\varphi_1,\dots, \varphi_n)$ op dezelfde manier als de standaardformules van §2: een valuatie V wordt zo uitgebreid dat

(*) $$V(F(\varphi_1,\dots, \varphi_n)) = F(V(\varphi_1),\dots, V(\varphi_n));$$

wegens unieke leesbaarheid berekenen we zo voor elke formule een unieke waarheidswaarde.

5.6.1 Definitie. Laat C een verzameling connectieven zijn. Dan is FP[C] de kleinste verzameling X van uitdrukkingen die
(i) alle propositieletters bevat, en waarvoor geldt
(ii) als $F \in C$ n-plaatsig is, en $\varphi_1,\dots, \varphi_n \in X$, dan ook $F(\varphi_1,\dots, \varphi_n) \in X$.

5.6.2 Definitie. Een verzameling C van connectieven is *functioneel volledig* als er, voor elke $n \geq 1$, voor elke n-plaatsige waarheidsfunctie f een formule $\varphi \in$ FP[C] bestaat zo dat $\varphi^{(n)} = f$.

Men spreekt ook wel van een *stelsel* van connectieven.

5.6.3 Voorbeelden. (i) $\{\neg, \wedge, \vee\}$ is functioneel volledig, en elke uitbreiding van die verzameling dus ook.
(ii) De lege verzameling is niet functioneel volledig, want propositieletters stellen projecties voor, en niet elke waarheidsfunctie is een projectie.
(iii) $\{\bot, \wedge, \vee\}$ is niet functioneel volledig. Als namelijk $\varphi \in$ FP[$\bot, \wedge, \vee$], dan $\varphi^{(n)}(0,\dots, 0) = 0$ (bewijs met inductie naar φ), dus negatie is niet uitdrukbaar.

Oefeningen
5:3 Bewijs dat $\bigwedge_{i<n} \varphi_i$ logisch equivalent is met $\neg \bigvee_{i<n} \neg\varphi_i$, en $\bigvee_{i<n} \varphi_i$ met $\neg \bigwedge_{i<n} \neg\varphi_i$. (Inductie naar n.)
5:4 Bewijs dat $\{\neg, \vee\}$ en $\{\neg, \wedge\}$ functioneel volledig zijn.
5:5 Toon aan dat de volgende stelsels *niet* functioneel volledig zijn:
(i) $\{\bot, \wedge\}$; (ii) $\{\wedge, \vee\}$; (ii) $\{\wedge, \rightarrow\}$; (iv) $\{\neg, \leftrightarrow\}$.

5.7 Substitutie

Elk stelsel C van connectieven bepaalt een propositielogische taal; FP[C] is de verzameling van alle 'beweringsvormen' van die taal. Laat nu C_1 en C_2 stelsels van connectieven zijn. Een functie f: FP[C_1] $\longrightarrow$ FP[C_2] is een correcte *vertaling* als, bij gegeven betekenissen van de propositieletters, $f(\varphi)$ steeds hetzelfde betekent als φ. We zullen onderzoeken hoe zo'n vertaling gebaseerd kan worden op een correspondentie van connectieven in C_1 met formules in FP[C_2].

5.7.1 Definitie (simultane substitutie). Laat C een stelsel van connectieven zijn, $q_0,\dots, q_{n-1}$ verschillende propositieletters, en $\varphi_0,\dots, \varphi_{n-1}$, $\psi \in$ FP[C]. Dan is $[\varphi_0/q_0,\dots, \varphi_{n-1}/q_{n-1}]\psi$ gedefinieerd door

(i) $[\varphi_0/q_0,\ldots,\varphi_{n-1}/q_{n-1}]\psi = \psi$ als $q_0,\ldots,q_{n-1}$ niet voorkomen in ψ;
(ii) $[\varphi_0/q_0,\ldots,\varphi_{n-1}/q_{n-1}]q_i = \varphi_i$ voor alle $i < n$;
(iii) als $\psi = F(\psi_1,\ldots,\psi_k)$, voor zeker k-plaatsig connectief $F \in C$, dan $[\varphi_0/q_0,\ldots,\varphi_{n-1}/q_{n-1}]\psi =$

$$F([\varphi_0/q_0,\ldots,\varphi_{n-1}/q_{n-1}]\psi_1,\ldots,[\varphi_0/q_0,\ldots,\varphi_{n-1}/q_{n-1}]\psi_k).$$

In een slordiger, maar meer aansprekende notatie, voert men ψ in als

$$\psi(q_0,\ldots,q_{n-1}),$$

met verschillende propositieletters $q_0,\ldots,q_{n-1}$ klaar voor substitutie, en noteert men $\psi(\varphi_0,\ldots,\varphi_{n-1})$ in plaats van $[\varphi_0/q_0,\ldots,\varphi_{n-1}/q_{n-1}]\psi$. Soms spreekt men dan meteen ook af dat ψ geen andere propositieletters bevat dan $q_0,\ldots,q_{n-1}$.

5.7.2 Lemma. Laat $\varphi_0,\ldots,\varphi_{n-1}, \psi(p_0,\ldots,p_{n-1}) \in \mathrm{FP}[C]$, waarbij ψ geen andere propositieletters bevat dan $p_0,\ldots,p_{n-1}$, laat V een valuatie zijn, en W een valuatie zo dat voor alle $i < n$, $W(p_i) = V(\varphi_i)$. Dan $V(\psi(\varphi_0,\ldots,\varphi_{n-1})) = W(\psi)$.

Bewijs. Met inductie naar ψ.
Als ψ een propositieletter is, dan $\psi = p_i$, met $i < n$. Dan

$$V(\psi(\varphi_0,\ldots,\varphi_{n-1})) = V(\varphi_i) = W(p_i).$$

Als $\psi = F(\psi_1,\ldots,\psi_k)$, voor zeker k-plaatsig connectief $F \in C$, dan

$$\begin{aligned} V(\psi(\varphi_0,\ldots,\varphi_{n-1})) &= V(F(\psi_1(\varphi_0,\ldots,\varphi_{n-1}),\ldots,\psi_k(\varphi_0,\ldots,\varphi_{n-1}))) \\ &= F(V(\psi_1(\varphi_0,\ldots,\varphi_{n-1})),\ldots,V(\psi_k(\varphi_0,\ldots,\varphi_{n-1}))) \end{aligned}$$

wegens (*) in 5.6. Dus volgens inductiehypothese en opnieuw (*),

$$V(\psi(\varphi_0,\ldots,\varphi_{n-1})) = F(W(\psi_1),\ldots,W(\psi_k)) = W(\psi). \qquad \boxtimes$$

5.7.3 Simultane Substitutiestelling. Laat $\varphi_0,\ldots,\varphi_{n-1}, \psi(p_0,\ldots,p_{n-1}) \in \mathrm{FP}[C]$, waarbij ψ geen andere propositieletters bevat dan $p_0,\ldots,p_{n-1}$, en zij V een valuatie. Dan $V(\psi(\varphi_0,\ldots,\varphi_{n-1})) = \psi^{(n)}[V(\varphi_0),\ldots,V(\varphi_{n-1})]$.

Bewijs. Neem een valuatie W als in het lemma. Dan

$$\psi^{(n)}[V(\varphi_0),\ldots,V(\varphi_{n-1})] = \psi^{(n)}[W(p_0),\ldots,W(p_{n-1})] = W(\psi)$$

volgens de definitie van $\psi^{(n)}$. Pas nu het lemma toe. $\boxtimes$

Oefeningen
5:6 Bewijs het volgende *Compositielemma*: als $\varphi_1,\ldots,\varphi_n, \chi(p_0,\ldots,p_{n-1}) \in \mathrm{FP}[C]$, waarbij χ geen andere propositieletters bevat dan $p_0,\ldots,p_{n-1}$, en φ_i, voor $1 \le i \le n$, geen dan $p_0,\ldots,p_{m-1}$, dan is voor alle $x_0,\ldots,x_{m-1} \in \{0, 1\}^m$,

$$\chi^{(n)}[\varphi_1^{(m)}[x_0,\ldots,x_{m-1}],\ldots,\varphi_n^{(m)}[x_0,\ldots,x_{m-1}]] = \chi(\varphi_1,\ldots,\varphi_n)^{(m)}[x_0,\ldots,x_{m-1}].$$

5:7 Oefening. In 2:2 beschouwden we de substitutie van een uitdrukking α voor een propositieletter p in een uitdrukking β, en bewezen dat het resultaat $[\alpha/p]\beta$ een formule is, mits α en β formules zijn. Dat geldt natuurlijk algemeen: als $\alpha, \beta \in \mathrm{FP}[C]$, dan $[\alpha/p]\beta \in \mathrm{FP}[C]$.
(a) Laat p en q verschillende propositieletters zijn. Geef een voorbeeld waaruit blijkt dat *niet* per se $[\varphi/p][\psi/q]\chi = [\varphi/p,\psi/q]\chi$. (We lezen $[\varphi/p][\psi/q]\chi$ als $[\varphi/p]([\psi/q]\chi)$.)

(b) Laat p en q verschillende propositieletters zijn, en stel dat q niet voorkomt in φ. Bewijs dat $[\varphi/p][\psi/q]\chi = [[\varphi/p]\psi/q][\varphi/p]\chi$.
(c) Laat zien dat er voor elke formule φ en elke simultane substitutie σ een serie enkelvoudige substituties $\tau_i = [\psi_i/q_i]$ bestaat zo dat $\sigma\varphi = \tau_1 \ldots \tau_n\varphi$.

5.7.4 Stelling. Laat C en C' stelsels van connectieven zijn zo dat voor elke n, voor elke n-plaatsige $G \in C$, een formule $\varphi \in \mathrm{FP}[C']$ bestaat die geen andere propositieletters bevat dan $p_0, \ldots, p_{n-1}$, zo dat

$$(\dagger) \qquad \models G(p_0, \ldots, p_{n-1}) \leftrightarrow \varphi(p_0, \ldots, p_{n-1});$$

dan is er voor elke $\psi \in \mathrm{FP}[C]$ een formule $\psi^* \in \mathrm{FP}[C']$ die logisch equivalent is met ψ.

Bewijs. Inductie naar de complexiteit van ψ. Als ψ een propositieletter is, neem $\psi^* = \psi$. Als $\psi = G(\psi_1, \ldots, \psi_n)$, neem dan φ als in (†), en definieer:

$$\psi^* = \varphi(\psi_1^*, \ldots, \psi_n^*),$$

waar $\psi_i^* \in \mathrm{FP}[C']$, $1 \leq i \leq n$, logisch equivalent is met ψ_i — zulke ψ_i^* bestaan volgens inductiehypothese. De Simultane Substitutiestelling geeft nu voor elke valuatie V:

$$V(\psi) = G(V(\psi_1), \ldots, V(\psi_n)) = \varphi^{(n)}[V(\psi_1^*), \ldots, V(\psi_n^*)] = V(\psi^*),$$

want $G = \varphi^{(n)}$ volgens (†). ⊠

Oefeningen

5:8 (a) Bewijs dat $\{\neg, \rightarrow\}$ functioneel volledig is.
(b) Ga na dat $\varphi \rightarrow \bot$ logisch equivalent is met $\neg\varphi$. Concludeer dat $\{\bot, \rightarrow\}$ functioneel volledig is.

5:9 De *pijl van Peirce* is gedefinieerd door de tabel

$(p \downarrow q)$

$p \backslash q$	1	0
1	0	0
0	0	1

Bewijs dat $\{\downarrow\}$ functioneel volledig is.

5:10 Het drieplaatsige *voorwaardelijke keuze*-connectief '… als … anders …' wordt gedefinieerd door onderstaande tabel:

p	q	r	$p \lhd q \rhd r$
1	1	1	1
1	1	0	1
1	0	1	1
1	0	0	0
0	1	1	0
0	1	0	0
0	0	1	1
0	0	0	0

(a) Laat zien dat $\{\text{-}\lhd\text{-}\rhd\text{-}\}$ niet functioneel volledig is.
(b) Is $\{\text{-}\lhd\text{-}\rhd\text{-}, \neg\}$ functioneel volledig? En $\{\text{-}\lhd\text{-}\rhd\text{-}, \bot\}$?

5:11 Een ridder wordt door een boze tovenaar ontwapend en in een vertrek gebracht met drie deuren. Voordat hij de deur waardoor de ridder is binnengekomen op slot doet, deelt de tovenaar hem mee dat hij de beide andere deuren van binnen kan openen; dat achter één daarvan een draak op de loer ligt; en dat zich achter de andere de prinses bevindt die hij kwam bevrijden. Dringende zaken roepen hem elders, maar hij heeft zijn leerling, die er alles van af weet, geïnstrueerd om door het cipiersluikje één vraag van de ridder te beantwoorden. Hij heeft de leerling opgedragen om de waarheid te spreken, of om te liegen.

De tovenaar vertrekt. Wat moet de ridder aan de leerling vragen om zeker te weten welke uitgang hij moet kiezen?

5:12 Een *Zjegalkin-term* is een conjunctie van verschillende propositie-letters. (We tellen $\top$ als een conjunctie van nul propositieletters.) Een *Zjegalkin-veelterm* is een som

$$\tau_1 + \ldots + \tau_n$$

van Zjegalkin-termen zo dat voor alle $i < j$, τ_i en τ_j niet precies dezelfde propositieletters bevatten. ($\bot$ telt als een som van nul Zjegalkin-termen.)

(a) Laat zien dat elke formule logisch equivalent is met een Zjegalkin-veelterm.

(b) Bewijs dat $\bot$ de enige contradictoire Zjegalkin-veelterm is.

(c) Bewijs dat Zjegalkin-veeltermen $\tau_1 + \ldots + \tau_n$ en $\sigma_1 + \ldots + \sigma_m$ slechts dan logisch equivalent zijn als er een bijectie f van $\{\tau_1, \ldots, \tau_n\}$ op $\{\sigma_1, \ldots, \sigma_m\}$ bestaat zo dat voor alle i, $1 \leq i \leq n$, $f(\tau_i)$ dezelfde propositieletters bevat als τ_i.

§6 Natuurlijke deductie

In §4 is beschreven hoe men de geldigheid van een gevolgtrekking na kan gaan met een waarheidstafel. De waarheidstafelmethode is *semantisch*, in de zin dat ze direct gebruik maakt van een eenvoudige betekenistheorie (in andere kringen zou men zeggen: een *betekenismodel*) van de connectieven. Er zijn drie redenen om ook nog op een andere manier naar geldige redeneringen te kijken. Te weten:

1° Een betoog bestaat meestal uit *meerdere* gevolgtrekkingen. De bedoeling is immers te overtuigen, en een moeilijke gevolgtrekking snapt niemand. We willen 'moeilijke' gevolgtrekkingen bewijzen door eenvoudige tussenstappen van een paar vaste typen.

2° In het vervolg zullen we het logische formalisme uitbreiden; waarheidstafels zullen dan te kort schieten.

3° Het eenvoudige betekenismodel waarop de methoden van §4 berusten, houdt onder meer in dat elke bewering in een gevolgtrekking waar is of onwaar. Men kan betwijfelen of dat juist is. Misschien kan een bewering ook *een beetje* waar zijn, of onnauwkeurig, of vooralsnog onduidelijk.

6.1 Afleidingen

Een *afleiding* is een rijtje formules. Sommige formulevoorkomens in het rijtje zijn *aannamen*; de andere zijn volgens bepaalde regels *afgeleid* uit eerdere formules. Een aanname kan tijdelijk zijn, en in de loop van de afleiding, opnieuw volgens bepaalde regels, worden *ingetrokken*. Vanaf het punt waarop een aanname is ingetrokken, is ze *niet meer van kracht*, samen met de andere formulevoorkomens tussen de aanname en het intrekkingspunt. Van een aanname die van kracht is, zeggen we ook wel dat ze *open staat*.

Een afleiding waarvan ψ de laatste formule is, en waarin $\varphi_1, \ldots, \varphi_n$ de niet-ingetrokken aannamen zijn, heet een afleiding *van* ψ *uit* $\varphi_1, \ldots, \varphi_n$. Als een dergelijke afleiding bestaat, dan noteren we dat met

$$\varphi_1, \ldots, \varphi_n \vdash \psi.$$

De simpelste *afleidingsregel* op grond waarvan formules anders dan als aanname voor kunnen komen is *herhaling*. Als φ als n-de formule voorkomt in de afleiding, en dat voorkomen m stappen later nog van kracht is, dan mag φ optreden als $(n + m + 1)$-ste formule als herhaling van formule nummer n. In een schema:

$$\begin{array}{rll} & \vdots & \\ \text{n.} & \varphi & \\ & \vdots & \\ \text{n + m + 1.} & \varphi & \qquad \text{(herhaling van n.)} \end{array}$$

Een vereenvoudigde vorm van het schema is:

$$\frac{\varphi}{\varphi} \qquad\qquad \text{herhalingsregel}$$

6.2 Introductie- en eliminatieregels

De overige afleidingsregels vallen uiteen in twee soorten. Bij elke clausule van de definitie van formules (2.2) kunnen we ons afvragen

— op grond van wat voor informatie in het voorafgaande we een volgens die clausule samengestelde formule mogen *introduceren*; en

— wat voor informatie we uit een volgens die clausule gevormde formule kunnen halen, of, kras gezegd, hoe we de samenstelling kunnen *elimineren*.

We weten dat $\varphi \wedge \psi$ als we weten dat φ en dat ψ. Dus als φ en ψ van kracht zijn, mogen we $\varphi \wedge \psi$ introduceren. Schematisch:

$$\begin{array}{rlcrll} & \vdots & & & \vdots & \\ \text{n.} & \varphi & & \text{n.} & \psi & \\ & \vdots & & & \vdots & \\ \text{n + m.} & \psi & & \text{n + m.} & \varphi & \\ & \vdots & & & \vdots & \\ \text{n + m + k + 1.} & \varphi \wedge \psi & \qquad & \text{n + m + k + 1.} & \varphi \wedge \psi & \quad \begin{array}{l}\text{(conjunctie-introductie} \\ \text{op n. en n + m.)}\end{array} \end{array}$$

In een vereenvoudigde vorm:

$$\frac{\varphi \qquad \psi}{\varphi \wedge \psi} \qquad \text{conjunctie-introductieregel}$$

De informatie die je *uit* $\varphi \wedge \psi$ kunt halen, is precies de informatie die je had moeten hebben om het te introduceren. In schema:

$$\begin{array}{ll}
\quad\vdots & \quad\vdots \\
n.\ \varphi \wedge \psi & n.\ \varphi \wedge \psi \\
\quad\vdots & \quad\vdots \\
n+m+1.\ \varphi\ (\wedge\text{-eliminatie op n, links}) & n+m+1.\ \psi\quad (\wedge\text{-eliminatie op n, rechts})
\end{array}$$

Als gevolgtrekkingsschema's:

$$\frac{\psi \wedge \varphi}{\psi}\ \wedge\text{-eliminatie links} \qquad\qquad \frac{\psi \wedge \varphi}{\varphi}\ \wedge\text{-eliminatie rechts}$$

De eliminatieregel voor implicatie ligt voor de hand. De betekenis van 'als φ, dan ψ' is dat we ψ weten zodra we φ weten, dus

$$\frac{\varphi \qquad \varphi \rightarrow \psi}{\psi} \qquad \text{implicatie-eliminatieregel}$$

De $\rightarrow$-introductieregel moet, zo mogelijk, de eliminatieregel rechtvaardigen. Anders gezegd, de informatie die we bij eliminatie uit een implicatie halen, moet bij de introductie beschikbaar zijn geweest. Nu zegt de eliminatieregel dat we, wegens $\varphi \rightarrow \psi$, uit φ mogen concluderen dat ψ; de informatie die dat rechtvaardigt is een afleiding Π van ψ uit φ.

Een dergelijke Π is een afleiding binnen een afleiding. We stipuleren dat Π binnen de hoofdafleiding een aaneengesloten blok van formules is, en dat de (voorlopige) conclusie $\varphi \rightarrow \psi$ meteen op Π volgt. Van alles dat in de hoofdafleiding voorafgaand aan Π van kracht is, mag binnen Π gebruik gemaakt worden. De eerste formule van Π is de aanname φ, en Π eindigt met ψ. Op het moment dat die laatste ψ wordt afgeleid, moet φ de enige aannname zijn binnen Π die nog open staat.

De rechtvaardiging van $\varphi \rightarrow \psi$ is de afleiding Π, niet het voorkomen van specifieke formules binnen Π. In het bijzonder hangt $\varphi \rightarrow \psi$ niet af van de aanname waar Π mee begint. Die is alleen van kracht binnen Π, en wordt *ingetrokken* zodra we besluiten met $\varphi \rightarrow \psi$. Verderop in de afleiding mogen we die aanname niet meer gebruiken; evenmin als de rest van Π.

Schematisch ziet de implicatie-introductie er als volgt uit:

$$\begin{array}{rl}
 & \vdots \\
n. & \varphi \\
 & \vdots \\
n+m. & \psi \\
n+m+1. & \varphi \rightarrow \psi
\end{array}$$

De grote haak zondert Π af van de rest van de afleiding, en benadrukt dat de regels n tot en met $n + m$ niet meer meedoen.

De introductieregels voor $\vee$ zijn de *verzwakkingen*

$$\frac{\varphi}{\varphi \vee \psi}\ \vee\text{-introductie links} \qquad\qquad \frac{\psi}{\varphi \vee \psi}\ \vee\text{-introductie rechts}$$

In omgekeerde richting betekent deze introductieregel dat, als we beschikken over $\varphi \vee \psi$, één van beide disjuncten waar moet zijn — we weten alleen niet welk. We kunnen die informatie benutten wanneer iets zowel uit φ volgt als uit ψ. De regel is:

$$\frac{\varphi \vee \psi \qquad \varphi \to \chi \qquad \psi \to \chi}{\chi} \qquad \text{disjunctie-eliminatieregel}$$

Een bijzondere rol heeft het nulplaatsige connectief $\bot$. Het heeft geen eigen introductieregel. We zullen *twee* mogelijke eliminatieregels overwegen.
I. *Ex falso sequitur quodlibet*. Gegeven dat $\bot$ geen introductieregel heeft, wat leren we als $\bot$ toch opduikt in de loop van een afleiding? We leren dat we in een uitzonderlijke situatie verkeren, en dat alle remmen los zijn. Zolang $\bot$ van kracht is, mogen we zeggen wat we willen. In schema:

$$\frac{\bot}{\varphi} \qquad \text{EFSQ}$$

II. *Reductio ad absurdum*. Iemand zou tegen kunnen werpen dat de ex falso-regel niets elimineert: de tegenspraak blijft staan. (*Daartegen* kunnen we dan weer inbrengen dat je uit een formule niet meer mag halen dan je erin stopt: wat je niet echt kunt introduceren, mag je dus ook niet echt elimineren.)

Zoals bekend (5:8b) is $\neg\varphi$ logisch equivalent met $\varphi \to \bot$; we zullen $\neg\varphi$ nu opvatten als afkorting van $\varphi \to \bot$. Als we uit $\neg\varphi$ de onwaarheid $\bot$ kunnen afleiden, dat is, als we bewijzen dat de aanname $\neg\varphi$ tot absurditeit leidt — hebben we dan niet bewezen dat φ waar moet zijn? De regel die dat goedkeurt ziet er schematisch zo uit:

$$\begin{array}{rl}
 & \vdots \\
\text{n.} & \neg\varphi \\
 & \vdots \\
\text{n + m.} & \bot \\
\text{n + m + 1.} & \varphi
\end{array}$$

6.3 Voorbeelden

(a) $p \wedge q \vdash q \wedge p$

1.	$p \wedge q$	aanname
2.	p	elim. $\wedge$, 1.
3.	q	elim. $\wedge$, 1.
4.	$q \wedge p$	intro $\wedge$, 2, 3.

(b) $p \to (q \to r), p \to q \vdash p \to r$

1.	$p \to (q \to r)$	aanname
2.	$p \to q$	aanname
3.	p	aanname
4.	q	elim. $\to$, 3, 2.
5.	$q \to r$	elim. $\to$, 3, 1.
6.	r	elim. $\to$, 4, 5.
7.	$p \to r$	

De bovenstaande afleidingen illustreren twee algemene tactische principes. Ten eerste beginnen we altijd met de premissen — de aannamen die van kracht mogen blijven. Afleiding (a) bestaat verder slechts in het uitpakken en

weer inpakken van de propositieletters. Ten tweede: als de te bewijzen formule een implicatie is, voegen we het antecedent meteen toe aan de premissen.
(c) Dat er een afleiding van φ bestaat zonder (blijvende) aannamen, noteren we met $\vdash \varphi$. Uit de afleiding in (b) hebben we in twee stappen een 'absolute' afleiding van $(p \to (q \to r)) \to (p \to q) \to p \to r$:

1.	$p \to (q \to r)$	aanname
2.	$p \to q$	aanname
	:	
	:	
7.	$p \to r$	
8.	$(p \to q) \to p \to r$	
9.	$(p \to (q \to r)) \to (p \to q) \to p \to r$	

De volgorde van de aannamen is belangrijk: eerst $p \to q$ aannemen en dan $p \to (q \to r)$ geeft een afleiding van $(p \to q) \to (p \to (q \to r)) \to p \to r$.
(d) $p \vdash p$

1.	p	aanname

Volgens de definitie is dit een afleiding. Dat er helemaal niets gebeurt, doet allicht vreemd aan. Als we dit in het echt als afleiding wilden slijten, zouden we op zijn minst doen alsof we redeneerden, als in: 'Neem aan dat p. Dan p. Dus p.' We kunnen zulke rondedansjes formaliseren met de herhalingsregel, maar in dit geval is dat niet nodig.

(e) $\vdash p \to p$

1.	p	aanname
2.	$p \to p$	

(f) $p \vee q \vdash q \vee p$

1.	$p \vee q$	aanname
2.	p	aanname
3.	$q \vee p$	intro $\vee$, 2
4.	$p \to q \vee p$	
5.	q	aanname
6.	$q \vee p$	intro $\vee$, 5
7.	$q \to q \vee p$	
8.	$q \vee p$	elim. $\vee$, 1, 4, 7

6:1 Oefening. Laat zien dat (i) $\vdash p \to q \to p$
(ii) $\vdash \neg(p \wedge \neg p)$
(iii) $p \wedge (q \wedge r) \vdash (p \wedge q) \wedge r$
(iv) $\neg p \vee \neg q \vdash \neg(p \wedge q)$
(v) $(p \to q) \to p \vdash q \to p$
(vi) $\vdash (p \to q) \to (\neg q \to \neg p)$
(vii) $\neg p \wedge \neg q \vdash \neg(p \vee q)$
(viii) $p \vee (q \vee r) \vdash (p \vee q) \vee r$
(ix) $p \to q \to r \vdash q \to p \to r$
(x) $\vdash p \to \neg\neg p$
(xi) $\vdash \neg\neg p \vee \neg\neg q \to \neg\neg(p \vee q)$.

6.4 De rol van de tegenspraak. De bovenstaande afleidingen zijn in zekere zin gemakkelijk: als je weet wat je moet bewijzen, dan zie je hoe het bewijs zal lopen. De bewijsstrategie is af te lezen aan de formules. Dat verandert wanneer de *reductio ad absurdum* in het spel komt. Je moet dan φ gaan bewijzen door $\perp$ af te leiden uit $\neg\varphi$; het vereist enige ervaring om te zien dat dat nodig is. De Wet van de Uitgesloten Derde vormt een goede illustratie:

$\vdash p \vee \neg p$

1.	$\neg(p \vee \neg p)$	aanname
2.	p	aanname
3.	$p \vee \neg p$	intro $\vee$, 2
4.	$\perp$	elim. $\to$, 1, 3
5.	$\neg p$	
6.	$p \vee \neg p$	intro $\vee$, 5
7.	$\perp$	elim. $\to$, 1, 6
8.	$p \vee \neg p$	

Men *kan* soms een disjunctie bewijzen door één van de disjuncten te bewijzen; maar in het algemeen mogen we noch van p, noch van $\neg p$ verwachten een afleiding te vinden. Dan proberen we het maar eens met de aanname $\neg(p \vee \neg p)$. Die blijkt voldoende om $p \vee \neg p$ af te leiden; vervolgens trekken we de aanname in. — Deze "maximale" aanpak is overigens niet altijd de handigste.

In feite is *reductio ad absurdum* equivalent met het uitgesloten derde. Als we namelijk naar believen formules van de vorm $\varphi \vee \neg\varphi$ mogen introduceren, bewijzen we *reductio* met het volgende afleidingsschema:

$\vdots$	
$\neg\varphi$	aanname
$\vdots$	
$\perp$	
φ	e.f.s.q.
$\neg\varphi \to \varphi$	
φ	aanname
$\varphi \to \varphi$	
$\varphi \vee \neg\varphi$	axioma
φ	elim. $\vee$

(Merk op dat *ex falso* wordt gebruikt.)

De *reductio ad absurdum*-regel is sterker dan *ex falso sequitur quodlibet*. Het onderstaande afleidingsschema toont dat de tweede regel volgt uit de eerste.

1.	$\perp$	
2.	$\neg\varphi$	aanname
3.	$\perp$	herhaling 1
4.	φ	

Andersom zouden we aan moeten tonen dat *reductio* niet volgt uit *ex falso*, maar dat zou ons te ver voeren. Misschien is een wijsgerige bespiegeling duidelijk genoeg.

Waarom zijn de principes van de logica geldig? In het voorafgaande zijn bijna alle eliminatieregels gerechtvaardigd vanuit de introductieregel: je mag iets concluderen, uit een bewering B van een bepaalde vorm, omdat het beschikbaar moet zijn geweest toen je B invoerde. Zo'n rechtvaardiging was er niet voor *reductio*.

De *reductio*-problematiek wordt gewoonlijk gedemonstreerd met de Wet van de Uitgesloten Derde. Waarom geloofden wij in 2008 dat over vijf jaar het Rijksmuseum weer open zou zijn, of niet?[5] Nu, we zouden na vijf jaar kunnen gaan kijken, en één van tweeën zou het geval zijn. De rechtvaardiging is dan: we weten wat er bedoeld wordt, en wat er nodig is om te beslissen welk alternatief het juiste is.

Die rechtvaardiging gaat in elk geval niet op ieder terrein op. Een bekend gebied waarvoor het betwijfeld is, is de wiskunde. Neem het Vermoeden van Goldbach: elk even getal groter dan 2 is te schrijven als $p + q$, met p en q priem. Wie weet wat er nodig is om te beslissen of het waar is of niet, gaat heel beroemd worden.

Of de Wet van de Uitgesloten Derde geldt voor de wiskunde, kunnen we af laten hangen van de aard van de in dat vak bestudeerde werkelijkheid. Is die eeuwig en onveranderlijk, en, vooral, bestaat ze onafhankelijk van wie haar onderzoekt — een opvatting toegeschreven aan Plato[6] — dan pleit dat voor de Wet, al was het maar omdat de goden weten wat Goldbach's Vermoeden betekent en hoe je beslist of het waar is. Is die daarentegen een product van de menselijke beschaving, of, zoals Brouwer[7] dacht, van de creativiteit van de individuele wiskundige, dan hangt het er maar van af hoe de wiskunde zich ontwikkelt. Heyting[8] ontwikkelde een vorm van logica die binnen de grenzen blijft van Brouwer's *intuïtionistische* wiskunde. Daarin is de Wet van de Uitgesloten Derde niet geldig.

Het natuurlijke deductie-systeem *zonder* Reductio, maar *met* Ex Falso, belichaamt Heyting's intuïtionistische propositielogica. Men kan overigens ook bezwaar maken tegen de *ex falso*-regel. Het systeem zonder enige $\perp$-eliminatieregel heet de *positieve* of *minimale* logica.

Oefeningen

6:2 Gebruik *reductio ad absurdum* om te laten zien dat

(i) $\vdash \neg\neg p \to p$

(ii) $\neg(p \wedge q) \vdash \neg p \vee \neg q$

(iii) $\neg p \to q \vdash p \vee q$

(iv) $\vdash (\neg p \to \neg q) \to q \to p$

6:3 (Wet van Peirce). Gebruik zowel *reductio ad absurdum* als *ex falso* om te laten zien dat $\vdash ((p \to q) \to p) \to p$.

6:4 (Intuïtionistische afleidbaarheid). We schrijven

[5] Van 2003 sloot het Rijksmuseum voor renovatie. De verbouwing zou in 2008 klaar zijn, maar het werd uiteindelijk 2013.

[6] Grieks wijsgeer, 427-347 v.C., leerling van Socrates; stichtte een school te Athene, de Academie.

[7] L.E.J Brouwer: Nederlands wiskundige (1881-1966), hoogleraar aan de Universiteit van Amsterdam.

[8] A. Heyting: Nederlands wiskundige (1898-1980), leerling van Brouwer, hoogleraar aan de Universiteit van Amsterdam.

$$\varphi_1,\ldots,\varphi_n \vdash_{\mathrm{I}} \psi$$

wanneer ψ afleidbaar is uit $\varphi_1,\ldots,\varphi_n$ in het 'intuïtionistische' deductiesysteem, zonder *reductio*, maar met *ex falso*. Laat zien dat

(i) $\vdash_{\mathrm{I}} \neg\neg\neg p \to \neg p$

(ii) $p \vee \neg p \vdash_{\mathrm{I}} ((p \to q) \to p) \to p$

(iii) $\vdash_{\mathrm{I}} \neg\neg(p \to q) \leftrightarrow (\neg\neg p \to \neg\neg q)$

6.5 Afgeleide regels. De connectieven $\neg$, $\top$ en $\leftrightarrow$ vatten we op als gedefinieerd — respectievelijk door $\neg\varphi = \varphi \to \bot$, $\top = \bot \to \bot$ en

$$\varphi \leftrightarrow \psi = (\varphi \to \psi) \wedge (\psi \to \varphi).$$

We kunnen de regels uit 6.2 gebruiken om introductie- en eliminatieregels af te leiden voor de gedefinieerde connectieven.

Voor de negatie zijn de $\bot$-regels voldoende. Uit de vorige subparagraaf weten we dat je *ex falso sequitur quodlibet* mag gebruiken als je beschikt over *reductio ad absurdum*; je kunt *ex falso* in dat geval beschouwen als een afkorting voor een deelbewijs volgens een vast patroon.

$\top$ bevat geen informatie, en heeft dus geen eliminatieregel; de introductieregel is

$$\begin{array}{ll} \vdots & \\ n.\ \top & \qquad\qquad (\top\text{-introductie}) \end{array}$$

Met andere woorden: $\top$ mag altijd geconcludeerd worden. De afleiding waar dat uit blijkt is

$$\begin{array}{ll} \lceil\ 1.\ \bot & \qquad\qquad \text{(aanname)} \\ \hline 2.\ \bot \to \bot & \end{array}$$

De introductieregel voor $\leftrightarrow$ volgt uit de regel voor $\wedge$ en de definitie:

$$(\text{intro} \leftrightarrow) \qquad \frac{\varphi \to \psi \qquad \psi \to \varphi}{\varphi \leftrightarrow \psi}$$

Een handige eliminatieregel is:

$$\frac{\varphi \leftrightarrow \psi \quad \psi}{\varphi}\ (\text{elim.} \leftrightarrow \text{(links)}) \qquad \frac{\varphi \leftrightarrow \psi \quad \varphi}{\psi}\ (\text{elim.} \leftrightarrow \text{(rechts)})$$

Oefeningen

6:5 Bewijs (met inductie naar n) dat (i), (ii) en (iii) equivalent zijn:

(i) $\varphi_1,\ldots,\varphi_n \vdash \psi$

(ii) $\vdash \varphi_1 \wedge\ldots\wedge \varphi_n \to \psi$

(iii) $\vdash \varphi_1 \to\ldots\to \varphi_n \to \psi$

6:6 Bewijs de geldige conclusies van het Busvertragingsprobleem (4:5) met natuurlijke deductie.

6.6 Correctheid en Volledigheid

Een afleiding verdeelt een gevolgtrekking in begrijpelijke stappen — althans, dat zouden we willen. De vraag of een afleidingssysteem in dit opzicht geslaagd is, heeft twee kanten:

a) Belichaamt elke afleiding een geldige gevolgtrekking? Zo ja, dan noemen we het afleidingssysteem *correct*.

b) Bestaat er bij elke geldige gevolgtrekking een afleiding van de conclusie uit de premissen? Zo ja, dan noemen we het afleidingssysteem *volledig*.

De verschillende falsumregels in #4 corresponderen met verschillende gevolgtrekkingsbegrippen. Slechts één daarvan, het *klassieke*, is in het voorafgaande (in §4) precies gedefinieerd. Voor dat begrip zullen we hieronder het correctheids- en het volledigheidsprobleem bespreken.

Definitie 4.2 laat gevolgtrekkingen met oneindig veel premissen toe. Het corresponderende afleidingsbegrip lijkt zwakker:

6.6.1 Definitie. Laat $\Phi \cup \{\psi\}$ een verzameling formules zijn. We schrijven

$$\Phi \vdash \psi$$

als er een afleiding van ψ bestaat uit aannamen in Φ.

Die afleiding is natuurlijk maar eindig, dus als $\Phi \vdash \psi$, dan is er een eindige verzameling $\Phi_0 \subseteq \Phi$ zo dat $\Phi_0 \vdash \psi$.

Het volgende lemma formuleert de rechtvaardiging van de deductieregels in termen van de klassieke semantiek.

6.6.2 Lemma. Laat Φ en Ψ verzamelingen formules zijn, en ψ, χ formules.
(a) $\Phi \models \psi$ als $\psi \in \Phi$.
(b) Als $\Phi \models \psi$ voor alle $\psi \in \Psi$, en $\Psi \models \chi$, dan $\Phi \models \chi$.
(c) $\Phi \models \psi \wedge \chi$ dan en slechts dan als $\Phi \models \psi$ en $\Phi \models \chi$.
(d) $\Phi \models \chi \to \psi$ dan en slechts dan als $\Phi \cup \{\chi\} \models \psi$.
(e) $\Phi \models \psi \vee \chi$ als $\Phi \models \psi$ of $\Phi \models \chi$.

Bewijs. (a) Als $V(\varphi) = 1$ voor alle $\varphi \in \Phi$, en $\psi \in \Phi$, dan zeker $V(\varphi) = 1$.
(b) Laat V een model zijn van Φ. Dan is V ook een model van Ψ; dus $V(\chi) = 1$.
$\boxtimes$

6:7 Oefening. Bewijs (c)-(e). (Vergelijk met 4:1.)

6.6.3 Correctheidsstelling. Laat $\Phi \cup \{\psi\}$ een verzameling formules zijn. Als $\Phi \vdash \psi$, dan $\Phi \models \psi$.

Bewijs. Met inductie naar de lengte k van een gegeven afleiding van ψ. We nemen aan dat, voor willekeurige formuleverzameling Γ, $\Gamma \models \chi$ voor elke formule χ die een afleiding heeft van lengte kleiner dan k uit aannamen in Γ.

Als ψ een aanname is, dan $\psi \in \Phi$. Dan $\Phi \models \psi$ volgens onderdeel (a) van het lemma.

Als ψ in de afleiding herhaald wordt, dan is er een afleiding van ψ van lengte minder dan k. Dan $\Phi \models \psi$ volgens inductieveronderstelling.

Als ψ is afgeleid uit ψ_1 en ψ_2 met de conjunctie-introductieregel, dan $\psi = \psi_1 \wedge \psi_2$, en $\Phi \models \psi_1$ en $\Phi \models \psi_2$ volgens inductieveronderstelling. Dus $\Phi \models \psi$ volgens onderdeel (c) van het lemma.

Als ψ is afgeleid uit $\psi \wedge \chi$ met linkse conjunctie-eliminatie, dan $\Phi \models \psi \wedge \chi$ volgens inductieveronderstelling. Dus $\Phi \models \psi$ volgens onderdeel (c) van het lemma. De redenering bij rechtse conjunctie-eliminatie is bijna hetzelfde.

Als ψ is afgeleid uit χ en $\chi \to \psi$ met implicatie-eliminatie, dan $\Phi \models \chi$ en $\Phi \models \chi \to \psi$ volgens inductieveronderstelling. Dus $\Phi \cup \{\chi\} \models \psi$ volgens onderdeel (d) van het lemma. Dus $\Phi \models \psi$ volgens onderdeel (b).

Als ψ is afgeleid met de implicatie-introductieregel, dan is ψ van de vorm $\psi_1 \to \psi_2$, en is er een afleiding van ψ_2 uit aannamen in $\Phi \cup \{\psi_1\}$ van lengte kleiner dan k. Dan $\Phi \cup \{\psi_1\} \models \psi_2$ volgens inductieveronderstelling. Dus $\Phi \models \psi$ volgens onderdeel (d) van het lemma.

Als ψ is afgeleid uit met de linkse disjunctie-introductieregel, dan $\psi = \psi_1 \vee \psi_2$, en $\Phi \models \psi_1$ volgens inductieveronderstelling. Dus $\Phi \models \psi$ volgens onderdeel (e) van het lemma. De redenering bij rechtse disjunctie-introductie is bijna hetzelfde.

Als ψ is afgeleid uit met de disjunctie-eliminatieregel, dan zijn er kortere afleidingen uit aannamen in Φ van formules $\chi_1 \vee \chi_2$, $\chi_1 \to \psi$ en $\chi_2 \to \psi$. Dus $\Phi \models \chi_1 \vee \chi_2$, $\Phi \models \chi_1 \to \psi$, en $\Phi \models \chi_2 \to \psi$, volgens inductieveronderstelling. Maar

$$\chi_1 \vee \chi_2, \chi_1 \to \psi, \chi_2 \to \psi \models \psi;$$

dus $\Phi \models \psi$ volgens (b).

Als ψ is afgeleid met reductio ad absurdum, dan is er een afleiding van $\perp$ van lengte $k - 1$, uit aannamen in $\Phi \cup \{\neg\psi\}$. Dus $\Phi \cup \{\neg\psi\} \models \perp$ volgens inductieveronderstelling. Laat V nu een model zijn van Φ. Dan $V(\neg\psi) \neq 1$, want anders moest $V(\perp) = 1$ zijn. Dus $V(\neg\psi) = 0$, en $V(\psi) = 1$. Dus $\Phi \models \psi$. ⊠

Nu willen we het omgekeerde bewijzen. Dat is weznlijk moeilijker. De bewering $\Phi \vdash \psi$ behelst het bestaan van een tamelijk nauw omschreven object. *Een* afleiding, al hebben we geen idee welke, geeft genoeg informatie voor een direct bewijs. De bewering $\Phi \models \psi$ daarentegen betreft *alle* valuaties. Uit een gegeven valuatie, hoe algemeen ook omschreven, zouden we misschien nog een afleiding kunnen construeren, maar zo zijn we kansloos. We hebben een nieuw idee nodig, voor een indirect bewijs.

6.6.4 Definitie. Een verzameling Φ van formules is *consistent* als $\Phi \nvdash \perp$.

In het tegengestelde geval, dat $\Phi \vdash \perp$, heet Φ *inconsistent*.

De semantische portée van consistentie is:

6.6.5 Vervulbaarheidsstelling. Elke consistente verzameling formules is vervulbaar.

Stel nu dat $\Phi \nvdash \psi$. Dan is $\Phi \cup \{\neg\psi\}$ consistent. Anders was er namelijk een afleiding van $\perp$ uit aannamen $\varphi_0, \ldots, \varphi_{n-1} \in \Phi$ en $\neg\psi$. De volgorde van niet-ingetrokken aannamen is irrelevant (en of ze echt nodig zijn, doet er ook al niet toe): we mogen dus aannemen dat $\neg\psi$ de laatste niet-ingetrokken aanname is in de afleiding van $\perp$. Dan kunnen we nog één stap verder gaan, en $\neg\psi$ intrekken door ψ te concluderen met *Reductio ad Absurdum*; en dan hebben we een bewijs van ψ uit aannamen in Φ, in tegenspraak met onze veronderstelling. De Vervulbaarheidsstelling zegt nu dat $\Phi \cup \{\neg\psi\}$ vervulbaar is; en dat impliceert meteen dat $\Phi \not\models \psi$. Met contrapositie concluderen we:

6.6.6 Volledigheidsstelling. Laat $\Phi \cup \{\psi\}$ een verzameling formules zijn. Als $\Phi \models \psi$, dan $\Phi \vdash \psi$.

Inconsistentie is een locaal verschijnsel, in de zin dat, als een oneindige verzameling Φ inconsistent is, er een eindige deelverzameling van Φ bestaat (de openblijvende aannamen in een afleiding van $\perp$) waar dat aan ligt. De contrapositie van de Vervulbaarheidsstelling is

elke onvervulbare verzameling formules is inconsistent;

kennelijk is onvervulbaarheid ook een locale eigenschap. De gebruikelijke formulering is omgekeerd:

6.6.7 Definitie. Een verzameling Φ van formules is *eindig vervulbaar* als elke eindige deelverzameling van Φ vervulbaar is.

6.6.8 Compactheidsstelling. Elke eindig vervulbare verzameling formules is vervulbaar.

Bewijs. Stel dat Φ eindig vervulbaar is. Dan is Φ consistent; anders waren er namelijk $n \in \mathbb{N}$ en $\varphi_0, \ldots, \varphi_{n-1} \in \Phi$ zo dat $\varphi_0, \ldots, \varphi_{n-1} \vdash \perp$; volgens de Correctheidsstelling geldt dan ook $\varphi_0, \ldots, \varphi_{n-1} \models \perp$, dus $\{\varphi_0, \ldots, \varphi_{n-1}\}$ is niet vervulbaar, in tegenspraak met de eindige vervulbaarheid van Φ. Volgens de Vervulbaarheidsstelling is Φ dus vervulbaar. ⊠

Rest nog het bewijs van de Vervulbaarheidsstelling. Laat Φ een consistente verzameling formules zijn. We moeten een model V van Φ construeren. Zo'n model bepaalt een 'theorie' $\mathrm{Th}(V) :=$

$$\{\psi \in \mathrm{F}\textsc{p}[\wedge, \vee, \to, \perp] \mid V \models \psi\},$$

en andersom; het is dus genoeg een verzameling $\Psi \supseteq \Phi$ te construeren die de theorie is van een valuatie. Eén van de bijzondere eigenschappen van zulke theorieën is dat je er niets aan kunt toevoegen.

6.6.9 Propositie. Als $\chi \notin \mathrm{Th}(V)$, dan is $\mathrm{Th}(V) \cup \{\chi\}$ niet consistent.

Bewijs. Als $V \not\models \chi$, dan $\neg\chi \in \mathrm{Th}(V)$, en $\{\chi, \neg\chi\} \vdash \perp$. ⊠

6.6.10 Definitie. Een consistente verzameling Γ van formules is *maximaal* consistent als elke echte uitbreiding van Γ inconsistent is.

Een maximaal consistente verzameling is gesloten onder afleidbaarheid:

6.6.11 Propositie. Als Γ maximaal consistent is, en $\Gamma \vdash \varphi$, dan $\varphi \in \Gamma$.

Bewijs. Stel dat φ afleidbaar is uit de maximaal consistente verzameling Γ. Dan is $\Gamma \cup \{\varphi\}$ consistent, want als er een afleiding is van $\perp$ uit φ en aannamen in Γ, dan kunnen we die combineren met een afleiding van φ uit aannamen in Γ; de gecombineerde afleiding zou aantonen dat Γ inconsistent is. Wegens maximaliteit moet gelden dat $\Gamma \cup \{\varphi\} = \Gamma$. ⊠

6.6.12 Lemma. Elke consistente verzameling heeft een maximaal consistente uitbreiding.

Bewijs. Zij een consistente verzameling Γ gegeven. Laat

$$\psi_0, \psi_1, \psi_2, \psi_3, \ldots$$

een opsomming zijn van alle formules. (Zie Appendix A voor een beschrijving van zo'n opsomming.) We definiëren nu een keten

$$\Gamma_0 \subseteq \Gamma_1 \subseteq \Gamma_2 \subseteq \Gamma_3 \subseteq \ldots$$

van consistente verzamelingen als volgt. $\Gamma_0 = \Gamma$. Stel Γ_n is geconstrueerd. Dan definiëren we:

$$\Gamma_{n+1} := \begin{cases} \Gamma_n \cup \{\psi_n\} \text{ als dat consistent is,} \\ \Gamma_n \text{ anders.} \end{cases}$$

Tenslotte nemen we de limiet: $\Gamma_\infty = \bigcup_{n=0}^{\infty} \Gamma_n$.

Γ_∞ is de gezochte maximaal consistente verzameling, want:
1° Γ_∞ is consistent. Als $\perp$ afleidbaar is uit zekere $\gamma_0, \ldots, \gamma_{m-1} \in \Gamma_\infty$, dan moet er een stadium Γ_n zijn dat $\gamma_0, \ldots, \gamma_{m-1}$ bevat. Maar ieder stadium Γ_n is consistent.
2° Γ_∞ is *maximaal* consistent. Want als $\psi_n \notin \Gamma_\infty$, dan $\psi_n \notin \Gamma_{n+1}$, en volgens constructie is $\Gamma_n \cup \{\psi_n\}$ dan inconsistent; dus is $\Gamma_\infty \cup \{\psi_n\}$ ook inconsistent. ☒

Laat Φ_∞ een maximaal consistente uitbreiding zijn van de gegeven consistente verzameling Φ. Definieer een bedeling V_∞ als volgt:

$$V_\infty(p_i) = \begin{cases} 1 \text{ als } p_i \in \Phi_\infty, \\ 0 \text{ anders.} \end{cases}$$

Formules φ en ψ heten *bewijsbaar equivalent* als $\vdash \varphi \leftrightarrow \psi$. Het is gemakkelijk in te zien dat twee bewijsbaar equivalente formules of allebei wèl, of allebei niet tot Φ_∞ behoren.

6.6.13 Lemma. $\mathrm{Th}(V_\infty) = \Phi_\infty$.

Bewijs. We tonen aan, met inductie naar de complexiteit van de formule φ:

(*) $\quad V_\infty \models \varphi$ dan en slechts dan als $\varphi \in \Phi_\infty$.

We mogen aannemen dat in φ geen andere connectieven voorkomen dan $\rightarrow$ en $\perp$; elke formule is immers, logisch en bewijsbaar, equivalent met een formule in $\mathrm{F}\textsc{p}[\rightarrow, \perp]$.

Als φ een propositieletter is, geldt (*) per definitie van V_∞. Als $\varphi = \perp$, dan $V_\infty \not\models \varphi$ en $\varphi \notin \Phi_\infty$.

Stel nu dat $\varphi = \varphi_1 \rightarrow \varphi_2$.
Als $V_\infty \models \varphi$ dan $V_\infty \not\models \varphi_1$ of $V_\infty \models \varphi_2$. In het eerste geval zegt de inductiehypothese dat $\varphi_1 \notin \Phi_\infty$, dus, wegens maximale consistentie, $\Phi_\infty \cup \{\varphi_1\} \vdash \perp$. Dan zeker $\Phi_\infty \cup \{\varphi_1\} \vdash \varphi_2$, dus $\Phi_\infty \vdash \varphi$, dus $\varphi \in \Phi_\infty$ volgens Propositie 11. In het tweede geval $\varphi_2 \in \Phi_\infty$, waardoor evengoed $\Phi_\infty \vdash \varphi$.
Als $V_\infty \not\models \varphi$ dan $V_\infty \models \varphi_1$ en $V_\infty \not\models \varphi_2$. Dan volgens inductiehypothese $\varphi_1 \in \Phi_\infty$ en $\varphi_2 \notin \Phi_\infty$. Maar $\varphi_1, \varphi \vdash \varphi_2$, dus $\varphi \notin \Phi_\infty$. ☒

Omdat $\Phi \subseteq \Phi_\infty$, is V_∞ zeker een model van Φ; dus Φ is vervulbaar.

Verdere Oefeningen

6:8 Laat C een willekeurige verzameling connectieven zijn. Een vervulbare verzameling $\Phi \subseteq \mathrm{F}\textsc{p}[C]$ is *maximaal vervulbaar* als voor elke $\psi \in \mathrm{F}\textsc{p}[C] - \Phi$, $\Phi \cup \{\psi\}$ niet vervulbaar is. Bewijs: als Φ en Ψ maximaal vervulbare deelverzamelingen zijn van $\mathrm{F}\textsc{p}[C]$ die dezelfde propositieletters bevatten (i.e. voor alle i, $p_i \in \Phi$ dan en slechts dan als $p_i \in \Psi$), dan $\Phi = \Psi$.

6:9 (Bewijsbare equivalenties). Bewijs (cf. 6:2):
(a) $\vdash \varphi \wedge \psi \leftrightarrow \neg(\varphi \rightarrow \neg\psi)$;

(b) $\vdash \varphi \vee \psi \leftrightarrow (\neg\varphi \to \psi)$.

Deel II. Termlogica

De propositielogica speelt in veel wiskundige redeneringen een rol, maar is op zichzelf niet voldoende om zelfs maar één interessant wiskundig bewijs te formaliseren. We bespreken nu een ander deelaspect, de logica van *vergelijkingen*, of, zoals we het bij voorkeur zullen noemen, de *termlogica*. We zullen die verderop nog combineren met de propositielogica, en uitbreiden; maar ze is ook in zoverre al een stap vooruit dat ze echte wiskundige redeneringen, of tenminste *berekeningen*, bestrijkt.

§7 Algebra's

In deel I hebben we waarheidsfuncties besproken, operaties op de verzameling der waarheidswaarden. Eerst waren dat vaste operaties, corresponderend met een aantal voegwoorden uit de gewone taal; in §5 beschouwden we waarheidsfuncties en de bijbehorende connectieven in het algemeen. Het ligt nu eigenlijk nogal voor de hand om ook de onderliggende verzameling te variëren. Uit een gegeven repertoire van operatiesymbolen kunnen we 'termen' construeren, analoog aan de formules uit een collectie C van connectieven.

7.1 Een *operationeel vocabulaire*, of *operationeel type*, is een verzameling $\mathcal{F}$ van operatiesymbolen. Wat de symbolen *zijn*, is niet belangrijk, net als in §2.1. We moeten ze uit elkaar kunnen houden, en we moeten altijd de *plaatsigheid* kennen, dat is, op hoeveel argumenten de bijbehorende operatie werkt, of in syntactische termen, met hoeveel termen je het symbool moet combineren om een betekenisvolle uitdrukking te krijgen. In het algemeen schrijven we operatiesymbolen vóór hun argumenten, zoals in §5.7, maar in concrete gevallen geven we dikwijls toe aan sentimentele redenen om een symbool ergens tussenin te schrijven.

7.2 Voorbeelden
(i) Het vocabulaire van de propositielogica zoals we dat in §1.3 hebben ingevoerd is $\mathcal{Prop} = \{\neg, \wedge, \vee, +, \rightarrow, \leftrightarrow\}$. Het symbool $\neg$ is éénplaatsig en wordt vóór zijn argument geschreven (men spreekt van *præfix*-notatie), de andere zijn tweeplaatsig en worden tussen hun argumenten geschreven (in *infix*-notatie). In §1.4 hebben we $\mathcal{Prop}$ uitgebreid met twee nulplaatsige operatiesymbolen, $\bot$ en $\top$. Een nulplaatsige operatie heet ook wel een *constante*.
(ii) We zagen in §5 dat $\mathcal{Prop}$ ruim bemeten is voor het doel om waarheidsfuncties te noteren. Zelfs $\mathcal{If} := \{\rightarrow, \bot\}$, het vocabulaire van de *implicatie-falsum-algebra's*, is al functioneel volledig, met inbegrip van de nulplaatsige waarheidsfuncties.
(iii) Een ander belangrijk functioneel volledig stelsel is $\mathcal{Bool} =$

$$\{\neg, \wedge, \vee, \bot, \top\},$$

het vocabulaire van de *Boole-algebra's*[9]. In de Boole-algebra schrijft men altijd 0 en 1 in plaats van $\bot$ en $\top$, en wij zullen ons daarbij aansluiten.

[9] Naar George Boole (1815-1864), de eerste die algebraïsche methoden gebruikte in de logica en wiens werk niet, zoals dat van G.W. Leibniz (1646-1716), meteen zoekraakte.

(iv) Als vocabulaire voor *groepen* nemen we $\mathcal{G}roep = \{\cdot, ^{-1}, e\}$. De symbolen zijn respectievelijk twee-, één- en nulplaatsig. Het inversiesymbool $^{-1}$ wordt *achter* het argument geschreven (*postfix*). Er is ook een additief vocabulaire $\mathcal{A}b = \{+, -, 0\}$, dat voornamelijk wordt gebruikt voor abelse groepen.
(v)* Het vocabulaire $\mathcal{R}ing$ van de ringen is $\{+. \cdot, -, 0\}$. Door een constantesymbool 1 toe te voegen, krijgen we $\mathcal{R}ing1$, het type van de ringen met multiplicatief eenheidselement.
(vi) Het vocabulaire $\mathcal{N}at$ van de natuurlijke getallen is $\{+. \cdot, S, 0\}$. Het symbool S is éénplaatsig.

7.3 De symbolen in $\mathcal{P}rop$ krijgen betekenis doordat we ze associëren met operaties op de verzameling der waarheidswaarden. In het algemeen is een *algebra van type* $\mathcal{F}$ een paar $\mathbf{A} = \langle A, I\rangle$ bestaande uit een niet-lege verzameling A, het *universum* van $\mathbf{A}$, en een *interpretatie* I die aan ieder symbool $F \in \mathcal{F}$ een operatie op A toekent van de juiste plaatsigheid. Behalve als $I(F)$ zullen we die operatie ook noteren als $F^{\mathbf{A}}$.

7.4 Voorbeelden
(ia) De twee waarheidswaarden, met de interpretatie van de connectieven als de waarheidsfuncties gedefinieerd door de tabellen van §1.3, vormen een algebra $\mathbf{W} = \langle W, I\rangle$ van type $\mathcal{P}rop$. Als we W en I uitschrijven, krijgen we

(7.1) $$\langle\{0,1\}, \{\langle\neg,\neg\rangle, \langle\wedge,\wedge\rangle, \langle\vee,\vee\rangle, \langle+,+\rangle, \langle\rightarrow,\rightarrow\rangle, \langle\leftrightarrow,\leftrightarrow\rangle\}\rangle,$$

waarin bijvoorbeeld het eerst opgesomde paar in de tweede component betekent: 'de operatie $\neg$, gedefinieerd in tabel (1.3.1), wordt benoemd door het symbool $\neg$'. Dat zou informatief geweest zijn als we, om verwarring te voorkomen, het symbool een andere naam gegeven hadden dan de operatie. Men geeft er echter vaak de voorkeur aan die verschillende dingen, omdat ze toch echt bij elkaar horen, met hetzelfde symbool aan te duiden. Dan kan de omschrijving van I korter: $\mathbf{W}$ =

(7.2) $$\langle\{0,1\}, \neg, \wedge, \vee, +, \rightarrow, \leftrightarrow\rangle,$$

suggererend dat de betekenis van de symbolen duidelijk moet zijn. De verkorte notatie van (7.2) kan trouwens ook gebruikt worden wanneer de operaties niet per se met hetzelfde teken worden aangeduid als de symbolen, als we gebruik maken van de volgorde waarin de symbolen in het type zijn opgesomd. In

(7.3) $$\langle\{\mathbf{f}, \mathbf{u}, \mathbf{t}\}, \sim, \&, \mathbf{v}, \rightarrowtail\!\!\!\leftarrow, \Rightarrow, \Leftrightarrow\rangle$$

is $\sim$ dan bijvoorbeeld de interpretatie van $\neg$.
(ib) In Voorbeeld 2.3 wordt een algebra van formules beschreven:

(7.4) $$\mathbf{F\scriptstyle P} = \langle \mathrm{F\scriptstyle P}, F_\neg, F_\wedge, F_\vee, F_+, F_\rightarrow, F_\leftrightarrow, \top, \bot\rangle.$$

Dit is een bijzonder soort algebra. Er is een uitgangsverzameling, PROP, van structuurloze, onderling verwisselbare elementen; en alle andere elementen kun je daaruit construeren door herhaaldelijk operaties uit het rijtje $F_\neg$, $F_\wedge$, $F_\vee$, F_+, $F_\rightarrow$, $F_\leftrightarrow$, $\top$, $\bot$ toe te passen. De unieke leesbaarheidsstelling 2.9 zegt dat je ieder element van FP daarbij maar één keer tegenkomt, in de zin dat als G en H operaties zijn in de opsomming van (7.4), respectievelijk n- en m-plaatsig, dus

$n, m \in \{0, 1, 2\}$, dan $G(\varphi_1,\ldots, \varphi_n) \neq p_i$, en $G(\varphi_1,\ldots, \varphi_n) = H(\psi_1,\ldots, \psi_m)$ impliceert dat $n = m$, $G = H$, en $\varphi_j = \psi_j$ voor $j = 1,\ldots, n$.
(iia) Laat $G = F_{\rightarrow} \upharpoonright \mathrm{FP}[\rightarrow, \bot]$. Dan is

$$\mathbf{FP}[\rightarrow, \bot] = \langle \mathrm{FP}[\rightarrow, \bot], G, \bot\rangle. \tag{7.5}$$

een formule-algebra van type $\mathcal{I}f$; een zuinige variant op **FP**.
(iib) Laat n een positief geheel getal zijn, en $M_n = \{0,\ldots, n-1\}$ de verzameling van de eerste n natuurlijke getallen. We definiëren een n-waardige logica $\mathbf{M}_n = \langle M_n, \rightarrow, 0\rangle$ door

$$m \rightarrow k = \begin{cases} k \text{ als } k < m, \\ n-1 \text{ als } k \geq m. \end{cases}$$

Als we weer $x \rightarrow 0$ opvatten als de ontkenning van x, dan is 0 de ontkenning van elke waarheidswaarde behalve 0, en $n-1$ de ontkenning van 0.
(iic) Een verwante logica, waarin de waarheidswaarden echter niet simpelweg lineair geordend zijn, is $\mathbf{M}_n \times \mathbf{M}_n = \langle M_n \times M_n, \rightarrow, \langle 0, 0\rangle\rangle$, waarin

$$\langle m_1, m_2\rangle \rightarrow \langle k_1, k_2\rangle = \langle m_1 \rightarrow k_1, m_2 \rightarrow k_2\rangle.$$

(iiia) De waarheidswaarden-algebra $\mathbf{2} = \langle\{0, 1\}, \neg, \wedge, \vee, 1, 0\rangle$ is de belangrijkste Boole-algebra.
(iiib) Laat X een verzameling zijn, en voor $Y \subseteq X$, $\overline{Y} = X \setminus Y$. De *machtsverzamelingsalgebra over* X is $\boldsymbol{\mathcal{P}X} = \langle \mathcal{P}X, \overline{}, \cap, \cup, X, \emptyset\rangle$. (Met $\cap$ en $\cup$ bedoelen we hier de doorsnede- en de verenigingsoperatie *voor elementen van het universum* $\mathcal{P}X$; we zullen er vaak van uitgaan dat zoiets vanzelf spreekt.)
(iv) Laat X een verzameling zijn, en S_X de verzameling van alle bijecties van X op X. Dan is $\mathbf{S}_X = \langle S_X, \circ, ^{-1}, 1_X\rangle$, waarin $\circ$ de gebruikelijke betekenis heeft van *functiecompositie*, $^{-1}$ staat voor *functie-inversie*, en 1_X de identieke functie is op X, de symmetrische groep op X. Een algebra van het additieve type is de (abelse) groep der gehele getallen in de voorstelling

$$\mathbf{Z} = \langle \mathbb{Z}, +, -, 0\rangle.$$

(v)* De gehele getallen vormen ook een *ring*, $\mathbf{Z} = \langle \mathbb{Z}, +, \cdot, -, 0\rangle$. Verder hebben we eindige ringen $\mathbf{Z}_n = \langle\{0,\ldots, n-1\}, +, \cdot, -, 0\rangle$, met operaties modulo n. De endomorfismen van een abelse groep **A** vormen een ring **End A** =

$$\langle \mathrm{End}\,\mathbf{A}, +, \circ, -, 0\rangle,$$

met $f + g$ gedefinieerd door $(f + g)(a) = f(a) + g(a)$, $(-f)(a) = -f(a)$, en $0(a) = 0^{\mathbf{A}}$. Met de superscripte **A** geven we aan dat de laatste 0 die van **A** is — al zou je ook kunnen vinden dat dat vanzelf spreekt.
(vi) De algebra der natuurlijke getallen is $\mathbf{N} = \langle \mathbb{N}, +, \cdot, S, 0\rangle$; $Sn = n + 1$, de opvolger (*successor*) van n.

7.5 We gaan nu een nieuwe logische taal definiëren, of, beter gezegd, een heel spectrum van talen. De formules van deze talen hebben de vorm

$$\mathbf{t}_1 \approx \mathbf{t}_2,$$

het zijn *vergelijkingen*, waarin we $\approx$ schrijven in plaats van $=$ om het onderscheid met echte beweringen te benadrukken. Met $\mathbf{t}_1$ en $\mathbf{t}_2$ worden *termen* aangeduid, en die zullen we nu eerst definiëren.

7.6 Termen zijn uitdrukkingen: rijtjes symbolen. Er zijn weer (net als in 2.1) drie groepen van symbolen in het spel:

— de *individuele variabelen*; oneindig veel, genummerd als $v_0, v_1, v_2, \dots$

— de *operatiesymbolen*. Welke dat zijn, hangt af van het *type* van de termen.

— haakjes:), (.

De haakjes zijn nodig als we operatiesymbolen infix willen schrijven. In het algemeen (in tegenstelling tot de concrete gevallen) gebruiken we Poolse notatie. Ook dan is de leesbaarheid soms gebaat met haakjes, en komma's.

7.7 Definitie. Zij $\mathcal{F}$ een operationeel vocabulaire. De *termen over* $\mathcal{F}$, of *van type* $\mathcal{F}$, zijn de elementen van de kleinste verzameling X van uitdrukkingen die
(i) alle individuele variabelen bevat; en waarvoor geldt
(ii) als $Q \in \mathcal{F}$ een n-plaatsig operatiesymbool is, en $\mathbf{t}_1, \dots, \mathbf{t}_n$ behoren tot X, dan ook $Q\mathbf{t}_1 \dots \mathbf{t}_n \in X$.

We duiden de termverzameling aan met $T_{\mathcal{F}}(\mathrm{Var})$. 'Var' staat hier voor de verzameling van alle variabelen; in het algemeen kunnen we $T_{\mathcal{F}}(W)$ schrijven voor de verzameling der termen die alleen variabelen uit $W \subseteq \mathrm{Var}$ bevatten.

7.8 Postulaat. Hoe we ze ook noteren, we eisen dat de termen over $\mathcal{F}$ uniek leesbaar zijn. Dat veronderstelt een minimale subtiliteit bij de keuze van symbolen. We willen bijvoorbeeld niet dat Q een operatiesymbool is en Qv_0 ook.

7.9 Termalgebra's. De termen over een vocabulaire $\mathcal{F}$ vormen op natuurlijke wijze een algebra $\mathbf{T} = \mathbf{T}_{\mathcal{F}}(\mathrm{Var})$ van type $\mathcal{F}$. Het universum is $T_{\mathcal{F}}(\mathrm{Var})$, en een n-plaatsig symbool $Q \in \mathcal{F}$ wordt geïnterpreteerd als

$$Q^{\mathbf{T}}\colon \langle \mathbf{t}_1, \dots, \mathbf{t}_n \rangle \longmapsto Q\mathbf{t}_1 \dots \mathbf{t}_n\,.$$

Voorbeelden van termalgebra's zijn al gegeven in 7.4(ib), (iia).

We willen termen interpreteren in willekeurige algebra's van passend type. Dat gaat via een heel algemeen begrip.

7.10 Definitie. Laat $\mathbf{A}$ en $\mathbf{B}$ algebra's zijn van hetzelfde type $\mathcal{T}$. Een afbeelding $f\colon A \longrightarrow B$ is een *homomorfisme* van $\mathbf{A}$ naar $\mathbf{B}$ als voor ieder natuurlijk getal n, voor elk n-plaatsig operatiesymbool $Q \in \mathcal{T}$, voor alle $a_0, \dots, a_{n-1} \in A$,

$$f(Q^{\mathbf{A}}(a_0, \dots, a_{n-1})) = Q^{\mathbf{B}}(f(a_0), \dots, f(a_{n-1})).$$

We noteren $f\colon \mathbf{A} \longrightarrow \mathbf{B}$, voor '$f$ is een homomorfisme van $\mathbf{A}$ naar $\mathbf{B}$'. Een bijectief homomorfisme heet een *isomorfisme*. We schrijven $f\colon \mathbf{A} \cong \mathbf{B}$, voor '$f$ is een isomorfisme van $\mathbf{A}$ naar $\mathbf{B}$', en $\mathbf{A} \cong \mathbf{B}$, voor 'er bestaat een isomorfisme van $\mathbf{A}$ naar $\mathbf{B}$'.

7.11 Voorbeelden
(i), (ii)* Homomorfismen van groepen en ringen.
(iii) Volgens Stelling 3.3 bepaalt elke valuatie V een uniek homomorfisme V^*: $\mathbf{F}\mathrm{P} \longrightarrow \mathbf{W}$ dat V uitbreidt.

7.12 De interpretatie van termen is een generalisatie van voorbeeld (iii). Fixeer een type $\mathcal{T}$; laat $\mathbf{A}$ een algebra zijn van dat type. Een functie

$$\boldsymbol{a}\colon \mathrm{Var} \longrightarrow A$$

noemen we een *bedeling* in **A**.

Stelling. Elke bedeling in **A** heeft precies één uitbreiding die een homomorfisme is van $\mathbf{T}_{\mathcal{T}}(\mathrm{Var})$ naar **A**.

Bewijs. Laat $\boldsymbol{a}$: Var $\longrightarrow A$ een bedeling zijn. Definieer $\boldsymbol{a}^*$ op $T_{\mathcal{T}}(\mathrm{Var})$ door

$\boldsymbol{a}^*(\mathbf{t}) = \boldsymbol{a}(\mathbf{t})$ als $\mathbf{t} \in \mathrm{Var}$;

$\boldsymbol{a}^*(\mathbf{t}) = Q^{\mathbf{A}}(\boldsymbol{a}^*(\mathbf{t}_1),\ldots, \boldsymbol{a}^*(\mathbf{t}_n))$ als $\mathbf{t} = Q\mathbf{t}_1\ldots\mathbf{t}_n$.

Wegens unieke leesbaarheid is dit een correcte definitie. Bovendien is het de enige mogelijke definitie die overeenstemt met Definitie 10. ⊠

We zullen $\boldsymbol{a}^*(\mathbf{t})$ noteren als $\mathbf{t}^{\mathbf{A}}[\boldsymbol{a}]$, of ook, wanneer dat niet tot verwarring hoeft te leiden, $\mathbf{t}[\boldsymbol{a}]$. We blijven daarnaast de notatie $\boldsymbol{a}^*$ gebruiken voor het door een bedeling $\boldsymbol{a}$ bepaalde homomorfisme van de termalgebra.

7.13 Eindigheidslemma. Laat **t** een term zijn over type $\mathcal{F}$, **A** een algebra van type $\mathcal{F}$, en $\boldsymbol{a}$ en $\boldsymbol{b}$ bedelingen in **A** die aan alle variabelen die in **t** voorkomen dezelfde waarde toekennen. Dan $\mathbf{t}^{\mathbf{A}}[\boldsymbol{a}] = \mathbf{t}^{\mathbf{A}}[\boldsymbol{b}]$.

Bewijs. Met inductie naar de lengte van **t**. ⊠

Het eindigheidslemma rechtvaardigt een interpretatie van termen als finitaire operaties. Laat **t** een term zijn die geen andere variabelen bevat dan $x_0,\ldots, x_{k-1}$ — de volgorde is belangrijk, maar het hoeft niet de volgorde te zijn waarin ze in **t** voorkomen — en **A** een passende algebra, en $a_0,\ldots, a_{k-1} \in A$. Dan definiëren we $\mathbf{t}^{\mathbf{A}}[a_0,\ldots, a_{k-1}]$ als: $\mathbf{t}^{\mathbf{A}}[\boldsymbol{a}]$ voor elke (equivalent: een) bedeling $\boldsymbol{a}$ zo dat $\boldsymbol{a}(x_i) = a_i$ voor alle $i < k$. Zo bezien staat **t** voor een k-plaatsige *termoperatie* van **A**. (Dit generaliseert de notatie $\psi^{(n)}[\ldots]$ van §5.)

Oefeningen bij §7:

7:1 Laat X een verzameling zijn. De algebra $\mathbf{2}^X$ van type $\mathcal{Bool}$ is als volgt gedefinieerd. Het universum 2^X bestaat uit alle functies van X naar $\{0, 1\}$. Voor $f, g \in 2^X$ en voor alle $x \in X$, $(\neg f)(x) = 1 - f(x)$, $(f \wedge g)(x) = f(x) \cdot g(x)$, $(f \vee g)(x) = f(x) + g(x) - f(x) \cdot g(x)$, $1(x) = 1$, en $0(x) = 0$.

Beschrijf het verband tussen $\mathbf{2}^X$ en $\mathcal{P}X$.

7:2 Laat $\mathcal{F}$ een type zijn, $\mathcal{T} \subseteq \mathcal{F}$, en $\mathbf{A} = \langle A, I\rangle$ een algebra van type $\mathcal{F}$. Dan heet $\mathbf{A}\lceil\mathcal{T} := \langle A, I\lceil\mathcal{T}\rangle$ een *reduct* van **A**, en **A** een *expansie* van $\mathbf{A}\lceil\mathcal{T}$. Het is gemakkelijk te zien dat een homomorfisme f: $\mathbf{A} \longrightarrow \mathbf{B}$ van algebra's van type $\mathcal{F}$ ook een homomorfisme is van $\mathbf{A}\lceil\mathcal{T}$ naar $\mathbf{B}\lceil\mathcal{T}$. Het omgekeerde geldt alleen in bijzondere gevallen.

Laat $\mathbf{G} = \langle G, \cdot^{\mathbf{G}}, {}^{-1\mathbf{G}}, e^{\mathbf{G}}\rangle$ en $\mathbf{H} = \langle H, \cdot^{\mathbf{H}}, {}^{-1\mathbf{H}}, e^{\mathbf{H}}\rangle$ groepen zijn, en

$$f\colon \langle G, \cdot^{\mathbf{G}}\rangle \longrightarrow \langle H, \cdot^{\mathbf{H}}\rangle$$

een homomorfisme. Bewijs dat f een homomorfisme is van **G** naar **H**.

7:3 Bewijs het Eindigheidslemma 7.13.

7:4 Ga na dat de projectie π: $\langle k, m\rangle \longmapsto k$ een surjectief homomorfisme is van $\mathbf{M}_n \times \mathbf{M}_n$ naar $\mathbf{M}_n$.

7:5 Als er een surjectief homomorfisme van **A** naar (men zegt dan ook wel: *op*) **B** bestaat, dan heet **B** een *homomorf beeld* van **A**. Beschrijf alle homomorfe beelden van $\langle \mathbb{N}, +\rangle$ die precies drie elementen hebben.

7:6 De aard van de elementen van X draagt niets bij aan de wiskundig interessante eigenschappen van $\mathbf{S}_X$. Men noteert daarom ook $\mathbf{S}_k$, voor: 'één of andere $\mathbf{S}_X$ waarbij X precies k elementen bevat'.

Voor welke natuurlijke getallen k is $\mathbf{S}_k$ abels?

§8 Vergelijkingen

Laat $\mathcal{T}$ een operationeel type zijn. Een *vergelijking* over $\mathcal{T}$ is een paar

$$\langle \mathbf{t}_1, \mathbf{t}_2 \rangle$$

van termen over $\mathcal{T}$. Om sentimentele redenen noteren we meestal

$$\mathbf{t}_1 \approx \mathbf{t}_2.$$

8.1 Definitie (satisfactie). Laat $\mathbf{t}_1, \mathbf{t}_2$ termen zijn over een operationeel vocabulaire $\mathcal{T}$, en $\mathbf{A}$ een algebra van type $\mathcal{T}$.
(i) Een bedeling $\boldsymbol{a}$ in $\mathbf{A}$ *vervult* $\mathbf{t}_1 \approx \mathbf{t}_2$ in $\mathbf{A}$ als $\mathbf{t}_1^{\mathbf{A}}[\boldsymbol{a}] = \mathbf{t}_2^{\mathbf{A}}[\boldsymbol{a}]$. Notatie:

$$\mathbf{A} \models (\mathbf{t}_1 \approx \mathbf{t}_2)[\boldsymbol{a}].$$

(ii) Stel dat in $\mathbf{t}_1 \approx \mathbf{t}_2$ geen andere variabelen voorkomen dan $x_0, \ldots, x_{k-1}$. Een rijtje $\overline{a} \in A^k$ *vervult* $\mathbf{t}_1 \approx \mathbf{t}_2$ in $\mathbf{A}$ als $\mathbf{t}_1^{\mathbf{A}}[\overline{a}] = \mathbf{t}_2^{\mathbf{A}}[\overline{a}]$. Notatie:

$$\mathbf{A} \models (\mathbf{t}_1 \approx \mathbf{t}_2)[\overline{a}].$$

8.2 Voorbeelden
(i) Zij $\varphi = (p_0 \to p_1) \vee (\neg p_0 \to p_2) \to p_2$, als in Voorbeeld 3.5.2. Als we even afspreken dat p_i voor v_i staat, dan is φ een term van type $\mathcal{Prop}$. Definieer

$$\boldsymbol{w}(v_i) = \begin{cases} 1 \text{ als } i < 2, \\ 0 \text{ als } i \geq 2. \end{cases}$$

Dan blijkt uit de tabel in 3.5.2 dat $\mathbf{W} \models (\varphi \approx p_1 \wedge p_2)[\boldsymbol{w}]$. Onder vermijding van de omweg langs $\boldsymbol{w}$ kunnen we ook schrijven:

$$\mathbf{W} \models (\varphi \approx p_1 \wedge p_2)[1, 1, 0].$$

(ii)* Laat x, y en z verschillende variabelen zijn. De vergelijking

$$x + y \approx z$$

is vervulbaar in de ring $\mathbf{Z}$ der gehele getallen — elke bedeling $\boldsymbol{b}$ die $\boldsymbol{b}(x) + \boldsymbol{b}(y)$ toekent aan z voldoet. Ook

$$x \cdot x + y \cdot y \approx z \cdot z$$

is vervulbaar: $\langle 5, 12, 13 \rangle$ voldoet, bijvoorbeeld. (We nemen daarbij stilzwijgend aan dat $x = v_0$, $y = v_1$, en $z = v_2$. Dat scheelt omhaal. Verder gebruiken we de conventie dat $\cdot$ sterker bindt dan $+$.) Opmerkelijk is dat

$$x \cdot x \cdot x + y \cdot y \cdot y \approx z \cdot z \cdot z$$

(de plaatsing van haakjes in de derdemachten is aan de lezer) *niet* vervulbaar is.
(iii)* Laat x en y verschillende variabelen zijn. Er zijn bedelingen in de ring $\mathbf{Z}$ die 6 toekennen aan y en $x \cdot x - x - y \approx 0$ vervullen. (Notatie-conventie: $\mathbf{s} - \mathbf{t} = \mathbf{s} + (-\mathbf{t})$.) De vergelijking wordt onvervulbaar als je eist dat 1 wordt toegekend aan y. Als je toch een oplossing wilt vinden, moet je zoeken in een grotere ring, zoals $\mathbf{Q}[\sqrt{5}]$.

8.3 Definitie. Een vergelijking α is *geldig* in een algebra **A**, notatie

$$\mathbf{A} \models \alpha,$$

als $\mathbf{A} \models \alpha[\boldsymbol{a}]$ voor *elke* bedeling $\boldsymbol{a}$ in **A**.

We zeggen ook wel dat **A** *voldoet aan* α.

8.4 Voorbeelden

Vele belangrijke klassen van algebra's zijn gedefinieerd door vergelijkingen.

(i) Een *groep* is een algebra van type $\mathcal{G}roep$ waarin de vergelijkingen

$$\begin{aligned} ex &\approx x \,, \\ x^{-1}x &\approx e \,, \text{ en} \\ x(yz) &\approx (xy)z \qquad\qquad \text{(assocatieve wet)} \end{aligned}$$

geldig zijn. Een groep **A** is *commutatief* of *abels* als bovendien

$$\mathbf{A} \models xy \approx yx \,.$$

In additieve notatie schrijft men:

$$\begin{aligned} 0 + x &\approx x \,, \\ -x + x &\approx 0 \,, \\ x + (y + z) &\approx (x + y) + z \,, \\ x + y &\approx y + x. \end{aligned}$$

(ii)* Een *ring* is een algebra van type $\mathcal{R}ing$ waarvan het $\mathcal{A}b$-reduct een abelse groep is, en waarin naast de associatieve wet

$$x(yz) \approx (xy)z$$

de distributieve wetten

$$\begin{aligned} x \cdot (y + z) &\approx xy + xz \quad \text{en} \\ (x + y) \cdot z &\approx xz + yz \end{aligned}$$

geldig zijn. Een ring **R** is *commutatief* als bovendien

$$\mathbf{R} \models xy \approx yx \,.$$

Een ring met eenheidselement is van type $\mathcal{R}ing1$ en voldoet ook nog aan

$$1 \cdot x \approx x \quad \text{en} \quad x \cdot 1 \approx x.$$

(iii) Een *Boole-algebra* is een algebra van type $\mathcal{B}ool$ die voldoet aan

de assocatieve wetten

$$x \vee (y \vee z) \approx (x \vee y) \vee z \,, \qquad x \wedge (y \wedge z) \approx (x \wedge y) \wedge z \,;$$

de commutatieve wetten

$$x \vee y \approx y \vee x \,, \qquad x \wedge y \approx y \wedge x \,;$$

de idempotentiewetten

$$x \vee x \approx x \,, \qquad x \wedge x \approx x \,;$$

de distributieve wetten

$$x \vee (y \wedge z) \approx (x \vee y) \wedge (x \vee z), \qquad x \wedge (y \vee z) \approx (x \wedge y) \vee (x \wedge z);$$

de absorptiewetten

$$x \vee (x \wedge y) \approx x \,, \qquad x \wedge (x \vee y) \approx x \,;$$

de wetten van De Morgan

$$\neg(x \vee y) \approx \neg x \wedge \neg y\ , \qquad \neg(x \wedge y) \approx \neg x \vee \neg y\ ;$$

de 0-1-wetten

$$x \vee 0 \approx x\ , \qquad x \wedge 1 \approx x\ ;$$
$$x \vee 1 \approx 1\ , \qquad x \wedge 0 \approx 0\ ;$$
$$x \vee \neg x \approx 1\ , \qquad x \wedge \neg x \approx 0\ ;$$

en de dubbele negatie-wet $\qquad \neg\neg x \approx x\ .$

8.5 Definitie. Een *equationele theorie* bestaat uit een operationeel vocabulaire $\mathcal{F}$ en een verzameling vergelijkingen over $\mathcal{F}$.

We kunnen een equationele theorie dus beschrijven als een paar

$$\mathcal{E} = \langle \mathcal{F}, E \rangle$$

van een type $\mathcal{F}$ en een stelsel E van vergelijkingen over $\mathcal{F}$.

8.6 Voorbeelden. Voorbeeld 4 beschrijft een aantal equationele theorieën: de groepentheorie, de theorie der abelse groepen, de ringentheorie, de theorieën van de commutatieve ringen en de ringen met eenheidselement, en de theorie van de Boole-algebra's.

8.7 Substitutie

Laat $\mathcal{T}$ een operationeel type zijn. Een substitutie, zeg van $\mathbf{t}_1$ voor $x_1,\ldots,\ \mathbf{t}_k$ voor x_k, komt overeen met een bedeling $\boldsymbol{t}$ in $\mathbf{T}_{\mathcal{T}}(\mathrm{Var})$ die $\mathbf{t}_1$ toekent aan $x_1,\ldots,$ $\mathbf{t}_k$ aan x_k, en y aan elke variabele $y \notin \{x_1,\ldots, x_k\}$. Als we $\mathbf{T}_{\mathcal{T}}(\mathrm{Var})$ afkorten tot $\mathbf{T}$, dan hebben we

$$[\mathbf{t}_1/x_1,\ldots, \mathbf{t}_k/x_k]\mathbf{s} = \mathbf{s}^{\mathbf{T}}[\boldsymbol{t}] = \boldsymbol{t}^*(\mathbf{s}),$$

en, wanneer $\mathbf{s}$ geen andere variabelen bevat dan $x_1,\ldots, x_k$,

$$[\mathbf{t}_1/x_1,\ldots, \mathbf{t}_k/x_k]\mathbf{s} = \mathbf{s}^{\mathbf{T}}[\mathbf{t}_1,\ldots, \mathbf{t}_k].$$

— En vaak schrijft men, zoals eerder opgemerkt onder Definitie 5.7.1, als $\mathbf{t} = [\mathbf{t}_1/x_1,\ldots, \mathbf{t}_k/x_k]\mathbf{s}$, $\mathbf{s}$ als $\mathbf{s}(x_1,\ldots, x_k)$, en $\mathbf{t}$ als $\mathbf{s}(\mathbf{t}_1,\ldots, \mathbf{t}_k)$.

We zullen in het vervolg de substitutie $\mathbf{t}_1/x_1,\ldots, \mathbf{t}_k/x_k$ *identificeren met* de bedeling $\boldsymbol{t}$. We schrijven dus

$$[\mathbf{t}_1/x_1,\ldots, \mathbf{t}_k/x_k]\mathbf{s} = \mathbf{s}^{\mathbf{T}}[\mathbf{t}_1/x_1,\ldots, \mathbf{t}_k/x_k] = (\mathbf{t}_1/x_1,\ldots, \mathbf{t}_k/x_k)^*(\mathbf{s}),$$

en: $\sigma\mathbf{s} = \mathbf{s}^{\mathbf{T}}[\sigma] = \sigma^*(\mathbf{s})$.[10]

Substituties hebben een voor de hand liggende uitbreiding over vergelijkingen — als σ een substitutie is, en $\alpha = (\mathbf{s}_1 \approx \mathbf{s}_2)$, dan

$$\sigma\alpha = (\sigma\mathbf{s}_1 \approx \sigma\mathbf{s}_2).$$

Als $\beta = \sigma\alpha$ voor één of andere substitutie σ, dan heet β een *instantie van* α. Net als bij termen kunnen we α schrijven als $\alpha(x_1,\ldots, x_n)$, en $[\mathbf{t}_1/x_1,\ldots, \mathbf{t}_n/x_n]\alpha$ als $\alpha(\mathbf{t}_1,\ldots, \mathbf{t}_n)$.

De werking van herhaalde substituties wordt beschreven in de onderstaande generalisatie van Oefening 5:7.

[10] Selectie en plaatsing van haakjes zijn tot op zekere hoogte een kwestie van smaak.

Substitutielemma. Laat σ een substitutie zijn zo dat
(i) voor elke variabele $y \neq x$ die voorkomt in $\mathbf{t}$, x niet voorkomt in $\sigma(y)$;
(ii) x een dekpunt is van σ (dus $\sigma(x) = x$).
Dan $\sigma[\mathbf{s}/x]\mathbf{t} = [\sigma\mathbf{s}/x]\sigma\mathbf{t}$.

Bewijs. Inductie over $\mathbf{t}$. Als x in $\mathbf{t}$ niet voorkomt, dan $\sigma[\mathbf{s}/x]\mathbf{t} = \sigma\mathbf{t}$; en x komt in $\sigma\mathbf{t}$ ook niet voor, dus $\sigma\mathbf{t} = [\sigma\mathbf{s}/x]\sigma\mathbf{t}$. Als $\mathbf{t} = x$, dan ook $\sigma\mathbf{t} = x$, en $\sigma[\mathbf{s}/x]\mathbf{t} = \sigma\mathbf{s} = [\sigma\mathbf{s}/x]\sigma\mathbf{t}$.

Neem voor de inductiestap aan dat $\mathbf{t} = Q\mathbf{t}_1\ldots\mathbf{t}_n$, en $\sigma[\mathbf{s}/x]\mathbf{t}_i = [\sigma\mathbf{s}/x]\sigma\mathbf{t}_i$, voor $i = 1,\ldots, n$. Dan

$$\begin{aligned}\sigma[\mathbf{s}/x]\mathbf{t} &= Q(\sigma[\mathbf{s}/x]\mathbf{t}_1, \ldots, \sigma[\mathbf{s}/x]\mathbf{t}_n)\\ &= Q([\sigma\mathbf{s}/x]\sigma\mathbf{t}_1, \ldots, [\sigma\mathbf{s}/x]\sigma\mathbf{t}_n) \text{ volgens inductiehypothese;}\\ &= [\sigma\mathbf{s}/x]\sigma\mathbf{t}.\end{aligned}$$ ⊠

8.8 Afleidingen

Laat $\mathcal{E} = \langle \mathcal{T}, E\rangle$ een equationele theorie zijn. Een *afleiding* in $\mathcal{E}$ is een rijtje $\Pi = \alpha_1, \ldots, \alpha_n$ van vergelijkingen over $\mathcal{T}$. Elke vergelijking in Π heeft een rechtvaardiging: α_i is 1. een *aanname*,

of 2. een *instantie van een vergelijking in E*,

of 3. van de vorm $\mathbf{t} \approx \mathbf{t}$;

of 4. α_i volgt uit eerdere vergelijkingen door vervanging van gelijken: er zijn $j, k < i$, termen $\mathbf{s}$ en $\mathbf{t}$, en een vergelijking $\beta(x)$ zo dat $\alpha_j = (\mathbf{s} \approx \mathbf{t})$, $\alpha_k = \beta(\mathbf{s})$, en $\alpha_i = \beta(\mathbf{t})$.

We schrijven $\alpha_1,\ldots, \alpha_m \vdash_{\mathcal{E}} \beta$ wanneer er een afleiding in $\mathcal{E}$ bestaat waarin geen andere aannamen voorkomen dan $\alpha_1,\ldots, \alpha_m$, en waarvan β het laatste element is.

De vergelijkingen in E zijn de *niet-logische axioma's* van $\mathcal{E}$. Een vergelijking $\mathbf{t} \approx \mathbf{t}$ noemen we een *logische identiteit*.

8.9 Afgeleide regels

Als eerste voorbeelden beschouwen we een paar schematische afleidingen. Ze demonstreren kenmerkende eigenschappen van de gelijkheidsrelatie. We gebruiken ze in het vervolg om afleidingen in te korten. We veronderstellen een willekeurige equationele theorie $\mathcal{E} = \langle \mathcal{T}, E\rangle$.

8.9.1 *Symmetrieregel*. $\mathbf{s} \approx \mathbf{t} \vdash_{\mathcal{E}} \mathbf{t} \approx \mathbf{s}$.

Bewijs.

1.	$\mathbf{s} \approx \mathbf{t}$	aanname
2.	$\mathbf{s} \approx \mathbf{s}$	logische identiteit
3.	$\mathbf{t} \approx \mathbf{s}$	vervanging volgens 1. in 2. als $[\mathbf{s}/x](x \approx \mathbf{s})$.

De variabele x in de rechtvaardiging van stap 3 is niet helemaal willekeurig: ze mag niet in $\mathbf{s}$ voorkomen, anders gaat het verkeerd. Dergelijke details worden vaak onderdrukt. ⊠

8.9.2 *Vervanging modulo symmetrie*. $\mathbf{s} \approx \mathbf{t}, \beta(\mathbf{t}) \vdash_{\mathcal{E}} \beta(\mathbf{s})$.

Bewijs.

1.	$\mathbf{s} \approx \mathbf{t}$	aanname
2.	$\mathbf{t} \approx \mathbf{s}$	uit 1, symmetrie
3.	$\beta(\mathbf{t})$	aanname
4.	$\beta(\mathbf{s})$	vervanging volgens 2. in 3.

⊠

8.9.3 *Transitiviteitsregel*. $\mathbf{r} \approx \mathbf{s}, \mathbf{s} \approx \mathbf{t} \vdash_{\mathcal{E}} \mathbf{r} \approx \mathbf{t}$.

Bewijs.
1. $\mathbf{r} \approx \mathbf{s}$ aanname
2. $\mathbf{s} \approx \mathbf{t}$ aanname
3. $\mathbf{r} \approx \mathbf{t}$ vervanging volgens 1. in 2. als $[\mathbf{s}/x](x \approx \mathbf{t})$. ☒

Gegeneraliseerde Transitiviteitsregel: Zij $n > 0$. Dan

$$\mathbf{t}_0 \approx \mathbf{t}_1, \ldots, \mathbf{t}_{n-1} \approx \mathbf{t}_n \vdash_{\mathcal{E}} \mathbf{t}_0 \approx \mathbf{t}_n.$$

Bewijs. Met inductie naar n. Het geval $n = 1$ is triviaal. Als de regel geldt met k gesubstitueerd voor n, en $n = k + 1$, dan is er een bewijs van $\mathbf{t}_0 \approx \mathbf{t}_k$ uit de aannamen $\mathbf{t}_0 \approx \mathbf{t}_1, \ldots, \mathbf{t}_{k-1} \approx \mathbf{t}_k$; uit $\mathbf{t}_0 \approx \mathbf{t}_k$ en de aanname $\mathbf{t}_k \approx \mathbf{t}_n$ concluderen we $\mathbf{t}_0 \approx \mathbf{t}_n$ volgens de Transitiviteitsregel. ☒

8.9.4 *Compatibiliteitsregel*. Laat $Q \in \mathcal{T}$ een n-plaatsig operatiesymbool zijn. Dan $\mathbf{s}_0 \approx \mathbf{t}_0, \ldots, \mathbf{s}_{n-1} \approx \mathbf{t}_{n-1} \vdash_{\mathcal{E}} Q\mathbf{s}_0\ldots\mathbf{s}_{n-1} \approx Q\mathbf{t}_0\ldots\mathbf{t}_{n-1}$.

Bewijs.
1. $\mathbf{s}_0 \approx \mathbf{t}_0$ aanname
2. $Q\mathbf{s}_0\ldots\mathbf{s}_{n-1} \approx Q\mathbf{s}_0\ldots\mathbf{s}_{n-1}$ logische identiteit
3. $Q\mathbf{s}_0\ldots\mathbf{s}_{n-1} \approx Q\mathbf{t}_0\mathbf{s}_1\ldots\mathbf{s}_{n-1}$ vervanging volgens 1. in 2. als $[\mathbf{s}_0/x](Q\mathbf{s}_0\ldots\mathbf{s}_{n-1} \approx Qx\mathbf{s}_1\ldots\mathbf{s}_{n-1})$
4. $\mathbf{s}_1 \approx \mathbf{t}_1$ aanname
5. $Q\mathbf{s}_0\ldots\mathbf{s}_{n-1} \approx Q\mathbf{t}_0\mathbf{t}_1\mathbf{s}_2\ldots\mathbf{s}_{n-1}$ vervanging volgens 4. in 3. als $[\mathbf{s}_1/x](Q\mathbf{s}_0\ldots\mathbf{s}_{n-1} \approx Q\mathbf{t}_0x\mathbf{s}_2\ldots\mathbf{s}_{n-1})$

…

$2n-1$. $Q\mathbf{s}_0\ldots\mathbf{s}_{n-1} \approx Q\mathbf{t}_0\ldots\mathbf{t}_{n-2}\mathbf{s}_{n-1}$
$2n$. $\mathbf{s}_{n-1} \approx \mathbf{t}_{n-1}$ aanname
$2n+1$. $Q\mathbf{s}_0\ldots\mathbf{s}_{n-1} \approx Q\mathbf{t}_0\ldots\mathbf{t}_{n-1}$ vervanging volgens $2n$. in $2n-1$. als $[\mathbf{s}_{n-1}/x](Q\mathbf{s}_0\ldots\mathbf{s}_{n-1} \approx Q\mathbf{t}_0\ldots\mathbf{t}_{n-2}x)$. ☒

8.9.5 *Substitutiewet*. Laat σ een substitutie zijn (van termen over $\mathcal{T}$ voor variabelen). Als $\alpha_1, \ldots, \alpha_m \vdash_{\mathcal{E}} \beta$, dan $\sigma\alpha_1, \ldots, \sigma\alpha_m \vdash_{\mathcal{E}} \sigma\beta$.

Bewijs. Met inductie naar de lengte van de gegeven afleiding van β uit $\alpha_1, \ldots, \alpha_m$.

Als β een aanname is, dus $\beta \in \{\alpha_1, \ldots, \alpha_m\}$, dan $\sigma\beta \in \{\sigma\alpha_1, \ldots, \sigma\alpha_m\}$. Als β een instantie is van een niet-logisch axioma, dan is $\sigma\beta$ dat ook. Als β een logische identiteit is, dan is $\sigma\beta$ ook een logische identiteit.

Als β volgt uit eerdere vergelijkingen door vervanging van gelijken, zeg dat $\beta = \gamma(\mathbf{t})$, en volgt uit $\mathbf{s} \approx \mathbf{t}$ en $\gamma(\mathbf{s})$, dan volgt $\sigma\beta$ uit $\sigma(\mathbf{s} \approx \mathbf{t})$ en $\sigma(\gamma(\mathbf{s}))$, want $\sigma(\mathbf{s} \approx \mathbf{t})$ is $\sigma\mathbf{s} \approx \sigma\mathbf{t}$ per definitie, en $\sigma(\gamma(\mathbf{r})) = \gamma'(\sigma\mathbf{r})$ voor een vergelijking γ' en $\mathbf{r} = \mathbf{s}, \mathbf{t}$. ☒

De substitutiewet is strict genomen geen afleidingsregel; het bewijs beschrijft geen afleiding, maar een transformatie van een afleiding in een afleiding van iets anders. De wet rechtvaardigt wel een regel:

8.9.6 *Substitutieregel*. Als $x_1, \ldots, x_n$ niet voorkomen in de aannamen, dan mag je $\alpha(\mathbf{t}_1, \ldots, \mathbf{t}_n)$ concluderen uit $\alpha(x_1, \ldots, x_n)$.

Als je iets eenmaal bewezen hebt, dan mag je het in latere bewijzen gebruiken zonder het bewijs te herhalen. Formeel gesproken:

8.9.7 *Snedelemma*. Als $\alpha_1,\ldots,\alpha_m \vdash_{\mathcal{E}} \beta$ en $\beta,\gamma_1,\ldots,\gamma_n \vdash_{\mathcal{E}} \delta$, dan

$$\alpha_1,\ldots,\alpha_m,\gamma_1,\ldots,\gamma_n \vdash_{\mathcal{E}} \delta.$$

Bewijs. Vervang in de afleiding van δ de aanname β door de afleiding van β. ⊠

8.10 Voorbeelden. Ook als we het gebruik van afgeleide regels toestaan, is de omzetting van equationele bewijzen in *formele* equationele bewijzen bewerkelijk.

(i) In de groepentheorie kunnen we losweg als volgt redeneren:

$$(x^{-1})^{-1}e \approx (x^{-1})^{-1}(x^{-1}x) \approx ((x^{-1})^{-1}x^{-1})x \approx ex \approx x.$$

Formeel moeten we alles rechtvaardigen. Het bovenstaande bewijs van $(x^{-1})^{-1}e \approx x$ wordt dan:

1. $(x^{-1})^{-1}(x^{-1}x) \approx (x^{-1})^{-1}(x^{-1}x)$ logische identiteit
2. $x^{-1}x \approx e$ niet-logisch axioma
3. $(x^{-1})^{-1}e \approx (x^{-1})^{-1}(x^{-1}x)$ 2. op 1. als $[(x^{-1}x)/y]((x^{-1})^{-1}y) \approx (x^{-1})^{-1}(x^{-1}x)$
4. $(x^{-1})^{-1}(x^{-1}x) \approx ((x^{-1})^{-1}x^{-1})x$ instantie van niet-logisch axioma
5. $(x^{-1})^{-1}x^{-1} \approx e$ instantie van niet-logisch axioma
6. $(x^{-1})^{-1}(x^{-1}x) \approx ex$ 5. op 4. als $[(x^{-1})^{-1}x^{-1}/y]((x^{-1})^{-1}(x^{-1}x) \approx yx)$
7. $ex \approx x$ niet-logisch axioma
8. $(x^{-1})^{-1}e \approx x$ transitiviteit op 3, 6. en 7.

(ii) In de Boole-algebra redeneren we informeel als volgt:

$$\neg 0 \approx \neg(x \wedge \neg x) \approx \neg x \vee \neg\neg x \approx 1.$$

Een formeel bewijs is:

1. $x \wedge \neg x \approx 0$ 0-1-wet
2. $0 \approx x \wedge \neg x$ symmetrie op 1.
3. $\neg 0 \approx \neg(x \wedge \neg x)$ compatibiliteit op 2.
4. $\neg(x \wedge \neg x) \approx \neg x \vee \neg\neg x$ instantie van De Morgan-wet
5. $\neg x \vee \neg\neg x \approx 1$ instantie van 0-1-wet (Wet van de Uitgesloten Derde)
6. $\neg 0 \approx 1$ transitiviteit op 3, 4. en 5.

Oefeningen bij §8:

8:1 Generaliseer het substitutielemma naar simultane substituties $[\mathbf{s}_1/x_1,\ldots,\mathbf{s}_k/x_k]$.

8:2 Leid af in de groepentheorie:
(a) $xe \approx x$;
(b) $x \cdot x^{-1} \approx e$;
(c) $(x^{-1})^{-1} \approx x$;
(d) $(xy)^{-1} \approx y^{-1}x^{-1}$.

8:3* Leid af in de ringentheorie:
(a) $x \cdot 0 \approx 0$;
(b) $x \cdot (-y) \approx -(xy)$.

8:4 Ga na dat de Boolese axioma's geldig zijn in machtsverzamelingsalgebra's (Voorbeeld 7.4(iii)).

8:5 Leid de Boolese axioma's in de rechterkolom af uit die in de linker.

8:6 De theorie der *positieve implicatie-algebra's* is van type $\{\to\}$, en heeft de axioma's

$$(x \to x) \to y \approx y \ ;$$

$$x \to (y \to z) \approx (x \to y) \to (x \to z) \ ;$$

$$(x \to y) \to ((y \to x) \to y) \approx (y \to x) \to ((x \to y) \to x).$$

(a) Ga na dat deze vergelijkingen geldig zijn in de algebra's $\mathbf{M}_n$ van Voorbeeld 7.4(ii). Concludeer dat ze ook geldig zijn in $\mathbf{M}_n \times \mathbf{M}_n$.
(b) Bewijs, in de theorie der positieve implicatie-algebra's,
(i) $x \to x \approx y \to y$,
(ii) $x \to (y \to x) \approx y \to y$,
(iii) $(x \to (y \to z)) \to ((x \to y) \to (x \to z)) \approx y \to y$,
(iv) $x \to y \approx y \to y, y \to x \approx y \to y \vdash x \approx y$.

8:7 De theorie der *Boolese implicatie-algebra's* is van type $\{\to\}$, en heeft naast de axioma's voor positieve implicatie-algebra's het axioma

$$(x \to y) \to x \approx x \ .$$

(a) Ga na dat deze vergelijking geldig is in expansies van Boole-algebra's waarin $a \to b$ gedefinieerd is als $\neg a \vee b$. Met andere woorden, als $\mathbf{B} =$

$$\langle B, \neg, \wedge, \vee, 1, 0 \rangle$$

een Boole-algebra is, en we definiëren $\mathbf{B}'$ als $(\mathbf{B}, \to) =$

$$\langle B, \neg, \wedge, \vee, 1, 0, \to \rangle$$

door $a \to^{\mathbf{B}'} b := \neg^{\mathbf{B}}(a) \vee^{\mathbf{B}} b$, dan $\mathbf{B}' \models (x \to y) \to x \approx x$.
(b) Bewijs, in de theorie der Boolese implicatie-algebra's,
(i) $(x \to y) \to y \approx (y \to x) \to x$,
(ii) $(x \to z) \to ((y \to z) \to (((x \to y) \to y) \to z)) \approx y \to y$,
(iii) $x \to (x \to y) \approx x \to y$,
(iv) $((x \to y) \to (y \to x)) \to (y \to x) \approx y \to y$.

8:8 De theorie der *Boolese implicatie-falsum-algebra's* is van type $\{\to, \bot\}$, en heeft naast de axioma's voor Boolese implicatie-algebra's het axioma

$$\bot \to x \approx y \to y \ .$$

(a) Ga na dat deze vergelijking geldig is in de expansies van Boole-algebra's waarin $a \to b$ gedefinieerd is als $\neg a \vee b$, als je $\bot$ interpreteert als 0.
(b) Bewijs, in de theorie der Boolese implicatie-falsum-algebra's,
(i) $(x \to \bot) \to \bot \approx x$,
(ii) $(x \to (x \to \bot)) \to (x \to \bot) \approx y \to y$.

8:9 Zij $\mathrm{I}(\mathcal{T})$ de equationele theorie zonder niet-logische axioma's over het vocabulaire $\mathcal{T}$. Bewijs: $\vdash_{\mathrm{I}(\mathcal{T})} \mathbf{s} \approx \mathbf{t}$ dan en slechts dan als $\mathbf{s} = \mathbf{t}$.

§9 Correctheid en volledigheid van de termlogica

Afleidingssystemen zijn, zoals betoogd in §6, in de eerste plaats bedoeld als bruikbare karakterisering van een notie van geldige gevolgtrekking. Het gevolgtrekkingsbegrip dat we in de termlogica op het oog hebben, zullen we nu (9.2) definiëren.

9.1 Definitie. Een *model* van een equationele theorie $\mathcal{E} = \langle \mathcal{T}, E \rangle$ is een algebra van type $\mathcal{T}$ waarin alle elementen van E geldig zijn.

De modellen van de groepentheorie zijn de groepen, die van de ringentheorie de ringen, Boole-algebra's zijn de modellen van de theorie der Boole-algebra's, enzovoort.

Als Γ een verzameling vergelijkingen is, en $\boldsymbol{a}$ een bedeling in een algebra $\mathbf{A}$, dan zullen we zeggen dat Γ vervuld wordt door $\boldsymbol{a}$ als $\boldsymbol{a}$ alle elementen van Γ vervult. Notatie: $\mathbf{A} \models \Gamma[\boldsymbol{a}]$.

9.2 Definitie. Laat $\mathcal{E} = \langle \mathcal{T}, E\rangle$ een equationele theorie zijn, en $\Gamma \cup \{\beta\}$ een verzameling vergelijkingen van type $\mathcal{T}$. Dan is β een gevolg van Γ in $\mathcal{E}$, notatie

$$\Gamma \models_{\mathcal{E}} \beta,$$

als in ieder model van $\mathcal{E}$, iedere bedeling die Γ vervult ook β vervult.

Als Γ eindig is, zeg $\Gamma = \{\alpha_1,\ldots, \alpha_n\}$, dan schrijven we ook

$$\alpha_1,\ldots, \alpha_n \models_{\mathcal{E}} \beta,$$

en zeggen dat β volgt uit $\alpha_1,\ldots, \alpha_n$.

9.3 Voorbeeld. $(xy)^{-1} \approx x^{-1}y^{-1}$ is een gevolg van $xy \approx yx$ in de groepentheorie.

9.4 Lemma. Laat $\mathbf{A}$, $\mathbf{B}$ en $\mathbf{C}$ algebra's zijn van hetzelfde type, en f: $\mathbf{A} \longrightarrow \mathbf{B}$ en g: $\mathbf{B} \longrightarrow \mathbf{C}$ homomorfismen. Dan is $g \circ f$ een homomorfisme van $\mathbf{A}$ naar $\mathbf{C}$.

Bewijs. Door uitschrijven van de definitie. Laat Q een n-plaatsig operatiesymbool zijn, en $a_0,\ldots, a_{n-1} \in A$. Dan

$$\begin{aligned}(g \circ f)(Q^{\mathbf{A}}(a_0,\ldots, a_{n-1})) &= g(f(Q^{\mathbf{A}}(a_0,\ldots, a_{n-1}))), \text{ per definitie,}\\ &= g(Q^{\mathbf{B}}(f(a_0),\ldots,f(a_{n-1}))) \text{ omdat } f \text{ een homomorfisme is,}\\ &= Q^{\mathbf{C}}(g(f(a_0)),\ldots, g(f(a_{n-1}))) \text{ omdat } g \text{ een homomorfisme is,}\\ &= Q^{\mathbf{C}}((g \circ f)(a_0),\ldots, (g \circ f)(a_{n-1})) \text{ per definitie.}\end{aligned}$$ ⊠

9.4.1 Gevolg. Laat $\mathbf{A}$ en $\mathbf{B}$ algebra's zijn van type $\mathcal{T}$; f: $\mathbf{A} \longrightarrow \mathbf{B}$ een homomorfisme; $\mathbf{t}$ een term over $\mathcal{T}$, en $\boldsymbol{a}$ een bedeling in $\mathbf{A}$. Dan

$$f(\mathbf{t}^{\mathbf{A}}[\boldsymbol{a}]) = \mathbf{t}^{\mathbf{B}}[f \circ \boldsymbol{a}].$$

Bewijs. Merk op dat $f \circ \boldsymbol{a}$ een bedeling is in $\mathbf{B}$. Laat $\boldsymbol{a}^*$: $\mathbf{T}_{\mathcal{T}}(\mathrm{Var}) \longrightarrow \mathbf{A}$ het unieke homomorfisme zijn dat $\boldsymbol{a}$ uitbreidt, en $(f \circ \boldsymbol{a})^*$: $\mathbf{T}_{\mathcal{T}}(\mathrm{Var}) \longrightarrow \mathbf{B}$ het unieke homomorfisme dat $f \circ \boldsymbol{a}$ uitbreidt. Volgens het lemma is $f \circ \boldsymbol{a}^*$ ook een homomorfisme van $\mathbf{T}_{\mathcal{T}}(\mathrm{Var})$ naar $\mathbf{B}$; dus $f \circ \boldsymbol{a}^* = (f \circ \boldsymbol{a})^*$.

Voor een term $\mathbf{t}$ betekent dit:

$$f(\mathbf{t}^{\mathbf{A}}[\boldsymbol{a}]) = f(\boldsymbol{a}^*(\mathbf{t})) = (f \circ \boldsymbol{a})^*(\mathbf{t}) = \mathbf{t}^{\mathbf{B}}[f \circ \boldsymbol{a}].$$ ⊠

9.4.2 Gevolg. Laat $\mathbf{A}$ een algebra zijn van type $\mathcal{T}$, $\mathbf{t}$ een term en β een vergelijking over $\mathcal{T}$, $\boldsymbol{a}$ een bedeling in $\mathbf{A}$, en σ, ρ: $\mathrm{Var} \longrightarrow \mathbf{T}_{\mathcal{T}}(\mathrm{Var})$ substituties.
(i) $(\sigma\mathbf{t})^{\mathbf{A}}[\boldsymbol{a}] = \mathbf{t}^{\mathbf{A}}[\boldsymbol{a}^* \circ \sigma]$.
(ii) $\mathbf{A} \models \sigma\beta[\boldsymbol{a}]$ dan en slechts dan als $\mathbf{A} \models \beta[\boldsymbol{a}^* \circ \sigma]$.
(iii) Als $(\sigma(x))^{\mathbf{A}}[\boldsymbol{a}] = (\rho(x))^{\mathbf{A}}[\boldsymbol{a}]$ voor elke variabele x die in $\mathbf{t}$ voorkomt, dan $(\sigma\mathbf{t})^{\mathbf{A}}[\boldsymbol{a}] = (\rho\mathbf{t})^{\mathbf{A}}[\boldsymbol{a}]$.
(iv) Als $(\sigma(x))^{\mathbf{A}}[\boldsymbol{a}] = (\rho(x))^{\mathbf{A}}[\boldsymbol{a}]$ voor elke variabele x die in β voorkomt, en $\mathbf{A} \models \sigma\beta[\boldsymbol{a}]$, dan $\mathbf{A} \models \rho\beta[\boldsymbol{a}]$.

Bewijs. (i) Per definitie, $(\sigma\mathbf{t})^{\mathbf{A}}[\boldsymbol{a}] = \boldsymbol{a}^*(\sigma^*(\mathbf{t}))$, en $\mathbf{t}^{\mathbf{A}}[\boldsymbol{a}^* \circ \sigma] = (\boldsymbol{a}^* \circ \sigma)^*(\mathbf{t})$. Maar $\boldsymbol{a}^* \circ \sigma^*$ is een homomorfisme dat $\boldsymbol{a}^* \circ \sigma$ uitbreidt, en daar is er maar één van, dus $\boldsymbol{a}^* \circ \sigma^* = (\boldsymbol{a}^* \circ \sigma)^*$.
(ii) Laat $\beta = (\mathbf{t}_0 \approx \mathbf{t}_1)$. Dan $\mathbf{A} \models \sigma\beta[\boldsymbol{a}] \Leftrightarrow (\sigma\mathbf{t}_0)^{\mathbf{A}}[\boldsymbol{a}] = (\sigma\mathbf{t}_1)^{\mathbf{A}}[\boldsymbol{a}]$ per definitie
$\Leftrightarrow \mathbf{t}_0^{\mathbf{A}}[\boldsymbol{a}^* \circ \sigma] = \mathbf{t}_1^{\mathbf{A}}[\boldsymbol{a}^* \circ \sigma]$ volgens (i),
$\Leftrightarrow \mathbf{A} \models \beta[\boldsymbol{a}^* \circ \sigma]$.
(iii) Merk op dat $\boldsymbol{a}^* \circ \sigma$ en $\boldsymbol{a}^* \circ \rho$ bedelingen zijn in $\mathbf{A}$, en dat ze aan alle variabelen die in $\mathbf{t}$ voorkomen dezelfde waarde toekennen. Dus volgens het Eindigheidslemma (7.13), $\mathbf{t}^{\mathbf{A}}[\boldsymbol{a}^* \circ \sigma] = \mathbf{t}^{\mathbf{A}}[\boldsymbol{a}^* \circ \rho]$. Pas nu (i) toe.
(iv) Laat $\beta = (\mathbf{t}_0 \approx \mathbf{t}_1)$. Volgens (iii), $(\sigma\mathbf{t}_0)^{\mathbf{A}}[\boldsymbol{a}] = (\rho\mathbf{t}_0)^{\mathbf{A}}[\boldsymbol{a}]$ en $(\sigma\mathbf{t}_1)^{\mathbf{A}}[\boldsymbol{a}] = (\rho\mathbf{t}_1)^{\mathbf{A}}[\boldsymbol{a}]$. Maar $\mathbf{A} \models \sigma\beta[\boldsymbol{a}]$ wil zeggen dat $(\sigma\mathbf{t}_0)^{\mathbf{A}}[\boldsymbol{a}] = (\sigma\mathbf{t}_1)^{\mathbf{A}}[\boldsymbol{a}]$; dat impliceert dan $(\rho\mathbf{t}_0)^{\mathbf{A}}[\boldsymbol{a}] = (\rho\mathbf{t}_1)^{\mathbf{A}}[\boldsymbol{a}]$, dat is, $\mathbf{A} \models \rho\beta[\boldsymbol{a}]$. ⊠

9.4.3 Gevolg. Laat $\mathbf{A}$ een algebra zijn van type $\mathcal{T}$, ρ: Var $\longrightarrow \mathbf{T}_{\mathcal{T}}(\text{Var})$ een substitutie, en β een vergelijking over $\mathcal{T}$. Als $\mathbf{A} \models \beta$, dan $\mathbf{A} \models \rho\beta$.

Bewijs. Stel $\mathbf{A} \models \beta$. Neem een willekeurige bedeling $\boldsymbol{a}$ in $\mathbf{A}$. Omdat $\boldsymbol{a}^* \circ \rho$ een bedeling is in $\mathbf{A}$, geldt

(1) $$\mathbf{A} \models \beta[\boldsymbol{a}^* \circ \rho].$$

Zij $\beta = (\mathbf{s} \approx \mathbf{t})$. Uit (1) volgt

(2) $$\mathbf{s}^{\mathbf{A}}[\boldsymbol{a}^* \circ \rho] = \mathbf{t}^{\mathbf{A}}[\boldsymbol{a}^* \circ \rho],$$

dus volgens .2(i), $(\rho\mathbf{s})^{\mathbf{A}}[\boldsymbol{a}] = (\rho\mathbf{t})^{\mathbf{A}}[\boldsymbol{a}]$, dus $\mathbf{A} \models \rho\beta[\boldsymbol{a}]$. Omdat $\boldsymbol{a}$ willekeurig was, mogen we concluderen dat $\mathbf{A} \models \rho\beta$. ⊠

9.5 In het vervolg schrijven we
$$\Gamma \vdash_{\mathcal{E}} \beta$$
voor: er bestaat een afleiding van β in $\mathcal{E}$ waarvan de aannamen tot Γ behoren. (Cf. 6.6.1.)

Correctheidsstelling. Zij $\mathcal{E} = \langle \mathcal{T}, E \rangle$ een equationele theorie, en $\Gamma \cup \{\beta\}$ een verzameling vergelijkingen van type $\mathcal{T}$. Als $\Gamma \vdash_{\mathcal{E}} \beta$, dan $\Gamma \models_{\mathcal{E}} \beta$.

Bewijs. Inductie naar de lengte van de afleiding. Stel dat Γ vervuld wordt door $\boldsymbol{a}$ in zeker model $\mathbf{M}$ van $\mathcal{E}$. We moeten laten zien dat β wordt vervuld door $\boldsymbol{a}$.
1. Als $\beta \in \Gamma$, dan is er niets te bewijzen.
2. Als β een instantie is van een niet-logisch axioma van $\mathcal{E}$, dan $\mathbf{M} \models \beta[\boldsymbol{a}]$ omdat $\mathbf{M}$ een model is van $\mathcal{E}$ (pas gevolg .4.3 toe).
3. Als β een logische identiteit is, zeg $\beta = (\mathbf{t} \approx \mathbf{t})$, dan $\mathbf{M} \models \beta[\boldsymbol{a}]$ omdat $\mathbf{t}[\boldsymbol{a}] = \mathbf{t}[\boldsymbol{a}]$.
4. Als β is afgeleid door vervanging van gelijken, zeg $\beta = \delta(\mathbf{t})$, en β volgt uit $\delta(\mathbf{s})$ en $\mathbf{s} \approx \mathbf{t}$, dan volgens inductiehypothese $\mathbf{s}[\boldsymbol{a}] = \mathbf{t}[\boldsymbol{a}]$ en $\mathbf{M} \models \delta(\mathbf{s})[\boldsymbol{a}]$. Volgens 9.4.2(iv) — laat $\boldsymbol{s}^* = [\mathbf{s}/x]$ en $\boldsymbol{r}^* = [\mathbf{t}/x]$ voor een geschikte variabele x — moet dan $\mathbf{M} \models \delta(\mathbf{t})[\boldsymbol{a}]$. ⊠

Net als in de propositielogica (§6.6) is het omgekeerde van het correctheidsprobleem, het volledigheidsprobleem, principieel moeilijker, en vereist de oplossing een nieuw idee.

9.6 Equivalentierelaties

Zij X een niet-lege verzameling, en R een binaire relatie op X. Dan is R een *equivalentierelatie op* X als R
— *reflexief* is, dat wil zeggen, xRx voor alle $x \in X$;
— *symmetrisch*, dat is, als xRy dan ook yRx;
— en *transitief*, als xRy en yRz dan xRz.
Een *partitie* van X is een collectie $\mathcal{A}$ van niet-lege paarsgewijs disjuncte deelverzamelingen van X waarvan de vereniging X is.

Laat nu R een equivalentierelatie zijn op X, en $x \in X$. De *equivalentieklasse* van x over R is de verzameling

$$x/R := \{y \in X \mid yRx\};$$

en het *quotient* van de verzameling X over R is

$$X/R := \{x/R \mid x \in X\}.$$

Propositie. Als R een equivalentierelatie is van X, dan is X/R een partitie van X.

Bewijs. De elementen van X/R zijn de equivalentieklassen van de elementen van X; omdat R reflexief is, geldt altijd $x \in x/R$, dus $x/R \neq \emptyset$.

De elementen van X/R zijn paarsgewijs disjunct, want als x/R en y/R *niet* disjunct zijn, zeg $z \in x/R \cap y/R$, dan zRx en zRy. Omdat R symmetrisch is, volgt xRz; en omdat R transitief is, xRy. Transitiviteit geeft dan $x/R \subseteq y/R$, en, omdat x en y verwisselbaar zijn, $x/R = y/R$.

Tenslotte, $x/R \subseteq X$, en $x \in x/R$, voor elke $x \in X$; dus $\bigcup(X/R) = X$. ⊠

9.7 Voorbeelden

(i) Laat X een niet-lege verzameling zijn. Gelijkheid, als relatie tussen elementen van X, is een equivalentierelatie. We noemen deze relatie ook wel de *diagonaal over* X, notatie Δ_X. Dus $\Delta_X = \{\langle x, x\rangle \mid x \in X\}$.
(ii) De universele relatie over X is $\nabla_X = X \times X$; ook een equivalentierelatie.
(iii) Zij n een natuurlijk getal. Gehele getallen x en y heten *congruent modulo* n als $x - y$ een veelvoud is van n. Congruentie modulo n is een equivalentierelatie, want
(refl) $x - x = 0 \cdot n$;
(sym) als $x - y = z \cdot n$, dan $y - x = (-z) \cdot n$; en
(trans) als $x - y = u \cdot n$, en $y - z = v \cdot n$, dan $x - z = (u + v) \cdot n$.
(iv) Laat $\mathbb{Z}_+ = \{1, 2, 3, \ldots\}$ de verzameling zijn der positieve gehele getallen. We noemen twee paren $v = \langle v_1, v_2\rangle$ en $w = \langle w_1, w_2\rangle$ van positieve gehele getallen *gelijkverschillig* als

$$v_1 + w_2 = w_1 + v_2.$$

Gelijkverschilligheid is een equivalentierelatie.
(v) Logische equivalentie, gedefinieerd in §3.7, is een equivalentierelatie van FP. Eigenlijk volgt dat uit voorbeeld (i), volgens algemene principes:
1° Laat $f\colon X \longrightarrow Y$ een afbeelding zijn. De *kern* van f is de relatie

$$\ker f := \{\langle x_1, x_2\rangle \in X \times X \mid f(x_1) = f(x_2)\}.$$

De kern van een afbeelding is altijd een equivalentierelatie.

2° Als $\mathcal{R}$ een collectie is van equivalentierelaties van X, dan is $\bigcap\mathcal{R}$ een equivalentierelatie van X.

9.8 Congruentierelaties

Een equivalentierelatie R op het universum van een algebra **A** kan 'correct' zijn in de zin dat bij toepassing van operaties op equivalente elementen de resultaten equivalent zijn. We noemen deze vorm van correctheid *compatibiliteit*. Bijvoorbeeld, *even lang zijn* is compatibel met *twintig centimeter langer maken*.

9.8.1 Definitie. Zij **A** een algebra, en R een binaire relatie op A. Dan is R *compatibel* met **A** als voor elke n, voor elke n-plaatsige operatie Q van **A**, geldt:

als $a_1Rb_1,\ldots$, en a_nRb_n, dan ook $\langle Q(a_1,\ldots,a_n), Q(b_1,\ldots,b_n)\rangle \in R$.

9.8.2 Definitie. Zij **A** een algebra. Een *congruentierelatie* van **A** is een equivalentierelatie van A die compatibel is met **A**.

9.9 Voorbeelden

(i) Laat **A** een algebra zijn. Dan zijn Δ_A en ∇_A congruentierelaties van **A**.
(ii)* Congruentie modulo n is een congruentierelatie van de ring der gehele getallen, want als $x_1 - x_2 = k \cdot n$ en $y_1 - y_2 = m \cdot n$, dan
(+) $(x_1 + y_1) - (x_2 + y_2) = (x_1 - x_2) + (y_1 - y_2) = (k + m) \cdot n$;
(·) $x_1y_1 - x_2y_2 = x_1(y_1 - y_2) + (x_1 - x_2)y_2 = (x_1m + ky_2) \cdot n$; en
(–) $-x_1 - (-x_2) = x_2 - x_1 = -k \cdot n$.
Voor 'x is congruent met y modulo n' is de notatie $x \equiv y\ (n)$ in zwang. We zullen die ook gebruiken voor andere congruentierelaties: $w \equiv x \equiv y\ (\theta)$ betekent dat $w\theta x$ en $x\theta y$.
(iii) *Constructie van de gehele getallen uit de positieve*. Tot vrij recent kenden de mensen alleen positieve getallen. (En de meesten niet veel: Het zevendeeeuwse Statuut van Shrewsbury bepaalt dat men om te mogen getuigen in een rechtsgeding tot negen moet kunnen tellen.) Voor positieve getallen is aftrekking een partiële operatie. Dat probleem is opgelost door de uitvinding van negatieve getallen. Een filosoof zou zich echter nog altijd af kunnen vragen of negatieve getallen bestaan, en dan zou hij baat kunnen hebben bij de volgende constructie. Definieer optelling en vermenigvuldiging op de verzameling $X = \mathbb{Z}_+ \times \mathbb{Z}_+$ door:

$$\langle x, y\rangle + \langle u, v\rangle = \langle x + u, y + v\rangle;$$

$$\langle x, y\rangle \cdot \langle u, v\rangle = \langle xu + yv, yu + xv\rangle.$$

Bovendien hebben we voor elk tweetal paren een verschil:

$$\langle x, y\rangle - \langle u, v\rangle = \langle x + v, y + u\rangle.$$

De gelijkverschilligheidsrelatie γ is een congruentierelatie van de algebra **X** $= \langle X, +, \cdot, -\rangle$. Want, stel dat $\langle x_1, x_2\rangle \equiv \langle y_1, y_2\rangle$ en $\langle u_1, u_2\rangle \equiv \langle v_1, v_2\rangle\ (\gamma)$. Dan tellen we op:

$$\begin{array}{c} x_1 + y_2 = x_2 + y_1 \\ u_1 + v_2 = u_2 + v_1 \qquad + \\ \hline (x_1 + u_1) + (y_2 + v_2) = (x_2 + u_2) + (y_1 + v_1), \end{array}$$

dus $\langle x_1, x_2\rangle + \langle u_1, u_2\rangle \equiv \langle y_1, y_2\rangle + \langle v_1, v_2\rangle$ (γ). Analoog bewijst men dat γ product en verschil respecteert.
(iv) Logische equivalentie is een congruentierelatie van **FP**. We kunnen de algemene principes van Voorbeeld .7(v) namelijk als volgt versterken:
1° Laat f: $\mathbf{A} \longrightarrow \mathbf{B}$ een homomorfisme zijn. Dan is ker$f$ een congruentierelatie van $\mathbf{A}$.
2° Als $\mathcal{R}$ een collectie is van congruentierelaties van $\mathbf{A}$, dan is $\bigcap\mathcal{R}$ een congruentierelatie van $\mathbf{A}$.

9.10 Quotient

Als θ een congruentie is van $\mathbf{A}$, dan is er een eenvoudige manier om uit de operaties van $\mathbf{A}$ een algebra te definiëren met universum A/θ.

Definitie. Zij $\mathbf{A}$ een algebra van type $\mathcal{T}$, en θ een congruentierelatie van $\mathbf{A}$. Dan is $\mathbf{A}/\theta$, het *quotient van* $\mathbf{A}$ *over* θ, de algebra van type $\mathcal{T}$ met universum A/θ en operaties $Q^{\mathbf{A}/\theta}$, voor $Q \in \mathcal{T}$, zeg van plaatsigheid n, gedefinieerd door

$$Q^{\mathbf{A}/\theta}(a_1/\theta, \ldots, a_n/\theta) = Q^{\mathbf{A}}(a_1, \ldots, a_n)/\theta.$$

Enig nadenken over deze definitie kan tot onzekerheid leiden. Het is alsof we een functie *het aantal letters van de achternaam* op personen definiëren; en nu blijken er mensen te zijn met meerdere achternamen. Bij *M. Junius Brutus* is dat geen probleem, maar *C. Cassius Longinus* leidt in uiterste consequentie tot een bewijs dat 7 = 8. Bij de definitie van het quotient worden zulke problemen uitgesloten door de compatibiliteitsconditie. Die zegt dat het niet uitmaakt welke representanten van $a_1/\theta, \ldots, a_n/\theta$ je neemt, omdat de waarde van $Q^{\mathbf{A}}$ altijd in dezelfde congruentieklasse blijkt te liggen.

Voorbeeld. Laat $\mathbf{X}$ de algebra zijn die we geconstrueerd hebben in 9(iii) hierboven. Het quotient $\mathbf{X}/\gamma$ kan worden beschouwd als een uitbreiding van $\mathbb{Z}_+$, want de afbeelding $n \longmapsto \langle n+1, 1\rangle/\gamma$ is injectief, en behoudt sommen (dus ook verschillen, voorzover ze bestaan) en producten.

*Het reduct $\langle X/\gamma, +, \cdot\rangle$ van $\mathbf{X}/\gamma$ heeft een ring-expansie: neem $\Delta_{\mathbb{Z}_+}$ als additief eenheidselement, en de inverse relatie als additief inverse.

Een onmiddellijk gevolg van de definitie is:

9.11 Propositie. Zij θ een congruentierelatie van een algebra $\mathbf{A}$. Dan is de afbeelding

$$\nu_\theta\colon a \longmapsto a/\theta$$

een homomorfisme van $\mathbf{A}$ op $\mathbf{A}/\theta$.

We noemen ν_θ het *natuurlijke*, of *kanonieke* homomorfisme van $\mathbf{A}$ op $\mathbf{A}/\theta$.

9.12 Stelling. Laat $\mathcal{E} = \langle \mathcal{T}, E\rangle$ een equationele theorie zijn, en Γ een verzameling vergelijkingen van type $\mathcal{T}$. Definieer θ op $T_{\mathcal{T}}(\mathrm{Var})$ door

$$\mathbf{t}_1 \theta \mathbf{t}_2 \text{ dan en slechts dan als } \Gamma \vdash_{\mathcal{E}} \mathbf{t}_1 \approx \mathbf{t}_2.$$

Dan is θ een congruentierelatie van $\mathbf{T}_{\mathcal{T}}(\mathrm{Var})$.

Bewijs. Korten we $\mathbf{T}_{\mathcal{T}}(\mathrm{Var})$ af tot $\mathbf{T}$. We moeten aantonen dat θ 1° een equivalentierelatie is van T, en 2° compatibel met $\mathbf{T}$.
1° θ is reflexief: voor elke $\mathbf{t} \in T$ is $\mathbf{t} \approx \mathbf{t}$ een logische identiteit, dus

$$\Gamma \vdash_{\mathcal{E}} \mathbf{t} \approx \mathbf{t}.$$

θ is symmetrisch: stel $\Gamma \vdash_{\mathcal{E}} \mathbf{t}_1 \approx \mathbf{t}_2$. Volgens de symmetrieregel (8.9.1),

$$\mathbf{t}_1 \approx \mathbf{t}_2 \vdash_{\mathcal{E}} \mathbf{t}_1 \approx \mathbf{t}_2.$$

Het Snedelemma (8.9.7) impliceert nu $\Gamma \vdash_{\mathcal{E}} \mathbf{t}_1 \approx \mathbf{t}_2$.
θ is transitief: stel $\Gamma \vdash_{\mathcal{E}} \mathbf{t}_1 \approx \mathbf{t}_2$ en $\Gamma \vdash_{\mathcal{E}} \mathbf{t}_2 \approx \mathbf{t}_3$. Volgens de transitiviteitsregel (8.9.3),

$$\mathbf{t}_1 \approx \mathbf{t}_2, \mathbf{t}_2 \approx \mathbf{t}_3 \vdash_{\mathcal{E}} \mathbf{t}_1 \approx \mathbf{t}_3.$$

Het Snedelemma impliceert nu eerst $\Gamma, \mathbf{t}_2 \approx \mathbf{t}_3 \vdash_{\mathcal{E}} \mathbf{t}_1 \approx \mathbf{t}_3$, en vervolgens

$$\Gamma \vdash_{\mathcal{E}} \mathbf{t}_1 \approx \mathbf{t}_3.$$

2° Laat $Q \in \mathcal{T}$ een n-plaatsig operatiesymbool zijn. Stel

$$\Gamma \vdash_{\mathcal{E}} \mathbf{s}_0 \approx \mathbf{t}_0, \ldots, \Gamma \vdash_{\mathcal{E}} \mathbf{s}_{n-1} \approx \mathbf{t}_{n-1}.$$

We moeten bewijzen dat $\langle Q^{\mathbf{T}}(\mathbf{s}_0,\ldots, \mathbf{s}_{n-1}),\ Q^{\mathbf{T}}(\mathbf{t}_0,\ldots, \mathbf{t}_{n-1})\rangle \in \theta$. Volgens de compatibiliteitsregel (8.9.4),

$$\mathbf{s}_0 \approx \mathbf{t}_0, \ldots, \mathbf{s}_{n-1} \approx \mathbf{t}_{n-1} \vdash_{\mathcal{E}} Q\mathbf{s}_0\ldots\mathbf{s}_{n-1} \approx Q\mathbf{t}_0\ldots\mathbf{t}_{n-1}.$$

Door n toepassingen van het Snedelemma krijgen we daaruit

$$\Gamma \vdash_{\mathcal{E}} Q\mathbf{s}_0\ldots\mathbf{s}_{n-1} \approx Q\mathbf{t}_0\ldots\mathbf{t}_{n-1}.$$

Dat volstaat, want per definitie $Q^{\mathbf{T}}(\mathbf{r}_0,\ldots, \mathbf{r}_{n-1}) = Q\mathbf{r}_0\ldots\mathbf{r}_{n-1}$. ☒

De in bovenstaande stelling gedefinieerde congruentierelatie is belangrijk genoeg om een naam te verdienen. We spreken van de *door* Γ *in* $\mathcal{E}$ *voortgebrachte congruentie*, en noteren $\Theta_{\mathcal{E}}(\Gamma)$.

9.13 Stelling. Zij $\mathcal{E} = \langle \mathcal{T}, E\rangle$ een equationele theorie, en Γ een verzameling vergelijkingen van type $\mathcal{T}$. Dan is $\mathbf{T}_{\mathcal{T}}(\mathrm{Var})/\Theta_{\mathcal{E}}(\Gamma)$ een model van $\mathcal{E}$.

Bewijs. Kort af: $\mathbf{T} = \mathbf{T}_{\mathcal{T}}(\mathrm{Var})$, $\theta = \Theta_{\mathcal{E}}(\Gamma)$, en $\mathbf{A} = \mathbf{T}/\theta$. Laat $\mathbf{s} \approx \mathbf{t}$ een niet-logisch axioma zijn van $\mathcal{E}$, en $\boldsymbol{a}$ een bedeling in $\mathbf{A}$. We moeten aantonen dat $\mathbf{s}^{\mathbf{A}}[\boldsymbol{a}] = \mathbf{t}^{\mathbf{A}}[\boldsymbol{a}]$.

Laat $\boldsymbol{r}$ een bedeling zijn in $\mathbf{T}$ zo dat voor alle i, $\boldsymbol{r}(v_i) \in \boldsymbol{a}(v_i)$. Dan $\boldsymbol{a} = \nu_\theta \circ \boldsymbol{r}$. Dus volgens .4.1, $\mathbf{s}^{\mathbf{A}}[\boldsymbol{a}] = \mathbf{s}^{\mathbf{A}}[\nu_\theta \circ \boldsymbol{r}] = \nu_\theta(\mathbf{s}^{\mathbf{T}}[\boldsymbol{r}]) = \mathbf{s}^{\mathbf{T}}[\boldsymbol{r}]/\theta$. Laat $\boldsymbol{r}^*\colon \mathbf{T} \longrightarrow \mathbf{T}$ het unieke homomorfisme (zie §7.12) zijn dat $\boldsymbol{r}$ uitbreidt; bedenk dat voor elke term $\mathbf{q}$ per definitie $\mathbf{q}^{\mathbf{T}}[\boldsymbol{r}] = \boldsymbol{r}^*(\mathbf{q})$. In het bijzonder geldt $\mathbf{s}^{\mathbf{A}}[\boldsymbol{a}] = \boldsymbol{r}^*(\mathbf{s})/\theta$, en evenzo $\mathbf{t}^{\mathbf{A}}[\boldsymbol{a}] = \boldsymbol{r}^*(\mathbf{t})/\theta$. Maar $\boldsymbol{r}^*(\mathbf{s}) \approx \boldsymbol{r}^*(\mathbf{t})$ is een instantie van een niet-logisch axioma, dus $\Gamma \vdash_{\mathcal{E}} \boldsymbol{r}^*(\mathbf{s}) \approx \boldsymbol{r}^*(\mathbf{t})$; dus $\boldsymbol{r}^*(\mathbf{s})/\theta = \boldsymbol{r}^*(\mathbf{t})/\theta$. ☒

9.14 Volledigheidsstelling. Zij $\mathcal{E} = \langle \mathcal{T}, E\rangle$ een equationele theorie, en $\Gamma \cup \{\beta\}$ een verzameling vergelijkingen van type $\mathcal{T}$. Als β in $\mathcal{E}$ volgt uit Γ, dan is β in $\mathcal{E}$ afleidbaar uit Γ.

Bewijs. Door contrapositie: stel dat β *niet* afleidbaar is uit Γ. Kort weer af: $\mathbf{T} = \mathbf{T}_{\mathcal{T}}(\mathrm{Var})$, $\theta = \Theta_{\mathcal{E}}(\Gamma)$, en $\mathbf{A} = \mathbf{T}/\theta$. Laat $\beta = (\mathbf{s} \approx \mathbf{t})$. Dat $\Gamma \nvdash_{\mathcal{E}} \beta$ impliceert $\mathbf{s}/\theta \neq \mathbf{t}/\theta$.

Laat ι de inbedding zijn van de variabelen in T. Dan is ι een bedeling in $\mathbf{T}$, en het unieke homomorfisme ι^* dat ι uitbreidt is de identieke functie 1_T. Beschouw de bedeling $\boldsymbol{a} = \nu_\theta \circ \iota$ in $\mathbf{A}$. Voor elke term $\mathbf{r}$ geldt:

$$\mathbf{r}^{\mathbf{A}}[\boldsymbol{a}] = \mathbf{r}^{\mathbf{A}}[\nu_\theta \circ \iota] = \nu_\theta(\mathbf{r}^{\mathbf{T}}[\iota]) = \mathbf{r}/\theta,$$

wegens Gevolg .4.1 en omdat $\mathbf{r}^{\mathbf{T}}[\iota] = \iota^*(\mathbf{r}) = \mathbf{r}$. Dus

$$\mathbf{A} \models \Gamma[\boldsymbol{a}] \text{ en } \mathbf{A} \not\models \beta[\boldsymbol{a}],$$

en omdat **A** volgens de vorige stelling een model is van $\mathcal{E}$, zien we daaraan dat β in $\mathcal{E}$ *niet* volgt uit Γ. ☒

Oefeningen bij §9:

9:1 Zij $\mathrm{I}(\mathcal{T})$ de equationele theorie zonder niet-logische axioma's over het vocabulaire $\mathcal{T}$. Bewijs: $\vdash_{\mathrm{I}(\mathcal{T})} \mathbf{s} \approx \mathbf{t}$ dan en slechts dan als $\mathbf{s} = \mathbf{t}$. (Cf. 8:9; kun je een ander bewijs bedenken?)

9:2 Laat $\mathcal{E} = \langle \mathcal{T}, E\rangle$ en $\mathcal{E}' = \langle \mathcal{T}', E\rangle$ equationele theorieën zijn met dezelfde niet-logische axioma's, maar $\mathcal{T}' \supset \mathcal{T}$. Bewijs: als $\Gamma \cup \{\beta\}$ een verzameling vergelijkingen is van type $\mathcal{T}$, en $\Gamma \vdash_{\mathcal{E}'} \beta$, dan ook al $\Gamma \vdash_{\mathcal{E}} \beta$.

Deze oefening rechtvaardigt de notatie $\Gamma \vdash \beta$ voor: β is afleidbaar uit Γ in de theorie $\mathrm{I}(\mathcal{T})$ over één of ander vocabulaire $\mathcal{T}$ dat de operatiesymbolen bevat die voorkomen in de elementen van $\Gamma \cup \{\beta\}$. Laat nu bovendien $E^{\mathcal{T}}$ de verzameling zijn van alle substitutie-instanties van elementen van E over type $\mathcal{T}$; dan kunnen we $\Gamma \vdash_{\mathcal{E}} \beta$ noteren als $E^{\mathcal{T}} \cup \Gamma \vdash \beta$.

9:3 Laat $\mathcal{A}$ een partitie zijn van een verzameling X. Vind een equivalentierelatie R van X zo dat $\mathcal{A} = X/R$.

9:4 (a) Bewijs dat *gelijkverschilligheid* (Voorbeeld 7(iv)) inderdaad een equivalentierelatie is.

(b) Zij **X** de algebra gedefinieerd in Voorbeeld 9(iii). Voltooi het bewijs dat gelijkverschilligheid een congruentierelatie is van **X**.

(c) Definieer f op $\mathbb{Z}_+$ door

$$f(n) = \langle n + 1, 1\rangle/\gamma.$$

Bewijs dat f injectief is, en dat voor alle $m, n \in \mathbb{Z}_+$, $f(m + n) = f(m) + f(n)$, $f(m \cdot n) = f(m) \cdot f(n)$, en, als $m > n$, $f(m - n) = f(m) - f(n)$.

9:5 (a) Bewijs de algemene beweringen in Voorbeeld 7(v). Hoe volgt daaruit dat logische equivalentie een equivalentierelatie is?

(b) Bewijs de algemene beweringen in Voorbeeld 9(iv). Hoe volgt daaruit dat logische equivalentie een congruentierelatie is van **Fp**?

9:6* Een algebra **A** heet een *subalgebra* van een algebra **B**, notatie $\mathbf{A} \leq \mathbf{B}$, als **A** en **B** van hetzelfde type zijn, $A \subseteq B$, en voor elk (n-plaatsig, zeg) operatiesymbool Q van het gemeenschappelijke type, voor alle $a_1,\ldots, a_n \in A$ geldt dat $Q^{\mathbf{A}}(a_1,\ldots, a_n) = Q^{\mathbf{B}}(a_1,\ldots, a_n)$.

Bewijs: als $\mathbf{A} \leq \mathbf{B}$, en α is een vergelijking van het type van **A** en **B** die geldig is in **B**, dan $\mathbf{A} \models \alpha$.

Een subalgebra van een algebra in een door vergelijkingen gedefinieerde klasse behoort dus ook tot die klasse. In het bijzonder heet een subalgebra van een groep een *ondergroep*, en een subalgebra van een ring een *deelring*.

9:7 Een ondergroep **N** van een groep **G** heet een *normaaldeler* van **G** als voor alle $x, y \in G$, $x \in N$ impliceert dat $y^{-1}xy \in N$.

(a) Laat θ een congruentierelatie zijn van een groep **G**. Bewijs dat e/θ het universum is van een normaaldeler van **G**.

(b) Laat **N** een normaaldeler zijn van **G**. Vind een congruentierelatie θ van **G** zo dat $e/\theta = N$.

(c) Geef een formele afleiding in de groepentheorie van $(xy^{-1})^{-1} \approx yx^{-1}$.
(d)* Construeer een één-op-één correspondentie tussen normaaldelers van **G** en congruentierelaties van **G**.

9:8* Een deelring **I** van een ring **R** heet een (*tweezijdig*) *ideaal* van **R** als voor alle $x, y \in R, x \in I$ impliceert dat xy en yx tot I behoren.
(a) Laat θ een congruentierelatie zijn van een ring **R**. Bewijs dat $0/\theta$ het universum is van een tweezijdig ideaal van **R**.
(b) Laat **I** een tweezijdig ideaal zijn van **R**. Vind een congruentierelatie θ van **R** zo dat $0/\theta = I$.
(c) Construeer een één-op-één correspondentie tussen idealen van **R** en congruentierelaties van **R**.

❀ §10 Boole-algebra

In deze § beschouwen we Boole-algebra's op drie manieren: rechtop, ondersteboven, en als iets anders.

10.1 Dualiteit

We weten uit Oefening 8:5 dat een groot deel van de in 8.4(iii) opgesomde axioma's voor Boole-algebra's redundant is. De reden voor de dubbele axiomatisering is een gewichtig *symmetrieprincipe*.

Laat $\mathbf{B} = \langle B, \neg, \wedge, \vee, 1, 0\rangle$ een Boole-algebra zijn. De *duale* van **B** is

$$\mathbf{B}^\partial := \langle B, \neg, \vee, \wedge, 0, 1\rangle.$$

(De veranderde volgorde geeft aan dat $\wedge^{\mathbf{B}^\partial} = \vee^{\mathbf{B}}$, etc. Zie 7.4(ia).)

Propositie. De duale van een Boole-algebra is een Boole-algebra.

Bewijs. Door de verandering van interpretatie krijgt iedere Boolese wet de betekenis van de corresponderende wet in de andere kolom van 8.4(iii). ☒

We kunnen ook termen en vergelijkingen dualiseren.

Definitie. (i) Zij **t** een term van type $\mathcal{B}ool$. De *duale* van **t** is de term $\mathbf{t}^\partial$, gedefinieerd door:

$\mathbf{t}^\partial = \mathbf{t}$ als **t** een variabele is;
$\mathbf{t}^\partial = \neg(\mathbf{s}^\partial)$ als $\mathbf{t} = \neg\mathbf{s}$;
$\mathbf{t}^\partial = \mathbf{r}^\partial \vee \mathbf{s}^\partial$ als $\mathbf{t} = \mathbf{r} \wedge \mathbf{s}$;
$\mathbf{t}^\partial = \mathbf{r}^\partial \wedge \mathbf{s}^\partial$ als $\mathbf{t} = \mathbf{r} \vee \mathbf{s}$;
$1^\partial = 0, 0^\partial = 1$.

(ii) De duale van een vergelijking $\mathbf{s} \approx \mathbf{t}$ is $\mathbf{s}^\partial \approx \mathbf{t}^\partial$.

Lemma. Zij **t** een term van type $\mathcal{B}ool$, **B** een Boole-algebra, en $\boldsymbol{b}$ een bedeling in **B**. Dan is $\boldsymbol{b}$ ook een bedeling in $\mathbf{B}^\partial$, en $\mathbf{t}^{\mathbf{B}}[\boldsymbol{b}] = (\mathbf{t}^\partial)^{\mathbf{B}^\partial}[\boldsymbol{b}]$.

Bewijs. Met inductie over **t**. Als **t** een variabele is, dan $\mathbf{t}^{\mathbf{B}}[\boldsymbol{b}] = \boldsymbol{b}(\mathbf{t}) = \boldsymbol{b}(\mathbf{t}^\partial) = (\mathbf{t}^\partial)^{\mathbf{B}^\partial}[\boldsymbol{b}]$. ☒

Oefening 1. Maak het hierboven begonnen bewijs af.

Dualiteitsprincipe voor afleidingen. Zij $\mathcal{B}$ de theorie der Boole-algebra's. Als $\alpha_1, \ldots, \alpha_m \vdash_{\mathcal{B}} \beta$, dan ook $\alpha_1^\partial, \ldots, \alpha_m^\partial \vdash_{\mathcal{B}} \beta^\partial$.

Bewijs. Met inductie naar de lengte van de afleiding; of door gebruik van de Volledigheidsstelling, en de propositie en het lemma hierboven. ☒

Iets dat identiek is met zijn duale heet *zelfduaal*. Bijvoorbeeld, de dubbele negatie-wet is zelfduaal.

10.2 Boolese ringen

In een deel van de literatuur over Boole-algebra worden de symbolen + en · gebruikt in plaats van ∨ en ∧. In het bijzonder gebruikte Boole zelf + en ·; gedreven als hij was door de verwantschap die hij waarnam tussen logica en waarschijnlijkheidsrekening, had hij juist niet de neiging om nieuwe symbolen uit te vinden.

Het verschil tussen onze notatie en die van Boole is echter kleiner dan het lijkt. In §1 hebben we + ingevoerd als symbool voor de *exclusieve* disjunctie. Welnu, Boole deed zijn best om in het midden te laten of zijn disjunctie inclusief was of exclusief, en wilde alleen over *p of q* spreken als *p* en *q* elkaar uitsloten. (Dat is ook beter als je kansen wilt optellen.) Men zou met enig recht kunnen beweren dat Boole niet de Boole-algebra heeft uitgevonden, maar iets anders.

Een *Boolese ring* is een commutatieve ring met multiplicatief eenheidselement waarin de vermenigvuldiging *idempotent* is, dat wil zeggen, voor ieder element x geldt

$$x \cdot x = x.$$

Lemma. In een Boolese ring geldt $x \approx -x$.

Bewijs. Omdat vermenigvuldiging idempotent is, geldt

$$x + x = (x + x)(x + x) = xx + xx + xx + xx = x + x + x + x,$$

dus $0 = (x + x) - (x + x) = (x + x + x + x) - (x + x) = x + x$. A fortiori, $-x = x$. ☒

10.3 Ringen en algebra's

Boolese ringen en Boole-algebra's zijn in wezen hetzelfde.

10.3.1. Laat $\mathbf{B} = \langle B, \neg, \wedge, \vee, 1, 0\rangle$ een Boole-algebra zijn. Definieer, voor $a, b \in B$, $a + b$ als $(a \wedge \neg b) \vee (\neg a \wedge b)$ en $a \cdot b$ als $a \wedge b$. Dan is $\mathbf{B}^{\mathbf{r}} :=$

$$\langle B, +, 1_B, 0, \cdot, 1\rangle$$

een Boolese ring. (De identieke functie 1_B is de interpretatie van de additieve inverse.)

Bewijs. Volgens de associatieve en commutatieve wetten en de idempotentiewet van de Boole-algebra's is de vermenigvuldiging inderdaad associatief, commutatief en idempotent. Merk op dat $x \cdot \neg x = 0$, en $x \cdot 0 = 0$. De distributieve wet (in een commutatieve ring heb je er maar één nodig) bewijst men dan als volgt:

$$\begin{aligned} x \cdot (y + z) &= x \cdot (y \cdot \neg z \vee \neg y \cdot z) = x \cdot y \cdot \neg z \vee x \cdot \neg y \cdot z \\ &= x \cdot y \cdot \neg x \vee x \cdot y \cdot \neg z \vee \neg x \cdot x \cdot z \vee \neg y \cdot x \cdot z \\ &= xy \cdot (\neg x \vee \neg z) \vee (\neg x \vee \neg y) \cdot xz = xy \cdot \neg(xz) \vee \neg(xy) \cdot xz = xy + xz. \end{aligned}$$

Merk op dat $\neg(a + b) = \neg(a \cdot \neg b \vee \neg a \cdot b) = \neg(a \cdot \neg b) \cdot \neg(\neg a \cdot b)$
$= (\neg a \vee \neg\neg b) \cdot (\neg\neg a \vee \neg b) = \neg a \cdot (a \vee \neg b) \vee b \cdot (a \vee \neg b)$
$= \neg a \cdot a \vee \neg a \cdot \neg b \vee b \cdot a \vee b \cdot \neg b = \neg a \cdot \neg b \vee b \cdot a.$

Nu bewijzen we dat $\langle B, +, 1_B, 0\rangle$ een abelse groep is:

$0 + x = 0 \cdot \neg x \vee \neg 0 \cdot x = 0 \vee 1 \cdot x = x,$

$-x + x = x + x = 0$ volgens Lemma 2, en

$x + (y + z) = x \cdot \neg(y + z) \vee \neg x \cdot (y + z) = x \cdot (\neg y \cdot \neg z \vee z \cdot y) \vee \neg x \cdot (y \cdot \neg z \vee \neg y \cdot z)$

$$= x{\cdot}\neg y{\cdot}\neg z \vee x{\cdot}z{\cdot}y \vee \neg x{\cdot}y{\cdot}\neg z \vee \neg x{\cdot}\neg y{\cdot}z$$

$$= (x{\cdot}\neg y \vee \neg x{\cdot}y){\cdot}\neg z \vee (x{\cdot}y \vee \neg x{\cdot}\neg y){\cdot}z = (x + y) + z.$$

10.3.2. Laat $\mathbf{R} = \langle R, +, -, 0, \cdot, 1\rangle$ een Boolese ring zijn. Definieer, voor $r, s \in R$, $\neg r$ als $r + 1$, $r \wedge s$ als $r \cdot s$, en $r \vee s$ als $r + s + rs$. Dan is $\mathbf{R^a} :=$

$$\langle R, \neg, \wedge, \vee, 1, 0\rangle$$

een Boole-algebra.

Bewijs. Volgens Oefening 8:5 hoeven we slechts de helft van de axioma's te bewijzen. Alleen komt de *rechterkolom* ons nu beter uit dan de linker. Gelukkig is de rechterkolom de duale van de linker, en dus gelijkwaardig (onder behoud van de, zelfduale, dubbele negatiewet) volgens het dualiteitsprincipe.

De associatieve wet, de commutatieve wet en de idempotentiewet voor $\wedge$ zijn direct gegeven.

Distributieve wet: $x \wedge (y \vee z) = x \cdot (y + z + yz) = xy + xz + xyz$
$= xy + xz + xyxz = (x \wedge y) \vee (x \wedge z)$.

Absorptiewet: $x \wedge (x \vee y) = x \cdot (x + y + xy) = xx + xy + xxy$
$= x + xy + xy = x$ volgens Lemma 2.

Wet van De Morgan: $\neg x \vee \neg y = x + 1 + y + 1 + (x + 1)(y + 1)$

$= x + y + xy + x + y + 1$ (Lemma 2)

$= xy + 1 = \neg(x \wedge y)$ (Lemma 2)

Noncontradictie: $x \wedge \neg x = x(x + 1) = x + x = 0$.

Dubbele Negatie: $\neg\neg x = x + 1 + 1 = x$ volgens Lemma 2.

10.4 Subuniversa

Laat $\mathbf{A}$ een algebra zijn. Een verzameling $X \subseteq A$ is een *subuniversum* van $\mathbf{A}$ als ze gesloten is onder de operaties van $\mathbf{A}$, i.e., als voor iedere operatie Q van $\mathbf{A}$, voor alle $x_1,\ldots, x_n \in X$ (als n de plaatsigheid is van Q) geldt dat ook $Q(x_1,\ldots, x_n) \in X$.

Voorbeelden. (i) De even getallen vormen een subuniversum van de ring $\mathbf{Z} = \langle \mathbb{Z}, +, \cdot, -, 0\rangle$, en de oneven getallen niet.
(ii) Zij $n > 2$. Dan is $\{0, n - 1\}$ een subuniversum van $\mathbf{M}_n = \langle M_n, \rightarrow, 0\rangle$ (zie 7.4(iib)), en $\{0, n - 2\}$ niet.

Propositie. (a) Als $\mathbf{A} \leq \mathbf{B}$, dan is A een subuniversum van $\mathbf{B}$.
(b) Ieder niet-leeg subuniversum van een algebra $\mathbf{B}$ is het universum van een subalgebra van $\mathbf{B}$.

Bewijs.
(a) Laat Q een (n-plaatsig) operatiesymbool zijn van het type van $\mathbf{A}$ en $\mathbf{B}$, en $x_1,\ldots, x_n \in A$. Dan $Q^{\mathbf{B}}(x_1,\ldots, x_n) = Q^{\mathbf{A}}(x_1,\ldots, x_n) \in A$, dus A is gesloten onder de operaties van $\mathbf{B}$.
(b) Zij A een niet-leeg subuniversum van $\mathbf{B}$. Definieer een interpretatie I van het vocabulaire van $\mathbf{B}$ als volgt: als Q n-plaatsig is, en $x_1,\ldots, x_n \in A$, dan

$$I(Q)(x_1,\ldots, x_n) = Q^{\mathbf{B}}(x_1,\ldots, x_n).$$

Dan is $\langle A, I\rangle$ een subalgebra van $\mathbf{B}$. ⊠

Het onderscheid tussen subalgebra's en subuniversa is vaak irrelevant, met name als het vocabulaire constantesymbolen bevat. Men noemt dan bijvoorbeeld een subuniversum van een groep kortweg 'ondergroep'.

10.5 Idealen

Idealen zijn gedefinieerd in Oefening 9:8, als een bepaald soort deelringen. Het ligt in de rede ook het universum van zo'n deelring 'ideaal' te noemen. We hebben dan de volgende karakterisering.

10.5.1 Propositie. Zij $\mathbf{R}$ een ring, en $X \subseteq R$ zo dat voor alle $x \in X$ en $r \in R$, $rx \in X$ en $xr \in X$. Dan is X een ideaal van $\mathbf{R}$ dan en slechts dan als
(i) $X \neq \emptyset$; en
(ii) voor alle $x, y \in X$, $x - y \in X$.

Bewijs.
($\Rightarrow$) Laat X een ideaal zijn van $\mathbf{R}$. Dan $0 \in X$, dus $X \neq \emptyset$. Als $x, y \in X$, dan $-y \in X$ omdat X een subuniversum is, en $x + (-y) \in X$ om dezelfde reden.
($\Leftarrow$) We moeten laten zien dat X gesloten is onder de operaties van $\mathbf{R}$. Geslotenheid onder vermenigvuldiging is gegeven. Zij $x \in X$; dan $0 = x - x \in X$; dus omdat $X \neq \emptyset$, $0 \in X$. Als $x, y \in X$, dan $-y = 0 - y \in X$, dus $x + y = x + -(-y) \in X$. ☒

In het bijzonder zijn $\{0\}$ en R idealen: de *triviale idealen* van $\mathbf{R}$.

Als $*$ een binaire operatie is, x een element, en Y, Z deelverzamelingen van het domein waarop $*$ gedefinieerd is, dan zijn de afkortingen

$$x * Y := \{x * y \mid y \in Y\}, \quad Y * x := \{y * x \mid y \in Y\}$$

en $Y * Z := \{y * z \mid y \in Y \text{ en } z \in Z\}$ soms handig.

10.5.2 Propositie. Laat I en J idealen zijn van een ring $\mathbf{R}$. Dan
(a) is $I + J$ een ideaal van $\mathbf{R}$, en
(b) als K een ideaal is van $\mathbf{R}$, en $I \cup J \subseteq K$, dan $I + J \subseteq K$.

Bewijs.
(a) Als $x \in I$ en $y \in J$, en $r \in R$, dan $r(x + y) = rx + ry$, $rx \in I$ en $ry \in J$ omdat I en J idealen zijn, dus $r(x + y) \in I + J$; en analoog $(x + y)r \in I + J$. We kunnen dus verder de vorige propositie toepassen.
(i) Omdat $0 = 0 + 0 \in I + J$, $I + J \neq \emptyset$.
(ii) Stel $u, v \in I + J$. Dan zijn er $u_1, v_1 \in I$ en $u_2, v_2 \in J$ zo dat $u = u_1 + u_2$ en $v = v_1 + v_2$. Omdat I en J idealen zijn, $u_1 - v_1 \in I$ en $u_2 - v_2 \in J$, dus

$$u - v = (u_1 - v_1) + (u_2 - v_2) \in I + J.$$

(b) Laat K een ideaal zijn van $\mathbf{R}$ dat $I \cup J$ omvat. Als $z \in I + J$, dan zijn er $x \in I$ en $y \in J$ zo dat $z = x + y$. Omdat $x, y \in K$, en K gesloten is onder optelling, moet dan $z \in K$. ☒

De idealen van een ring-met-eenheidselement (van type $\mathcal{Ring1}$) zijn per definitie de idealen van haar $\mathcal{Ring}$-reduct. (Cf. Oefening 11:2.)

10.5.3 Propositie. Zij $\mathbf{R}$ een commutatieve ring met 1, en $a \in R$. Dan is
(a) Ra een ideaal van $\mathbf{R}$, en
(b) als I een ideaal is van $\mathbf{R}$, en $a \in I$, dan $Ra \subseteq I$.

Bewijs.
(a) Als $x \in Ra$ en $r \in R$, dan $x = sa$ voor zekere $s \in R$. Dus $rx = (rs)a \in Ra$. Omdat **R** commutatief is, volgt meteen dat $xr \in Ra$. We kunnen dus verder Propositie .1 toepassen.
(i) Omdat $0 = 0 \cdot a \in Ra, Ra \neq \emptyset$.
(ii) Stel $u, v \in Ra$. Dan zijn er $u_1, v_1 \in R$ zo dat $u = u_1a$ en $v = v_1a$. Dus

$$u - v = (u_1 - v_1)a \in Ra.$$

(b) Triviaal. ☒

10.6 Priemidealen

Een ideaal P van een commutatieve ring **R** is *priem* als $P \neq R$ en voor alle x, $y \in R$ geldt: als $xy \in P$, dan $x \in P$ of $y \in P$.

Lemma. Zij P een priemideaal van een Boolese ring **R**. Dan geldt voor alle $r \in R$: òf $r \in P$, òf $r + 1 \in P$.

Bewijs. Voor elke $r \in R$ geldt: $r \cdot (r + 1) = r + r = 0 \in P$. Omdat P priem is, moet minstens één van r en $r + 1$ tot P behoren. Ze kunnen echter niet allebei tot P behoren, want $r + r + 1 = 1$, en als $1 \in P$, dan voor alle $x \in R, x = x \cdot 1 \in P$, dus $P = R$. ☒

Propositie. Als P een priemideaal is van een Boolese ring **R**, dan

$$\mathbf{R}/P \cong (\mathbf{Z}_2, 1).$$

Uitleg. $(\mathbf{Z}_2, 1)$ is de expansie van de ring $\mathbf{Z}_2$ met de voor de hand liggende interpretatie van 1; het is tegelijkertijd, als je $\wedge$ gelijk stelt met $\cdot$, een reduct van de waarheidswaarden-algebra **W**.
Bewijsschets. Een homomorfisme van $\mathbf{R}/P$ naar $(\mathbf{Z}_2, 1)$ moet P afbeelden naar 0, en de nevenklasse $1 + P$ naar 1. Uit het lemma volgt dat er geen andere nevenklassen zijn: als $r \notin P$, dan $r + 1 \in P$, dus $r = 1 + r + 1 \in 1 + P$. ☒

Verdere oefeningen

10:2 Laat $\mathbf{B} = \langle B, \neg, \wedge, \vee, 1, 0\rangle$ een Boole-algebra zijn. Bewijs dat de operatie $\neg$ een isomorfisme is van **B** op $\mathbf{B}^\partial$.

10:3 Laat $\mathbf{B} = \langle B, \neg, \wedge, \vee, 1, 0\rangle$ een Boole-algebra zijn. Definieer, voor $a, b \in B$, $a \leq b$ dan en slechts dan als $a \vee b = b$.
(a) Bewijs dat $a \leq b$ dan en slechts dan als $a \wedge b = a$.
(b) Bewijs dat $\leq$ een ordening is, i.e. dat $\leq$ reflexief is, *antisymmetrisch* (als $a \leq b$ en $b \leq a$ dan $a = b$), en transitief. Bewijs dat 1 het grootste element is, en 0 het kleinste.

10:4 (Cf. 5:12.) Een *Zjegalkin-normaalvorm* is een term over $\mathcal{Ring1}$ van de vorm

$$\mathbf{t}_1 + \ldots + \mathbf{t}_n$$

(n mag 0 zijn, dan is de som 0), waarin elke $\mathbf{t}_i$ een product

$$x_1 \cdot \ldots \cdot x_{k_i}$$

is van verschillende variabelen (k_i mag 0 zijn, dan is het product 1), en geen twee termen $\mathbf{t}_i$ en $\mathbf{t}_j$ ($i \neq j$) precies dezelfde variabelen bevatten. — Dus $x \cdot x$ en $(xy + x)z$ zijn geen Zjegalkin-normaalvormen, maar x en $xyz + xz$ wèl. Laat $\mathcal{BR}$ de theorie zijn van de Boolese ringen (ringentheorie met extra axioma's $xy \approx$

yx en $x \cdot 1 \approx x$), en $\mathbf{t}$ een term van $\mathcal{BR}$. Een Zjegalkin-normaalvorm $\mathbf{z}$ is een Zjegalkin-normaalvorm van $\mathbf{t}$ als $\vdash_{\mathcal{BR}} \mathbf{t} \approx \mathbf{z}$.
(a) Vind Zjegalkin-normaalvormen van
(i) $\neg(p \wedge q) \to \neg q$,
(ii) $\neg(p \vee q) \to (p \to q)$, en
(iii) $(p_0 \to p_1) \vee (\neg p_0 \to p_2) \to p_2$.
(vertaal eerst in ringennotatie).
(b) Laat zien dat in de theorie der Boolese ringen elke term een Zjegalkin-normaalvorm heeft. (Ofwel: bij elke term $\mathbf{t}$ van $\mathcal{BR}$ bestaat een Zjegalkin-normaalvorm $\mathbf{z}$ zo dat $\vdash_{\mathcal{BR}} \mathbf{t} \approx \mathbf{z}$.)

10:5 Zij $\mathbf{G}$ een groep, en $X \subseteq G$. Bewijs dat X een ondergroep is van $\mathbf{G}$ dan en slechts dan als
(i) $X \neq \emptyset$;
(ii) voor alle $x, y \in X, x \cdot y^{-1} \in X$.

10:6 Laat $\mathbf{B}$ een Boole-algebra zijn. Een verzameling $X \subseteq B$ is een *ideaal* van $\mathbf{B}$ als X een ideaal is van $\mathbf{B^r}$.
(a) Bewijs dat een niet-lege deelverzameling X van B een ideaal is dan en slechts dan als X (i) omlaag gesloten is, d.w.z. wanneer $b \le x \in X$, dan $b \in X$, en (ii) gesloten is onder $\vee$, dus als $x, y \in X$, dan $x \vee y \in X$.
(b) Bewijs dat een ideaal $X \neq B$ een priemideaal is dan en slechts dan als $x \wedge y \in X$ alleen als $x \in X$ of $y \in X$.

10:7 (a) Laat $\mathbf{B}$ een Boole-algebra zijn. Ga na dat $\mathbf{B^{ra}} = \mathbf{B}$.
(b) Laat $\mathbf{R}$ een Boolese ring zijn. Ga na dat $\mathbf{R^{ar}} = \mathbf{R}$.

❀ §11 De priemideaalstelling

Een priemideaal verdeelt systematisch de elementen van een Boolese ring in ware en onware (Propositie 10.6). Als we nu willen dat x waar is en y onwaar, kunnen we dan een bijpassend priemideaal vinden? Dat hangt af van de onderlinge verhouding van x en y.

We beginnen met twee lemma's over ringen in het algemeen. Onder een *keten* van verzamelingen verstaan we een collectie $\mathcal{K}$ van verzamelingen zo dat voor alle $K_1, K_2 \in \mathcal{K}$, $K_1 \subseteq K_2$ of $K_2 \subseteq K_1$.

11.1 Lemma. Zij $\mathbf{R}$ een ring, en $\mathcal{K}$ een niet-lege keten van idealen van $\mathbf{R}$. Dan is $\bigcup\mathcal{K}$ een ideaal van $\mathbf{R}$.

Bewijs. $\mathcal{K}$ heeft minstens één element; dat is niet leeg; dus $\bigcup\mathcal{K}$ is niet leeg. Als $x, y \in \bigcup\mathcal{K}$, dan zijn er $K_1, K_2 \in \mathcal{K}$ zo dat $x \in K_1$ en $y \in K_2$. Omdat $K_1 \subseteq K_2$ of $K_2 \subseteq K_1$, is er zeker een $K \in \mathcal{K}$ waar x en y beide toe behoren. Dan $x - y \in K \subseteq \bigcup\mathcal{K}$. Tenslotte, als $x \in \bigcup\mathcal{K}$ en $r \in R$, dan behoort x tot een element K van $\mathcal{K}$; K is een ideaal, dus $rx, xr \in K \subseteq \bigcup\mathcal{K}$. ☒

Laat $\mathcal{X}$ een collectie van verzamelingen zijn. Een *bovengrens* van een deelcollectie $\mathcal{Y} \subseteq \mathcal{X}$ is een verzameling $X \in \mathcal{X}$ die alle elementen van $\mathcal{Y}$ omvat. Een verzameling $M \in \mathcal{X}$ is *maximaal* als er geen $X \in \mathcal{X}$ bestaat waarvan M een echte deelverzameling is.

11.2 Lemma.[11] Zij I een ideaal van een ring $\mathbf{R}$, en $x \in R \setminus I$. Dan bestaat er een ideaal M van $\mathbf{R}$ zo dat
(i) $x \notin M$ en $I \subseteq M$;
(ii) als $J \supset M$ een ideaal is, dan $x \in J$.

Bewijs. Laat $\mathcal{I}$ de verzameling zijn van alle idealen van $\mathbf{R}$ die I omvatten en waar x niet in zit. De collectie $\mathcal{I}$ is niet leeg, want $I \in \mathcal{I}$. Laat $\mathcal{K}$ een keten zijn in de geordende verzameling $\boldsymbol{\mathcal{I}} = \langle \mathcal{I}, \subseteq \rangle$, dat wil zeggen, $\mathcal{K}$ is een keten en $\mathcal{K} \subseteq \mathcal{I}$. Dan heeft $\mathcal{K}$ een bovengrens in $\boldsymbol{\mathcal{I}}$. Als namelijk $\mathcal{K}$ leeg is, dan is I een bovengrens; en als $\mathcal{K} \neq \emptyset$, dan $\bigcup\mathcal{K} \in \mathcal{I}$; dus dan is $\bigcup\mathcal{K}$ een bovengrens.

Volgens het *Lemma van Zorn* heeft $\boldsymbol{\mathcal{I}}$ een maximaal element M. Als $J \supset M$ een ideaal is, dan $J \notin \mathcal{I}$, dus $x \in J$. ☒

In het geval dat x het eenheidselement is van $\mathbf{R}$, is M maximaal in de collectie van alle niet-triviale idealen van $\mathbf{R}$.

11.3 Stelling. Zij I een ideaal van een Boolese ring $\mathbf{R}$, en $x \in R \setminus I$. Dan bestaat er een priemideaal P van $\mathbf{R}$ dat I omvat en waar x niet in zit.

Bewijs. Volgens Lemma 2 bestaat er een ideaal P waarvoor geldt: $x \notin P$, $I \subseteq P$, en als $J \supset P$ een ideaal is, dan $x \in J$. We zullen laten zien dat P priem is.

Stel dat $ab \in P$. Stel dat $a, b \notin P$. Kennelijk zit x dan in ieder ideaal dat $\{a\} \cup P$ omvat, en in ieder ideaal dat $\{b\} \cup P$ omvat. Dan zijn er $r, s \in R$ en $p_1, p_2 \in P$ zo dat $x = ra + p_1$ en $x = sb + p_2$ (Propositie 10.5.2, 3). Dan

$$x = x \cdot x = (ra + p_1)(sb + p_2) = rasb + p_1sb + rap_2 + p_1p_2.$$

Maar dat impliceert dat $x \in P$, quod non. Dus $a \in P$ of $b \in P$, en P is priem. ☒

11.4 Idealen en Filters in Boole-algebra's

Laat $\mathbf{B}$ een Boole-algebra zijn. Een *ideaal* van $\mathbf{B}$ is een ideaal van de Boolese ring $\mathbf{B}^{\mathbf{r}}$. Een ideaal van $\mathbf{B}^{\partial}$ heet een *filter* van $\mathbf{B}$; een priemideaal van $\mathbf{B}^{\partial}$ een *priemfilter* van $\mathbf{B}$. Evenals een ideaal, correspondeert een filter F van $\mathbf{B}$ met een unieke congruentierelatie; we noteren het quotient als $\mathbf{B}/F$. (Zie Oefening 4.)

Propositie. Als Q een priemfilter is van een Boole-algebra $\mathbf{B}$, dan $\mathbf{B}/Q \cong \mathbf{2}$.

Bewijsschets. Een homomorfisme van $\mathbf{B}/Q$ naar $\mathbf{2}$ moet Q afbeelden naar 1, en het complement van Q naar 0. ☒

Priemfilterstelling. Zij F een filter van een Boole-algebra $\mathbf{B}$, en $x \in B \setminus F$. Dan bestaat er een priemfilter Q van $\mathbf{B}$ dat F omvat en waar x niet in zit.

Bewijs. Dualiseer de priemideaalstelling. ☒

Oefeningen

11:1 Geef een voorbeeld van twee idealen in een ring, waarvan de vereniging geen ideaal is.

[11] Het bewijs van dit lemma is een toepassing van het Lemma van Zorn uit de verzamelingsleer. Zie Appendix A, waar ook een bewijs staat voor deelverzamelingen van een *aftelbare* verzameling dat Zorn's Lemma vermijdt.

11:2 Bewijs: als M een maximaal ideaal is van een ring $\mathbf{R}$ met eenheidselement, en $J \supset M$ is een ideaal van $\mathbf{R}$, dan $J = R$.

11:3 Bewijs dat de priemidealen van een Boolese ring maximaal zijn.

11:4* Laat $\mathbf{B}$ een Boole-algebra zijn.
(a) Zij F een filter van $\mathbf{B}$. Definieer een binaire relatie θ_F op B door

$$\langle x, y\rangle \in \theta_F \text{ dan en slechts dan als } (\neg x \vee y) \wedge (\neg y \vee x) \in F.$$

Bewijs dat θ_F een congruentierelatie is van $\mathbf{B}$, en $1/\theta_F = F$.
(b) Bewijs: als θ een congruentierelatie is van $\mathbf{B}$, dan is $1/\theta$ een filter, en $\theta_{1/\theta} = \theta$.

11:5 Laat P een priemfilter zijn van een Boole-algebra $\mathbf{B}$. Bewijs dat $B \setminus P$ een priemideaal is van $\mathbf{B}$.

11:6 Laat $\mathbf{B}$ een Boole-algebra zijn, I een ideaal van $\mathbf{B}$ en F een filter, zo dat $I \cap F = \emptyset$. Construeer een priemideaal $P \supseteq I$ dat F niet snijdt. [Pas de bewijzen van Lemma 2 en Stelling 3 aan.]

11:7* Definieer $\mathcal{B}(\mathrm{FP})$ als de algebra

$$\langle \mathrm{FP}, F_\neg, F_\wedge, F_\vee, \top, \bot\rangle$$

van type $\mathcal{Bool}$.

Formules φ en ψ zijn *bewijsbaar equivalent*, afgekort $\langle \varphi, \psi\rangle \in \mathrm{Beq}$ of $\mathrm{Beq}(\varphi, \psi)$, als $\vdash \varphi \leftrightarrow \psi$.
(a) Ga na dat Voorbeeld 6.3(a) impliceert dat $\varphi \wedge \psi$ bewijsbaar equivalent is met $\psi \wedge \varphi$.

Gebruik bij de twee volgende onderdelen de resultaten — voorbeelden en oefeningen — van §6:
(b) Bewijs dat Beq een congruentierelatie is van $\mathcal{B}(\mathrm{FP})$.
(c) Laat zien dat $\mathcal{B}(\mathrm{FP})/\mathrm{Beq}$ een Boole-algebra is.
(d) Leid Lemma 6.6.12 af uit de Priemideaalstelling.

❀ §12 De Stelling van Stone

Machtsverzamelingsalgebra's zijn in het voorafgaande (7.4(iiib), 8:4) genoemd als voorbeelden van Boole-algebra's. Subalgebra's van zulke algebra's — we zullen ze *verzamelingsalgebra's* noemen — zijn natuurlijk ook Boole-algebra's (9:6). M. Stone ontdekte rond 1935 dat *alle* Boole-algebra's in wezen verzamelingsalgebra's zijn.

12.1 Voorbeeld. Laat X een oneindige verzameling zijn. We noemen een deelverzameling Y van X *coeindig* als $X \setminus Y$ eindig is. De eindige en coeindige deelverzamelingen van X vormen het universum van een verzamelingsalgebra.

12.2 Stelling. Elke Boole-algebra is isomorf met een verzamelingsalgebra.

Bewijs. Een toepassing van de priemfilterstelling. We gebruiken bekende eigenschappen van idealen in gedualiseerde vorm: bijvoorbeeld, ieder filter bevat 1, want ieder ideaal bevat 0.

Laat $\mathbf{B}$ een Boole-algebra zijn. Als $0 = 1$ in $\mathbf{B}$, dan $\mathbf{B} \cong \mathcal{P}\emptyset$. Neem voor het vervolg aan dat $0^{\mathbf{B}} \neq 1^{\mathbf{B}}$.

Zij P de collectie van alle priemfilters van $\mathbf{B}$. Defineer een afbeelding
$\phi\colon B \longrightarrow \mathcal{P}(P)$ door

$$\phi(b) = \{p \in P \mid b \in p\}.$$

Nu geldt:
(i) $\phi(1) = P$, want ieder filter bevat 1.
(ii) $\phi(0) = \emptyset$, want een filter dat 0 bevat, moet gelijk zijn aan B, en is dus niet priem.
(iii) $\phi(x \vee y) = \phi(x) \cup \phi(y)$, want een priemfilter dat $x \vee y$ bevat, moet x of y bevatten.
(iv) $\phi(\neg x) = P \setminus \phi(x)$. Aan de ene kant: een filter dat x en $\neg x$ bevat, bevat 0, en is dus niet priem. Aan de andere kant, een priemfilter p dat x niet bevat, moet $\neg x$ bevatten, omdat $x \vee \neg x = 1 \in p$.

Uit (i)-(iv) volgt dat ϕ een homomorfisme is van **B** naar $\mathcal{P}(P)$, en dat $\phi[B]$ het universum is van een verzamelingsalgebra. We hoeven alleen nog te laten zien dat ϕ injectief is. Laat x en y twee verschillende elementen van **B** zijn. We mogen aannemen dat $y \neq x \vee y$. Dan behoort y dus niet tot het filter $B \vee x$ (cf. Prop. 10.5.3); volgens de priemfilterstelling is er dan een priemfilter p dat $B \vee x$ omvat en waar y niet inzit. Daarentegen $x = 0 \vee x \in p$, dus $p \in \phi(x) \setminus \phi(y)$. ⊠

Oefeningen

12:1 Verifieer Voorbeeld 1.

12:2 Een *atoom* in een Boole-algebra **B** is een element $a \neq 0$ met de eigenschap dat voor alle $b \in B$, $b \wedge a \in \{0, a\}$. We noemen **B** *atomistisch* als voor ieder element $b \neq 0$ een atoom a bestaat zo dat $b \wedge a = a$.
(a) Bewijs dat elke atomistische Boole-algebra isomorf is met een machtsverzamelingsalgebra.
(b) Concludeer dat elke eindige Boole-algebra isomorf is met een machtsverzamelingsalgebra.

12:3 Laat f: $\mathbf{A} \longrightarrow \mathbf{B}$ een homomorfisme zijn van een of ander type algebra's. Bewijs dat $f[A]$ een subuniversum is van **B**.

Deel III. Predikaatlogica

Aristoteles (±350 v.C.) wordt geacht de eerste te zijn geweest die de formele geldigheid van gevolgtrekkingen systematisch onderzocht. Zijn werk bleef meer dan tweeduizend jaar de logische standaard. Deze traditionele logica wordt ook *termlogica* genoemd: net als het in vorige deel van deze syllabus gaat het om uitspraken van de vorm

$$t_1 \text{ is } t_2 \tag{1}$$

waarbij t_1 en t_2 'termen' heten. Alleen zijn deze termen simpele algemene begrippen, zoals *kat* en *zwart*. Een concreet geval van (1) is dus

$$\text{kat is zwart.} \tag{2}$$

(2) is echter geen Nederlands. We moeten het verband tussen *kat* en *zwart* nader specificeren. Aristoteles onderscheidde daarin vier vormen:

(A) Universeel bevestigend: Elke kat is zwart.

(I) Bijzonder bevestigend: Minstens één kat is zwart.

(E) Universeel ontkennend: Geen kat is zwart.

(O) Bijzonder ontkennend: Minstens één kat is niet zwart.

In bepaalde combinaties vormen zulke uitspraken een geldig *syllogisme*, zoals

$$\begin{array}{l} \text{Elke kat is een zoogdier.} \\ \text{Minstens één kat is niet zwart.} \\ \hline \text{Minstens één zoogdier is niet zwart.} \end{array} \tag{3}$$

Over de interpretatie van de termen valt veel diepzinnigs te zeggen, maar het meest voor de hand ligt een interpretatie als klassen. Schema (3) vatten we dan op als

$$\begin{array}{l} K \subseteq M \\ K \setminus Z \neq \emptyset \\ \hline M \setminus Z \neq \emptyset, \end{array} \tag{4}$$

met K de klasse der katten, M die der zoogdieren (*mammalia*), en Z de klasse der zwarten. Het schema (4) is algemeen geldig. Door alle mogelijkheden te onderzoeken vond men in totaal 19 van zulke algemeen geldige schema's.

De syllogistiek speelde een belangrijke rol in wijsbegeerte en theologie. Het systeem heeft echter opvallende beperkingen.

Ten eerste valt de propositielogica erbuiten. Lange tijd viel dat niet op, omdat er zo weinig van bekend was; Boole's logische algebra was de eerste omvattende formalisering van de propositielogica. Boole meende de syllogistiek te kunnen incorporeren in zijn algebra, maar in (4) zien we *ongelijkheden*, die dwars zitten in een algebraïsche benadering. Boole introduceerde daarom ongespecificeerde niet-lege klassen (zie Appendix B); een oplossing waar de wereld op den duur niet tevreden mee was.

Ten tweede heeft de syllogistiek heel weinig te melden over het redeneren in de wiskunde, terwijl dat toch juist, volgens Aristoteles, de deductieve wetenschap bij uitstek is.

§13 Relaties en quantoren

In deel II hebben we redeneringen geformaliseerd van wiskundig belang. Ze betreffen willekeurige operaties, waarvoor noch de syllogistiek, noch de Boole-algebra ruimte geeft; en een *relatie*, de gelijkheid, die in de syllogistiek niet voorkomt, en die in de Boole-algebra een *middel* is, maar geen onderwerp van beschouwing. Een ander typisch wiskundig voorbeeld is

$$\begin{array}{l} a \text{ is niet langer dan } b. \\ \underline{a \text{ is niet even lang als } b.} \\ b \text{ is langer dan } a. \end{array} \tag{13.1}$$

over lijnstukken a en b. Deze gevolgtrekking valt niet te formaliseren in de propositielogica of de syllogistiek, evenmin als haar verborgen premissen. Ook de universele geldigheid van

(13.2) Als iemand het beter weet dan iedereen, dan weet iemand het beter dan hijzelf.

is zo niet verklaarbaar.

13.1 Redenering (13.1) maakt gebruik van de betekenissen van 'langer dan' en 'even lang als'. Dat zijn geen logische begrippen. Het verband tussen hun betekenissen is dus geen logica, maar de logica moet ons de middelen geven om het verband uit te drukken met een extra premisse; zoals we in de propositielogica een verband tussen weersgesteldheden kunnen uitdrukken met

$$\text{de zon schijnt} \rightarrow \neg(\text{het regent} \vee \text{het sneeuwt})$$

of in de termlogica de associativiteit van de vermenigvuldiging met

$$x \cdot (y \cdot z) \approx (x \cdot y) \cdot z.$$

Zoals proposities in de propositielogica, operaties in de termlogica, en eigenschappen (of klassen) in de syllogistiek, dienen *relaties* waarin twee dingen tot elkaar kunnen staan een kategorie te zijn van ons logische systeem. Relaties heten ook wel *predikaten*; vandaar de naam *predikaatlogica*.

De verzwegen premisse van (13.1) is

(13.3) Voor alle [lijnstukken] x en y geldt: x is langer dan y, of x is even lang als y, of y is langer dan x.

Het gedeelte achter de dubbele punt heeft propositielogische structuur; we kunnen het symbolisch weergeven met

(13.4) $x > y \vee x \equiv y \vee y > x.$

We hebben dus een uitbreiding van de propositielogica op het oog, waarin atomaire proposities inwendige structuur kunnen hebben.

Resteert de aanduiding van algemeenheid 'Voor alle x en y'. Zulke aanduidingen komen voor in de syllogistiek; de *major* van (3) kunnen we formuleren als

(13.5) Voor alle x geldt: als x een kat is, dan is x een zoogdier.

Alleen is het algemeenheidsmechanisme van de syllogistiek niet flexibel: je kunt maar één ding tegelijk algemeen maken, en het soort uitspraken waarop de generalisatie betrekking heeft is zeer beperkt.

We sluiten aan bij de wiskundige formulering van (13.3); voor 'voor alle … geldt' voeren we de *universele quantor* $\forall$ in. Resultaat:

(13.6) $\forall xy\,(x > y \vee x \equiv y \vee y > x)$.

Aangevuld en geformaliseerd ziet (13.1) er dan zo uit:

$$\begin{array}{l} \forall xy\,(x > y \vee x \equiv y \vee y > x) \\ \neg(a > b) \\ \neg(a \equiv b) \\ \hline b > a. \end{array} \tag{13.7}$$

De symbolen zijn natuurlijk bijzaak; het gaat om de ideeën erachter, die (13.7) rechtvaardigen. De redenering is geldig omdat de eerste, algemene premisse in het bijzonder a en b betreft; we kunnen dus de tussenstap

$$a > b \vee a \equiv b \vee b > a$$

afleiden. De rest is propositielogica.

In het vervolg zullen we deze ideeën systematisch uitwerken.

13.2 We kunnen het formalisme van de predikaatlogica nu als volgt omschrijven. We hebben

Predikaatletters, die staan voor predikaten. (We spreken ook van *relatiesymbolen*, die staan voor relaties; dat is hetzelfde.) De voorbeelden in 13.1 ($\approx$, $>$, $\equiv$) zijn tweeplaatsig, maar predikaten kunnen ook eenplaatsig zijn, zoals *zwart*, nulplaatsig zoals *het regent*, drieplaatsig zoals … *ligt tussen* … *en* …; hoewel drie volgens kenners de grootste plaatsigheid is die in de natuur voorkomt, laten we ieder natuurlijk getal toe. In het algemeen gebruiken we præfix-notatie: Rxy, Px e.d.; maar in bijzondere gevallen heeft infix-notatie de voorkeur. Soms verhogen we de leesbaarheid met haakjes: $R(x, y)$ etc.

Operatiesymbolen staan voor operaties. De predikaatlogica is een uitbreiding van de termlogica die behandeld is in deel II.

Van al deze symbolen heeft alleen $\approx$ een vaste, *logische* betekenis. Het symbool $\approx$ staat altijd voor de identiteitsrelatie; $a \approx b$ betelkent dat "a" en "b" naar hetzelfde individu verwijzen. Voor de rest moet de betekenis apart toegelicht worden, door een interpretatie of een theorie.

Uit termen en relatiesymbolen kunnen we *atomaire formules* vormen, zoals $a > b$, $0 \approx 1$, $(x^{-1})^{-1}(x^{-1}x) \approx ((x^{-1})^{-1}x^{-1})x$, enzovoort.

Connectieven, uit de propositielogica. Doordat we nulplaatsige predikaatletters hebben, is de propositielogica letterlijk bevat in de predikaatlogica.

Quantoren. We gebruiken er twee: de *universele* quantor $\forall$, besproken in 13.1, en de *existentiële* quantor $\exists$. Het gebruik van $\exists$ is analoog aan dat van $\forall$: $\exists x$ betekent: 'er is minstens één x waarvoor geldt:'.

Een voorvoegsel als $\forall xy$, $\exists x_0x_2x_5$, etc., bestaande uit een quantor en een rijtje variabelen, zullen we een *quantificatie* noemen.

13.3 *Historische noot*. Als ontdekker van de combinatie van quantoren en variabelen met relaties geldt Gottlob Frege (*Begriffsschrift, eine der arithmetischen nachgebildeten Formelsprache des reinen Denkens*, 1879).

13.4 Voorbeelden

(a) Het syllogisme (3) heeft type A-O-O. Hier is een geldig syllogisme van type A-A-A:

$$\frac{\begin{array}{l}\text{Zoogdieren kunnen verdrinken.}\\ \text{Potvissen zijn zoogdieren.}\end{array}}{\text{Potvissen kunnen verdrinken.}} \tag{13.8}$$

In onze nieuwe notatie wordt dat

$$\frac{\begin{array}{l}\forall x\,(Mx \to Vx)\\ \forall x\,(Px \to Mx)\end{array}}{\forall x\,(Px \to Vx),} \tag{13.8$'$}$$

weer met M voor *mammale*. Dat het schema geldig is, op grond van de betekenis van $\forall$ en $\to$, beredeneren we als volgt: laat y een willekeurige potvis zijn. Uit de premissen hebben we dan $My \to Vy$ en $Py \to My$. Omdat Py gegeven is, volgt met propositielogica Vy. Dus $Py \to Vy$; en omdat y willekeurig is (de aanname Py is ingetrokken), $\forall x\,(Px \to Vx)$.

Merk op dat algemeenheid in (13.8) wordt uitgedrukt door het *ontbreken* van een bepaling, bij *Zoogdieren* en *Potvissen*.

(b) De quantificatie in (13.6) slaat op alle *lijnstukken* x en y. Het komt niet vaak voor dat we echt over *alles* willen praten, het is dan ook nogal onduidelijk wat dat is, en veel predikaten kunnen niet overal zinvol op worden toegepast — was Cleopatra's neus groter dan het getal 1? Quantificatie is daarom steevast gerelateerd aan een 'discussiedomein', de collectie van alle individuen waar we het over hebben.

In Voorbeeld (a) viel dat niet zo op, omdat de quantor telkens met een beperking verbonden is: alle *zoogdieren*, alle *potvissen*. Zulke beperkte quantificatie komt veel voor, en is eenvoudig weer te geven in predikaatlogisch symbolisme. De universele quantor $\forall$ beperkt men als in (13.8$'$): "Alle M …" wordt $\forall x\,(Mx \to \ldots)$. De *existentiële* quantor $\exists$ beperkt men met conjunctie: "Er is een M zo dat …" wordt $\exists x\,(Mx \wedge \ldots)$. Ter illustratie is hier de vertaling van syllogisme (3):

$$\frac{\begin{array}{l}\forall x\,(Kx \to Mx)\\ \exists x\,(Kx \wedge \neg Zx)\end{array}}{\exists x\,(Mx \wedge \neg Zx),} \tag{13.9}$$

(c) Het Nederlands kent vele manieren om algemeenheid uit te drukken. Naast wat we al zijn tegengekomen: iedere, iedereen, iets, sommige, enkele, alle. Voornaamwoorden als *die*, *zij*, *haar*, *hij* spelen de rol van variabelen. De veelheid helpt om dubbelzinnigheid te bestrijden, evenals het plaatsen van komma's en het leggen van klemtonen. De combinatie van quantoren en variabelen is echter veel flexibeler. In principe kunnen quantoren naar believen gestapeld worden zonder dat dubbelzinnigheid ontstaat.

Komma's, klemtoon en fantasie geven van

(13.10) Sommige mensen hebben honden die niet naar hun baas luisteren.

de volgende vier predikaatlogische lezingen, met M voor Mens, Hxy voor x Heeft y, C voor hond (*Canis*), Lxy voor x Luistert naar y en B voor de Baas van:

(i) $\exists x\,(Mx \wedge \exists y\,(Cy \wedge Hxy \wedge \neg Lyx))$

(ii) $\exists x\,(Mx \wedge \exists y\,(Cy \wedge Hxy \wedge \neg L(y, B(x)))$

(iii) $\exists x\,(Mx \wedge \exists y\,(Cy \wedge Hxy) \wedge \neg L(x, B(x))$

(iv) $\exists x\,(Mx \wedge \exists y\,(Cy \wedge Hxy)) \wedge \forall x\,(Cx \rightarrow \neg L(x, B(x))$

Oefeningen bij §13:

13:1 Laat het discussiedomein bestaan uit alle mensen; lees Mx als "x is van het mannelijk geslacht", Vx als "x is van het vrouwelijk geslacht", en Oxy als "x is een ouder van y".

(a) Ga van de volgende formules na of ze (nagenoeg[12]) waar zijn.
(i) $\forall x\,\exists y\,(My \wedge Oyx)$;
(ii) $\exists x\,(Mx \wedge \forall y\,Oxy)$;
(iii) $\forall xy\,(Oxy \rightarrow \forall z\,(Oyz \rightarrow Oxz))$;
(iv) $\exists x\,(Vx \wedge \forall y\,(Oxy \rightarrow Vy))$.

(b) Vertaal in Nederlandse zinnen:
(i) $\forall x\,\neg Oxx$;
(ii) $\forall x\,\exists y\,(Oyx \wedge \neg My)$;
(iii) $\forall x\,(Vx \leftrightarrow \neg Mx)$;
(iv) $\forall x\,\exists y\,(Oyx \wedge \forall z\,(Oyz \rightarrow z \approx x))$;
(v) $\forall x_0 \exists x_1 x_2 (Ox_1x_0 \wedge \exists x_3 (Ox_3x_1 \wedge Ox_3x_2) \wedge Vx_2)$.

(c) Construeer formules die uitdrukken:
(i) Iedereen heeft een grootmoeder.
(ii) Iedereen heeft minstens twee grootmoeders. [Gebruik $\approx$.]
(iii) Iedere vrouw heeft een (half-)zuster.
(iv) Iedere man heeft een volle zuster.

13:2 Neem als discussiedomein de verzameling $\mathbb{Z}$ der gehele getallen, en beschouw de relatie $<$ op $\mathbb{Z}$. Construeer formules die uitdrukken:
(i) $<$ is transitief;
(ii) er is geen grootste en geen kleinste getal;
(iii) $<$ is asymmetrisch (i.e. de relatie is nooit wederzijds);
(iv) elk getal heeft een onmiddellijke opvolger en een onmiddellijke voorganger.

13:3 Vertaal (13.2) in een formule, en leg uit waarom die logisch waar is.

13:4 Neem als discussiedomein de verzameling $\mathbb{N}$ der natuurlijke getallen, en beschouw de operaties + (optelling) en $\cdot$ (vermenigvuldiging) op $\mathbb{N}$. In de corresponderende predikaatlogische taal bestaat een formule die uitdrukt dat een getal x even is: namelijk, $\exists y\,(y + y \approx x)$. Construeer zelf zulke formules voor $x \leq y$, $x = 1$, $x \mid y$ (x is een deler van y) en x *is priem*. Gebruik ze om uit te drukken:
(i) Er is een kleinste getal.
(ii) Er is een precies één kleinste getal. [Gebruik $\approx$.]

[12] Dode mensen doen ook mee; we zien daarbij af van problemen als gemeenschappelijke voorouders met chimpansees.

(iii) Er is geen grootste priemgetal.
(iv) Elk even getal groter dan 2 is de som van twee priemgetallen.

13:5 Formaliseer het volgende syllogisme:

Elke kauw is zwart.
Elke kauw is een vogel.
―――――――――――――
Minstens één vogel is zwart.

Is het geldig? Waarom?

13:6 (Russell) Formaliseer de redenering

Onze barbier scheert alle dorpsbewoners die zichzelf niet scheren, en verder niemand. Dus onze barbier woont niet in ons dorp.

Is is ze geldig? Waarom?

§14 Predikaatlogische talen

In deze en de volgende § zullen we de informele beschouwingen van §13 in een exacte vorm gieten. De opzet is in grote lijnen dezelfde als in de §§ 2 en 3.

14.1 Vocabulaires. Een *vocabulaire*, of *type*, is een verzameling $\mathcal{L}$ van relatie- en operatiesymbolen, elk met een vaste plaatsigheid.

14.2 Voorbeelden
(a) De operationele typen zoals gedefinieerd in §7.1.
(b) Het vocabulaire van (13.7) is $\{>, \equiv\}$, als we a en b als variabelen opvatten; zijn het constantesymbolen, dan is het vocabulaire $\{>, \equiv, a, b\}$. In het eerste geval bevat het type uitsluitend relatiesymbolen, we spreken dan van een *relationeel type*.

14.3 Elk vocabulaire $\mathcal{L}$ bepaalt een predikaatlogische taal. De formules van al zulke talen worden op dezelfde manier gevormd uit de *niet-logische* symbolen van het vocabulaire en de volgende logische en hulpsymbolen, die geacht worden *niet* tot het vocabulaire te behoren:

— de *individuele variabelen*, $v_0, v_1, v_2, \ldots$;
— het *gelijkheidssymbool* $\approx$;
— de *connectieven* $\top, \bot, \neg, \wedge, \vee, \rightarrow, \leftrightarrow$;
— de *quantoren* $\forall$ en $\exists$;
— en haakjes), (.

14.4 Termen. De operatiesymbolen van een vocabulaire $\mathcal{L}$ vormen samen een operationeel vocabulaire $Op_{\mathcal{L}}$, het *operationele subvocabulaire* van $\mathcal{L}$. De *termen* van $\mathcal{L}$ zijn de termen over $Op_{\mathcal{L}}$, zoals gedefinieerd in §7.7.

We gaan ervan uit dat termen uniek leesbaar zijn; bovendien, dat ze evenveel linkerhaakjes bevatten als rechterhaakjes, en dat een beginsegment van een term nooit een term is, en altijd minstens zoveel linkerhaakjes bevat als rechterhaakjes.

14.5 Atomaire formules. Zij $\mathcal{L}$ een vocabulaire. De *atomaire formules* van $\mathcal{L}$ zijn de elementen van de kleinste verzameling X die voldoet aan
(a) als $R \in \mathcal{L} \cup \{\approx\}$ een tweeplaatsige infix-predikaatletter is, en $\mathbf{s}$ en $\mathbf{t}$ zijn termen van $\mathcal{L}$, dan $(\mathbf{s}\ R\ \mathbf{t}) \in X$;

(b) als $R \in \mathcal{L}$ een n-plaatsige predikaatletter is ($n \in \mathbb{N}$), en $\mathbf{t}_1,\ldots, \mathbf{t}_n$ zijn termen van $\mathcal{L}$, dan $R\mathbf{t}_1\ldots\mathbf{t}_n \in X$.

Uit de definitie en de eigenschappen van termen volgt direct:

❀ **14.5.1 Lemma**. (a) Een atomaire formule bevat evenveel linkerhaakjes als rechterhaakjes.
(b) Een beginstuk van een atomaire formule bevat niet meer rechterhaakjes dan linkerhaakjes.

❀ **14.5.2 Lemma**. Een echt beginstuk van een atomaire formule is geen atomaire formule.

Bewijs. Laat α een echt beginstuk zijn van een atomaire formule β. Het lege rijtje is geen atomaire formule; we kunnen dus aannemen dat α niet leeg is. Er zijn twee gevallen.
(a) $\beta = (\mathbf{s}\ R\ \mathbf{t})$, met $\mathbf{s}$ en $\mathbf{t}$ termen, en R een tweeplaatsige infix-predikaatletter. Als α een beginstuk is van $(\mathbf{s}\ R\ \mathbf{t}$, dan bevat α meer linkerhaakjes dan rechter, en dan is α dus geen atomaire formule.
(b) $\beta = R\mathbf{t}_1\ldots\mathbf{t}_n$, met $\mathbf{t}_1,\ldots, \mathbf{t}_n$ termen, en R een n-plaatsige predikaatletter. Als α een echt beginstuk is van β, dan bevat α niet genoeg complete termen. ☒

Voor het bewijs is van wezenlijk belang dat we relatie- en operatiesymbolen uit elkaar kunnen houden, en dat je de plaatsigheid aan het symbool kunt aflezen.

14.6 Formules. Zij $\mathcal{L}$ een vocabulaire. De verzameling $\mathrm{F}_{\mathcal{L}}$ der *formules* van (of over) $\mathcal{L}$ is de kleinste verzameling X die
(a) de atomaire formules van $\mathcal{L}$ bevat; en (b) voldoet aan
(i) $\top, \bot \in X$;
(ii) als $\varphi \in X$, dan $\neg\varphi \in X$;
(iii) als $\circ$ een tweeplaatsig connectief is, en $\varphi, \psi \in X$, dan $(\varphi \circ \psi) \in X$;
(iv) als $\varphi \in X$ en x is een variabele, dan $\forall x\, \varphi, \exists x\, \varphi \in X$.

Subclausule (iv) houdt slechts rekening met quantificaties over één variabele. De langere zullen we als afkorting beschouwen: $\forall xy$ is eigenlijk $\forall x \forall y$, enzovoort.

❀ **14.6.1 Lemma**. (a) Een formule bevat evenveel linkerhaakjes als rechterhaakjes.
(b) Een beginstuk van een formule bevat niet meer rechterhaakjes dan linkerhaakjes.

Bewijs. Inductie naar de lengte van de formule. Voor atomaire formules gelden (a) en (b) volgens Lemma .5.1. De nulplaatsige connectieven bevatten helemaal geen haakjes, en voor $\neg\varphi$, $\forall x\, \varphi$ en $\exists x\, \varphi$ volgen (a) en (b) direct uit de overeenkomstige beweringen voor φ.

Zij tenslotte $\circ$ een tweeplaatsig connectief. Als φ en ψ evenveel linkerhaakjes als rechterhaakjes bevatten, dan bevat ook $(\varphi \circ \psi)$ evenveel linkerhaakjes als rechterhaakjes. En aangezien een beginstuk van $\varphi \circ \psi$ al niet meer rechterhaakjes dan linkerhaakjes bevat, zal een beginstuk van $(\varphi \circ \psi)$ evenmin meer rechterhaakjes dan linkerhaakjes bevatten. ☒

❀ **14.6.2 Lemma**. Een echt beginstuk van een formule is geen formule.

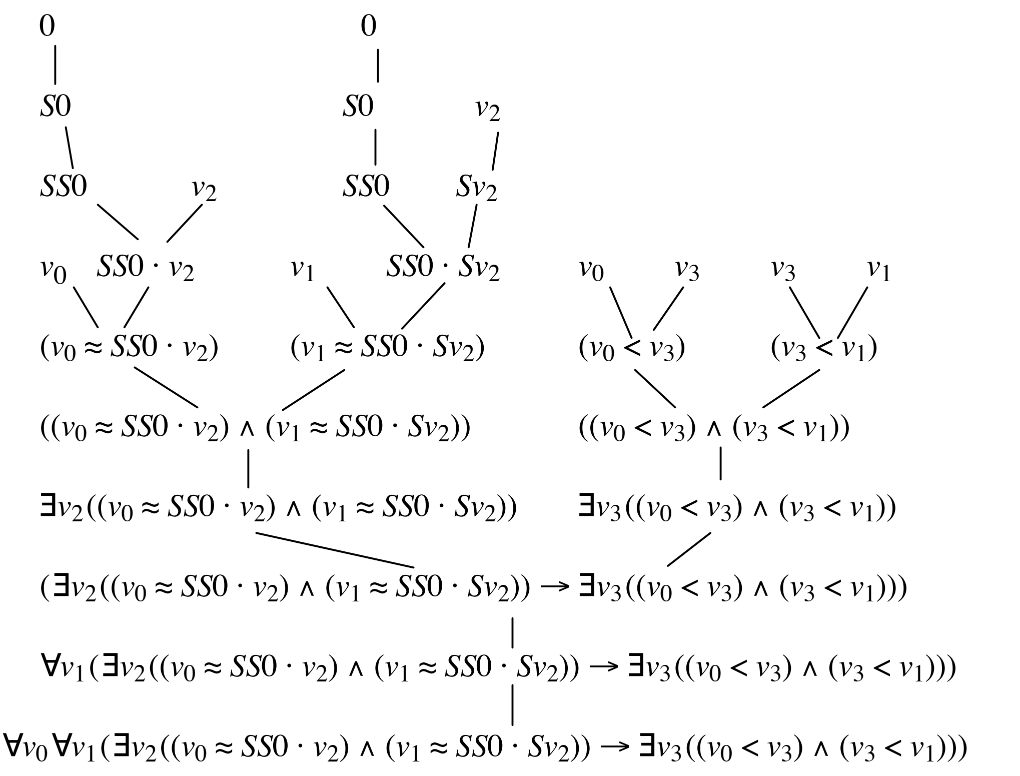
Bewijs. Laat α een echt beginstuk zijn van een formule φ. Het lege rijtje is geen formule; we kunnen dus aannemen dat α niet leeg is. We gebruiken inductie naar de lengte van φ.
(a) Als φ atomair is, dan is α volgens Lemma .5.2 in elk geval geen atomaire formule. Maar α is zeker geen niet-atomaire formule, want α bevat geen connectieven of quantoren.
(b) (i) Het enige echte beginstuk van $\top$ en $\bot$ is leeg.
(ii) Een niet-leeg echt beginstuk van een formule $\neg\varphi$ is van de vorm $\neg\beta$, met β een echt beginstuk van φ. Volgens inductiehypothese, $\beta \notin \mathrm{F}_{\mathcal{L}}$. Dan ook $\neg\beta \notin \mathrm{F}_{\mathcal{L}}$: want als $\neg\beta \in \mathrm{F}_{\mathcal{L}}$, dan zou de verzameling $X = \mathrm{F}_{\mathcal{L}} - \{\neg\beta\}$ voldoen aan de voorwaarden (a) en (b) van de definitie van formules, wat in strijd is met het gegeven dat $\mathrm{F}_{\mathcal{L}}$ de *kleinste* verzameling is die daaraan voldoet.
(iii) Zij $\circ$ een tweeplaatsig connectief. Een niet-leeg echt beginstuk van een formule $(\varphi \circ \psi)$ bevat meer linkerhaakjes dan rechterhaakjes, en is dus geen formule.
(iv) Een niet-leeg echt beginstuk van een formule $\mathrm{Q}x\,\varphi$, met $\mathrm{Q} \in \{\forall, \exists\}$, is ofwel Q, of van de vorm $\mathrm{Q}x\,\beta$, met β een echt beginstuk van φ. Een quantor alleen is zeker geen formule; en omdat (volgens inductiehypothese) β geen formule is, is $\mathrm{Q}x\,\beta$ ook geen formule. (Redeneer als bij (ii).) ⊠

Een bewijs dat een rijtje symbolen een term, atomaire formule, of formule is, over een predikaatlogisch vocabulaire $\mathcal{L}$, vormt net als in het geval van formules van de propositielogica (§2) een *constructieboom*.

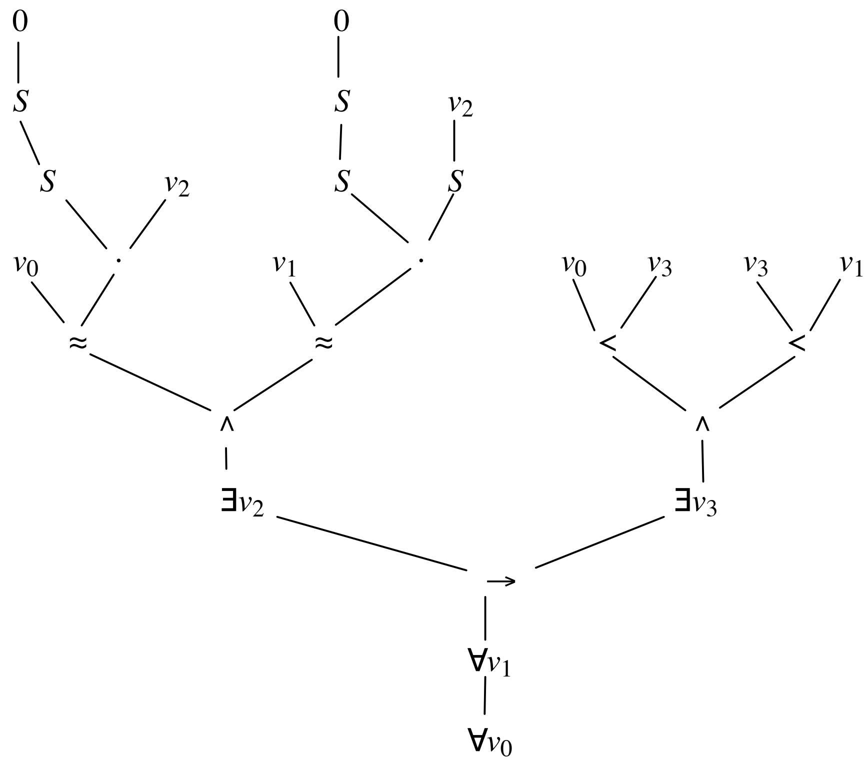
14.6.3 Voorbeeld. De constructieboom voor

$$\forall v_0 \forall v_1 (\exists v_2((v_0 \approx SS0 \cdot v_2) \wedge (v_1 \approx SS0 \cdot Sv_2)) \rightarrow \exists v_3((v_0 < v_3) \wedge (v_3 < v_1)))$$

ziet er zo uit:



of vereenvoudigd:



14:1 Oefening. Schets constructiebomen voor:

(i) $\forall v_0 \exists v_1 (Mv_1 \wedge Ov_1v_0)$;

(ii) $\exists v_0(\exists v_1 (Cv_1 \wedge Hv_0v_1) \wedge \neg Lv_0Bv_0)$;

(iii) $\forall v_0((v_0 > Fa) \to \exists v_1 ((v_0 > v_1) \wedge (v_0 > Fa)))$;

(iv) $\neg \forall v_0 \forall v_1((v_0 > v_1) \to (FFv_0 > Fv_1))$;

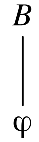
(v) $\forall v_0 \forall v_1(((v_0 \approx SS0 \cdot v_1) \wedge \exists v_2 (v_0 \approx v_2 \cdot v_2)) \to \exists v_2 (v_1 \approx SS0 \cdot v_2))$.

❀ **14.7 Stelling** (*unieke leesbaarheid*). Zij $\mathcal{L}$ een vocabulaire. Een formule van $\mathcal{L}$ heeft slechts één constructieboom.

Bewijs. Laat φ een formule zijn van $\mathcal{L}$. We doen inductie naar de lengte van φ.

Als φ een atomaire formule is, dan bevat φ geen connectieven of quantoren. Bijgevolg kan φ alleen een *atomaire* formule zijn. Per definitie is φ dan van de vorm $(\mathbf{s}\ R\ \mathbf{t})$, met $R \in \mathcal{L}$ een tweeplaatsige infix-predikaatletter, en $\mathbf{s}$ en $\mathbf{t}$ termen van $\mathcal{L}$, of van de vorm $R\mathbf{t}_1 \ldots \mathbf{t}_n$, met $R \in \mathcal{L}$ een n-plaatsige predikaatletter ($n \in \mathbb{N}$), en $\mathbf{t}_1, \ldots, \mathbf{t}_n$ termen van $\mathcal{L}$. Die mogelijkheden sluiten elkaar uit, want $\mathcal{L}$ bevat geen haakjes. Unieke leesbaarheid volgt nu uit de unieke leesbaarheid van termen.

Als $\varphi \in \{\bot, \top\}$, dan is er geen twijfel mogelijk. Als φ begint met een negatieteken, zeg $\varphi = \neg\psi$, of een quantificatie, zodat $\varphi = \forall x \psi$ of $\varphi = \exists x \psi$, dan is een constructieboom voor φ noodzakelijkerwijs van de vorm



met B een constructieboom voor ψ; B is uniek volgens inductieveronderstelling.

Als φ begint met een haakje, dan is φ van de vorm $(\psi \circ \chi)$, voor een of ander tweeplaatsig connectief $\circ$, en

$$\begin{tikzcd}[column sep=small] B_\psi \arrow[dr, no head] & & B_\chi \arrow[dl, no head] \\ & \varphi & \end{tikzcd}$$

met B_ψ en B_χ constructiebomen voor respectievelijk ψ en χ, een constructieboom voor φ. Volgens inductieveronderstelling zijn B_ψ en B_χ uniek. Een andere constructieboom vereist dus dat φ ook gezien kan worden als $(\psi' * \chi')$, met andere formules ψ' en χ', en een tweeplaatsig connectief $*$. Maar dat is onmogelijk; want dan moet ψ' een echt beginstuk zijn van ψ, of ψ een echt beginstuk van ψ'; en volgens Lemma .6.2 is één van beide dan geen formule. ⊠

Terminologie. De formules die voorkomen in de constructieboom van een formule φ heten de *subformules* van φ. Het *bereik* van een voorkomen van een quantificatie in φ is het subformulevoorkomen onmiddellijk volgend op dat quantificatievoorkomen.

Voorbeelden. Het bereik van $\exists v_1$ in formule (i) van Oefening 1 is

$$(Mv_1 \wedge Ov_1v_0);$$

in formule (ii), $(Cv_1 \wedge Hv_0v_1)$. Het bereik van het eerste voorkomen van $\exists v_2$ in formule (v) is $(v_0 \approx v_2 \cdot v_2))$, dat van het tweede voorkomen $(v_1 \approx SS0 \cdot v_2))$.

Terwille van de Unieke Leesbaarheidsstelling hebben we onze formules rijkelijk bezaaid met haakjes. In de praktijk (zie §13) kunnen we met veel minder toe dan de definitie eist. In het vervolg laten we haakjes weg volgens de conventies van §3. Haakjes om atomaire formules kunnen ook weggelaten worden. Aan de andere kant is $R(\mathbf{t}_1,\ldots, \mathbf{t}_n)$ soms duidelijker dan $R\mathbf{t}_1\ldots\mathbf{t}_n$. De *eis* dat unieke leesbaarheid gewaarborgd is, geldt onverkort.

We zullen ook, voor het gemak, in algemene beschouwingen abstraheren van de positie van niet-logische symbolen in relatie tot hun argumenten — door altijd præfix-notatie te gebruiken. Zoals we met '2 + 2' het getal 4 kunnen aanduiden, zo kan '$Q\mathbf{t}_1\mathbf{t}_2$' een geschikte benaming zijn van 2 + 2, of '$R\mathbf{t}_1\mathbf{t}_2$' voor $\mathbf{t}_1 \leq \mathbf{t}_2$.

Verdere Oefeningen bij §14:

14:2 (Poolse notatie). Haakjes zijn zelfs geheel overbodig, als de syntax maar streng is. Laat weer $\mathcal{L}$ een vocabulaire zijn, bestaande uit relatie- en operatiesymbolen van vaste plaatsigheid. Definieer de termen van $\mathcal{L}$ als de kleinste verzameling T die Var omvat en voldoet aan

$$\text{als } \mathbf{t}_1,\ldots, \mathbf{t}_n \in T, \text{ dan } Q\mathbf{t}_1\ldots\mathbf{t}_n \in T,$$

voor alle $n \in \mathbb{N}$ en elk n-plaatsig operatiesymbool $Q \in \mathcal{L}$; de atomaire formules van $\mathcal{L}$ als de kleinste verzameling A die voldoet aan

$$\text{als } \mathbf{t}_1,\ldots, \mathbf{t}_k \text{ termen zijn van } \mathcal{L}, \text{ dan } R\mathbf{t}_1\ldots\mathbf{t}_k \in A,$$

voor alle $k \in \mathbb{N}$ en elk k-plaatsig relatiesymbool $R \in \mathcal{L} \cup \{\approx\}$; en de formules van $\mathcal{L}$ als de kleinste verzameling F die de atomaire formules bevat, en voldoet aan

$$\text{als } \varphi_1,\ldots,\varphi_m \in F, \text{ dan } C\varphi_1\ldots\varphi_m \in F,$$

voor elk m-plaatsig connectief C ($m = 0, 1, 2$), en aan

$$\text{als } \varphi \in F \text{ en } x \in \mathrm{Var}, \text{ dan } \forall x\varphi, \exists x\varphi \in F.$$

a) Schrijf de formules op in Poolse Notatie die corresponderen met de formules in Oefening 1.
b) Onderzoek of de volgende uitdukkingen formules zijn in de Poolse notatie, over het vocabulaire bestaande uit een éénplaatsig relatiesymbool M, een tweeplaatsig relatiesymbool G, en een éénplaatsig operatiesymbool B:
(i) $\neg\rightarrow Gv_1Bv_0\forall v_0\exists v_1Mv_1$;
(ii) $\forall v_0\forall v_1 v_0GBBv_1$;
(iii) $\neg\forall v_0\forall v_1\rightarrow\wedge\leftrightarrow Mv_0\neg Mv_0\neg\approx v_1v_0MBv_1$;
(iv) $\neg\rightarrow\exists v_2\top Mv_2\wedge\neg Gv_3\neg Gv_3v_0$.

Laat nu a en b twee incommensurabelen zijn (zeg, appels en beren). Geef de symbolen gewichten:
variabelen hebben gewicht $-a$;
quantoren hebben gewicht a;
een k-plaatsig operatiesymbool heeft gewicht $(k-1)a$;
een n-plaatsig relatiesymbool heeft gewicht $na - b$;
een m-plaatsig connectief heeft gewicht $(m-1)b$.

Definieer de gewichtsfunctie σ op uitdrukkingen (rijtjes van symbolen) α als volgt:
(i) $\sigma(\alpha)$ is het gewicht van s als α bestaat uit één voorkomen van één symbool s;
(ii) zij ε het lege rijtje: $\sigma(\varepsilon) = 0$;
(iii) $\sigma(\alpha\beta) = \sigma(\alpha) + \sigma(\beta)$.
Als $\sigma(\alpha) = ma + nb$, met $m, n \in \mathbb{Z}$, dan $\sigma_a(\alpha) = m$, $\sigma_b(\alpha) = n$.

We verdelen de symbolen in twee groepen: *termsymbolen* zijn de variabelen en de operatiesymbolen; de relatiesymbolen, connectieven en quantoren zijn *propositiesymbolen*.
c) Bewijs dat een niet-lege uitdrukking τ die geheel bestaat uit termsymbolen een term is dan en slechts dan als 1° voor elk echt beginstuk υ van τ, $\sigma_a(\upsilon) \geq 0$, en 2° $\sigma(\tau) = -a$. [Cf. 2:3(d).]
d) Bewijs dat een uitdrukking α een formule is in Poolse notatie dan en slechts dan als
1° $\sigma(\alpha) = -b$.
2° als $\alpha = \beta s\gamma$, voor een symbool s, dan $\sigma_a(\beta s) \geq 0$, en s is een propositiesymbool dan en slechts dan als $\sigma_a(\beta) = 0$;
3° als $\alpha = \beta s\gamma$, voor een propositiesymbool s, dan $\sigma_b(\beta) \geq 0$;
4° elk quantorvoorkomen in α direct gevolgd wordt door een variabele.
[$\Rightarrow$: inductie over formules; $\Leftarrow$: inductie naar de lengte van de uitdrukking.]
e) Uit (d) volgt unieke leesbaarheid van formules in Poolse notatie. Waarom?

14:3 Dat de materiële implicatie de betekenis van "als … dan …" uitdrukt, is aanvechtbaar. Met quantoren kunnen we een meer acceptabele formalisering bereiken. Redenering (4.1), bijvoorbeeld, kunnen we weergeven als:

$$\begin{array}{l} \forall x\,(Zx \to \neg(Rx \vee Sx)) \\ \underline{Rh\qquad\qquad\quad} \\ \neg Zh \end{array}$$

met als discussiedomein *tijdstippen*, Zx voor 'de zon schijnt op x', etc., en h voor *heden*.
(a) Geef zelf zo'n vertaling voor (4.4),

Als het regent, schijnt de zon niet. De zon schijnt niet. Dus het regent.

(b) Vertaal ook in predikaatlogische formules:
(i) Honden die blaffen, bijten niet; maar elke hond blaft weleens niet.
(ii) (A. Lincoln) You may fool all the people some of the time, you can even fool some of the people all of the time, but you cannot fool all of the people all the time.

§15 De semantiek van de predikaatlogica

Om aan predikaatlogische formules over een gegeven vocabulaire $\mathcal{L}$ een waarheidswaarde toe te kennen, hebben we drie soorten informatie nodig.
—Ten eerste moeten we weten wat *alles* is: daaruit volgt dan wat quantificatie betekent. We hebben een verzameling nodig, het *universum*, dat alle dingen bevat waar we het over willen hebben.
—Ten tweede moeten we weten wat de symbolen in $\mathcal{L}$ betekenen. We hebben een *interpretatie* nodig, die ieder relatiesymbool in $\mathcal{L}$ verbindt met een relatie op A, en ieder operatiesymbool met een operatie op A, met inachtneming van de voorgeschreven plaatsigheid.
—Ten derde moeten we er rekening mee houden dat niet alle variabelen geregeerd worden door een quantor. Zulke 'vrije' variabelen vertegenwoordigen elementen van het universum; welke, dat wordt bepaald door een *bedeling*, een aanvulling *ad hoc* op de interpretatie. Bedelingen zijn gedefinieerd in 7.12.

15.1 Structuren. Laat $\mathcal{L}$ een vocabulaire zijn. Een *structuur* voor $\mathcal{L}$ is een paar $\mathbf{A} = \langle A, I\rangle$ van een niet-lege verzameling A, het universum of *domein* van $\mathbf{A}$, en een functie I op $\mathcal{L}$, de interpretatie, die voor elke n
— aan elke n-plaatsige predikaatletter $P \in \mathcal{L}$ een relatie $I(P) \subseteq A^n$ toekent;
— en aan elk n-plaatsig operatiesymbool $Q \in \mathcal{L}$ een functie $I(Q)$ van A^n naar A.

We kunnen structuren ook beschrijven als rijtjes bestaande uit een universum en een aantal relaties en operaties, wanneer we, bijvoorbeeld door de volgorde, weten welk element van het rijtje met welk symbool correspondeert; zoals uitgelegd aan de hand van de algebra **W** in Voorbeeld 7.4(ia).

15.2 Voorbeelden
(i) Als het vocabulaire $\mathcal{L}$ operationeel is, dan is een structuur voor $\mathcal{L}$ een algebra van type $\mathcal{L}$. In het algemeen is het *operationele reduct* $\langle A, I{\restriction}Op_{\mathcal{L}}\rangle$ van een $\mathcal{L}$-structuur $\langle A, I\rangle$ een algebra.
(ii) Aan de andere kant zijn $\langle \mathbb{Z}, <\rangle$, $\langle \mathbb{N}, \leq\rangle$ en $\langle \mathcal{P}\mathbb{N}, \subseteq\rangle$ *relationele* structuren.

Een bedeling in een structuur **A**, of in het universum A van **A**, is een functie van de variabelen naar A. In §7.12 is beschreven hoe een bedeling de betekenis van termen bepaalt. De algebra $\mathbf{T}_{Op_{\mathcal{L}}}(\mathrm{Var})$ der $\mathcal{L}$-termen noteren we ook, wat korter, als $\mathbf{T}_{\mathcal{L}}(\mathrm{Var})$.

15.3 Laat $\boldsymbol{b}$ een bedeling zijn in een verzameling A, x een variabele, en $a \in A$. Dan is $\boldsymbol{b}(a/x)$ de bedeling $\boldsymbol{a}$ gedefinieerd door

$$\boldsymbol{a}(v_i) = \begin{cases} a \text{ als } v_i = x, \\ \boldsymbol{b}(v_i) \text{ als } v_i \neq x. \end{cases}$$

15:1 Oefening. Ga na dat

(a) $\boldsymbol{b}(a_2/x)(a_1/x) = \boldsymbol{b}(a_1/x)$;

(b) als $x_1 \neq x_2$, dan $\boldsymbol{b}(a_2/x_2)(a_1/x_1) = \boldsymbol{b}(a_1/x_1)(a_2/x_2)$.

In de onderstaande definitie gebruiken we de met de connectieven corresponderende (en met hetzelfde teken aangeduide) waarheidsfuncties die in §1 zijn gedefinieerd. Bovendien hebben we de herhaalde conjunctie en disjunctie nodig die geïntroduceerd zijn in 3.8, maar in een wezenlijk algemenere vorm: als $f\colon M \longrightarrow \{0, 1\}$ een toekenning is van waarheidswaarden aan de elementen van een (mogelijk oneindige) verzameling M, dan is

$$\bigwedge_{m \in M} f(m) = \begin{cases} 1 \text{ als } f(m) = 1 \text{ voor alle } m \in M, \\ 0 \text{ als er een } m \in M \text{ bestaat zo dat } f(m) = 0; \end{cases}$$

$$\bigvee_{m \in M} f(m) = \begin{cases} 1 \text{ als er een } m \in M \text{ bestaat zo dat } f(m) = 1, \\ 0 \text{ als } f(m) = 0 \text{ voor alle } m \in M. \end{cases}$$

15.4 Lemma (gegeneraliseerde De Morgan-wet). Zij $f\colon M \longrightarrow \{0, 1\}$ een toekenning van waarheidswaarden. Dan

$$\neg \bigwedge_{m \in M} f(m) = \bigvee_{m \in M} \neg f(m)$$

Bewijs. Als $\neg\bigwedge f(m) = 1$, dan $\bigwedge f(m) = 0$, dus voor zekere $m_0 \in M$, $f(m_0) = 0$. Dan $\neg f(m_0) = 1$, dus $\bigvee \neg f(m) = 1$.

Als $\neg\bigwedge f(m) = 0$, dan $\bigwedge f(m) = 1$, dus voor alle $m \in M$, $f(m) = 1$. Dan $\neg f(m) = 0$, dus $\bigvee \neg f(m) = 0$. ⊠

15.5 Definitie. Zij $\mathcal{L}$ een vocabulaire, $\mathbf{A} = \langle A, I \rangle$ een structuur voor $\mathcal{L}$, φ een formule van $\mathcal{L}$, en $\boldsymbol{b}$ een bedeling in $\mathbf{A}$. Dan definiëren we de waarheidswaarde $\varphi^{\mathbf{A}}[\boldsymbol{b}]$ van φ in $\mathbf{A}$ onder $\boldsymbol{b}$ als volgt:

(i) Als φ een vergelijking is, dan $\varphi^{\mathbf{A}}[\boldsymbol{b}] = 1$ als φ vervuld wordt door $\boldsymbol{b}$, en anders $\varphi^{\mathbf{A}}[\boldsymbol{b}] = 0$.

(ii) Als $\varphi = P\mathbf{t}_1 \ldots \mathbf{t}_n$, voor een n-plaatsig relatiesymbool $P \in \mathcal{L}$, dan $\varphi^{\mathbf{A}}[\boldsymbol{b}] = 1$ als $\langle \mathbf{t}_1^{\mathbf{A}}[\boldsymbol{b}], \ldots, \mathbf{t}_n^{\mathbf{A}}[\boldsymbol{b}] \rangle \in I(P)$, en anders $\varphi^{\mathbf{A}}[\boldsymbol{b}] = 0$.

(iii) $\bot^{\mathbf{A}}[\boldsymbol{b}] = 0$ en $\top^{\mathbf{A}}[\boldsymbol{b}] = 1$.

(iv) Als $\varphi = \neg\psi$, dan $\varphi^{\mathbf{A}}[\boldsymbol{b}] = \neg(\psi^{\mathbf{A}}[\boldsymbol{b}])$.

(v) Als $\varphi = (\psi \circ \chi)$, voor een tweeplaatsig connectief $\circ$, dan $\varphi^{\mathbf{A}}[\boldsymbol{b}] = \psi^{\mathbf{A}}[\boldsymbol{b}] \circ \chi^{\mathbf{A}}[\boldsymbol{b}]$.

(vi) Als $\varphi = \forall x\psi$, dan $\varphi^{\mathbf{A}}[\boldsymbol{b}] = \bigwedge_{a \in A} \psi^{\mathbf{A}}[\boldsymbol{b}(a/x)]$.

(vii) Als $\varphi = \exists x\psi$, dan $\varphi^{\mathbf{A}}[\boldsymbol{b}] = \bigvee_{a \in A} \psi^{\mathbf{A}}[\boldsymbol{b}(a/x)]$.

Net als in Definitie 8.1 kunnen we de bedeling beperken tot de eerste k variabelen. In eerste instantie (zie overigens het eind van 15.10 voor een heilzame conventie) is daarbij enige voorzichtigheid geboden. We veronderstellen dat φ geen andere variabelen bevat dan $v_0,\ldots, v_{k-1}$. We krijgen dan, voor $\overline{a} = a_0,\ldots, a_{k-1}$:

(i′) $(\mathbf{t}_1 \approx \mathbf{t}_2)^{\mathbf{A}}[\overline{a}] = 1$ als $\mathbf{t}_1^{\mathbf{A}}[\overline{a}] = \mathbf{t}_2^{\mathbf{A}}[\overline{a}]$, en anders 0.

(ii′) $(P\mathbf{t}_1\ldots\mathbf{t}_n)^{\mathbf{A}}[\overline{a}] = 1$ als $\langle \mathbf{t}_1^{\mathbf{A}}[\overline{a}],\ldots, \mathbf{t}_n^{\mathbf{A}}[\overline{a}]\rangle \in I(P)$, en anders 0.

(iii′)-(v′) $\perp^{\mathbf{A}}[\overline{a}] = 0$, enzovoort.

(vi′) $(\forall v_i\psi)^{\mathbf{A}}[a_0\ldots a_{k-1}] = \bigwedge_{a\in A} \psi^{\mathbf{A}}[a_0\ldots a_{i-1}aa_{i+1}\ldots a_{k-1}]$.

(vii′) $(\exists v_i\psi)^{\mathbf{A}}[a_0\ldots a_{k-1}] = \bigvee_{a\in A} \psi^{\mathbf{A}}[a_0\ldots a_{i-1}aa_{i+1}\ldots a_{k-1}]$.

De notatie $a_0\ldots a_{i-1}aa_{i+1}\ldots a_{k-1}$ moet ruim worden opgevat: als $i = 0$, bijvoorbeeld, leze men $aa_1\ldots a_{k-1}$.

15.6 Het gebruik van bovenstaande definitie kan soms vereenvoudigd worden door beperking tot de connectieven in een geschikt functioneel volledig stelsel. In een dergelijk geval kan ook bezuinigd worden op quantoren.

Propositie. Laat x een variabele zijn, φ een formule, **A** een structuur voor de taal van φ, en $\boldsymbol{b}$ een bedeling in **A**. Dan

(i) $(\forall x\varphi)^{\mathbf{A}}[\boldsymbol{b}] = (\neg\exists x\neg\varphi)^{\mathbf{A}}[\boldsymbol{b}]$;

(ii) $(\exists x\varphi)^{\mathbf{A}}[\boldsymbol{b}] = (\neg\forall x\neg\varphi)^{\mathbf{A}}[\boldsymbol{b}]$.

Bewijs. (i) Volgens Definitie 5 en Lemma 4,

$$(\forall x\varphi)^{\mathbf{A}}[\boldsymbol{b}] = \bigwedge_{a\in A} \varphi^{\mathbf{A}}[\boldsymbol{b}(a/x)] = \neg\neg\bigwedge_{a\in A} \varphi^{\mathbf{A}}[\boldsymbol{b}(a/x)] = \neg\bigvee_{a\in A} \neg\varphi^{\mathbf{A}}[\boldsymbol{b}(a/x)]$$
$$= \neg\bigvee_{a\in A} (\neg\varphi)^{\mathbf{A}}[\boldsymbol{b}(a/x)] = \neg(\exists x\neg\varphi)^{\mathbf{A}}[\boldsymbol{b}] = (\neg\exists x\neg\varphi)^{\mathbf{A}}[\boldsymbol{b}].$$

(ii) Analoog. ⊠

15:2 Oefening. Voer het bewijs van onderdeel (ii) uit.

De interpretatie van een niet-logisch symbool S in een structuur $\mathbf{A} = \langle A, I\rangle$ noteren we, wanneer dat zo uitkomt, als $S^{\mathbf{A}}$, in plaats van $I(S)$. (Cf. §7.) Verder schrijven we in plaats van

$$\langle a_1,\ldots, a_n\rangle \in P^{\mathbf{A}}$$

soms: $P^{\mathbf{A}}(a_1,\ldots, a_n)$.

15.7 *Vrij en gebonden voorkomen van variabelen*. Er zijn drie soorten contexten waarin een variabele x in een formule kan voorkomen:

1° onmiddellijk volgend op een quantor, als deel van een quantificatie;

2° binnen het bereik van een quantificatie Qx;

3° elders.

Alleen in het laatste geval verwijst x naar een individu in het domein; welk, dat bepaalt de bedeling. Een dergelijk voorkomen van x noemen we *vrij*. Een voorkomen van de tweede soort is *gebonden*, door de quantificatie Qx. Een voorkomen van de eerste soort zouden we *bindend* kunnen noemen. Dus bijvoorbeeld: in

$$\forall x(\forall xAx \vee Cx) \wedge Bx$$

zijn de eerste twee voorkomens van x bindend, en het derde en het vierde gebonden, en is het vijfde vrij. Merk op dat we strict genomen moeten spreken van binding van een variabelevoorkomen door een *voorkomen* van een quantificatie.
Notatie. Zij φ een formule: we schrijven $\mathrm{Vr}(\varphi)$ voor de verzameling van alle variabelen die vrij voorkomen in φ.

15.8 Eindigheidslemma's

De evaluatie van een predikaatlogische formule φ is 'locaal', in drie opzichten: we hoeven alleen de interpretatie te kennen van niet-logische symbolen die in φ daadwerkelijk voorkomen (cf. 3.5.1); we hebben de bedeling alleen nodig voor variabelen die in φ daadwerkelijk vrij voorkomen (cf. 7.13); en als φ geen quantoren bevat, dan hebben we het universum alleen nodig voor de bedeling (cf. Oefening 9:6).

15.8.1 Lemma. Laat φ een formule zijn over een vocabulaire $\mathcal{L}$, $\mathbf{A}$ een structuur voor $\mathcal{L}$, en $\boldsymbol{b}_0$ en $\boldsymbol{b}_1$ bedelingen in $\mathbf{A}$. Als $\boldsymbol{b}_0(v) = \boldsymbol{b}_1(v)$ voor elke variabele v die vrij voorkomt in φ, dan $\varphi^{\mathbf{A}}[\boldsymbol{b}_0] = \varphi^{\mathbf{A}}[\boldsymbol{b}_1]$.

Bewijs. Laat $\mathcal{L}$ en $\mathbf{A}$ gegeven zijn. We bewijzen met inductie over φ:
Voor alle bedelingen $\boldsymbol{b}_0$ en $\boldsymbol{b}_1$ in $\mathbf{A}$: als $\boldsymbol{b}_0(v) = \boldsymbol{b}_1(v)$ voor alle $v \in \mathrm{Vr}(\varphi)$, dan
$$\varphi^{\mathbf{A}}[\boldsymbol{b}_0] = \varphi^{\mathbf{A}}[\boldsymbol{b}_1].$$

1° Laat φ een vergelijking zijn, zeg $\varphi = (\mathbf{s} \approx \mathbf{t})$. Volgens Lemma 7.13, $\mathbf{s}^{\mathbf{A}}[\boldsymbol{b}_0] = \mathbf{s}^{\mathbf{A}}[\boldsymbol{b}_1]$ en $\mathbf{t}^{\mathbf{A}}[\boldsymbol{b}_0] = \mathbf{t}^{\mathbf{A}}[\boldsymbol{b}_1]$. Dus $\boldsymbol{b}_0$ vervult φ dan en slechts dan als φ vervuld wordt door $\boldsymbol{b}_1$.
2° Laat $\varphi = P\mathbf{t}_0\ldots\mathbf{t}_{n-1}$een atomaire fomule zijn. Volgens Lemma 7.13, $\mathbf{t}_i^{\mathbf{A}}[\boldsymbol{b}_0] = \mathbf{t}_i^{\mathbf{A}}[\boldsymbol{b}_1]$ voor alle $i < n$. Dus
$$\langle \mathbf{t}_1^{\mathbf{A}}[\boldsymbol{b}_0],\ldots, \mathbf{t}_n^{\mathbf{A}}[\boldsymbol{b}_0]\rangle = \langle \mathbf{t}_1^{\mathbf{A}}[\boldsymbol{b}_1],\ldots, \mathbf{t}_n^{\mathbf{A}}[\boldsymbol{b}_1]\rangle,$$
en daaruit volgt direct dat $\varphi^{\mathbf{A}}[\boldsymbol{b}_0] = \varphi^{\mathbf{A}}[\boldsymbol{b}_1]$.
3° Als $\varphi \in \{\bot, \top\}$, dan is de waarheidswaarde van φ onafhankelijk van de bedeling.
4° Als $\varphi = \neg\psi$, dan $\varphi^{\mathbf{A}}[\boldsymbol{b}_0] = \neg\psi^{\mathbf{A}}[\boldsymbol{b}_0]$ per definitie,
$= \neg\psi^{\mathbf{A}}[\boldsymbol{b}_1]$ volgens inductieveronderstelling,
$= \varphi^{\mathbf{A}}[\boldsymbol{b}_1]$.
5° Als $\varphi = (\psi \circ \chi)$, voor een tweeplaatsig connectief $\circ$, dan
$\varphi^{\mathbf{A}}[\boldsymbol{b}_0] = \psi^{\mathbf{A}}[\boldsymbol{b}_0] \circ \chi^{\mathbf{A}}[\boldsymbol{b}_0]$ per definitie,
$= \psi^{\mathbf{A}}[\boldsymbol{b}_1] \circ \chi^{\mathbf{A}}[\boldsymbol{b}_1]$ volgens inductieveronderstelling,
$= \varphi^{\mathbf{A}}[\boldsymbol{b}_1]$.
6° Als $\varphi = \forall x\psi$, dan $\varphi^{\mathbf{A}}[\boldsymbol{b}_0] = \bigwedge_{a\in A} \psi^{\mathbf{A}}[\boldsymbol{b}_0(a/x)]$ per definitie,
$= \bigwedge_{a\in A} \psi^{\mathbf{A}}[\boldsymbol{b}_1(a/x)]$, want $\boldsymbol{b}_0(v) = \boldsymbol{b}_1(v)$ voor alle $v \in \mathrm{Vr}(\varphi)$, dus
$\boldsymbol{b}_0(a/x)(v) = \boldsymbol{b}_1(a/x)(v)$ voor alle $v \in \mathrm{Vr}(\psi)$,
$= \varphi^{\mathbf{A}}[\boldsymbol{b}_1]$.
7° Het geval dat $\varphi = \exists x\psi$ gaat analoog. ⊠

Laat $\mathcal{L}$ en $\mathcal{L}'$ twee vocabulaires zijn, $\mathcal{L}' \subseteq \mathcal{L}$. In het vervolg zullen we $\mathcal{L}'$ in zo'n geval een *subvocabulaire* of *subtype* van $\mathcal{L}$ noemen; omgekeerd spreken we van *supervocabulaire* en *supertype*. Als $\mathbf{A} = \langle A, I\rangle$ een structuur is van type $\mathcal{L}$, dan heet $\mathbf{A}\lceil\mathcal{L}' := \langle A, I\lceil\mathcal{L}'\rangle$ een *reduct* van $\mathbf{A}$, en $\mathbf{A}$ een *expansie* van $\mathbf{A}\lceil\mathcal{L}'$.

(Cf. Oefening 7:2 en Voorbeeld 2(i) hierboven.) Merk op dat bedelingen in **A** en in $\mathbf{A}\lceil\mathcal{L}'$ hetzelfde zijn.

15.8.2 Lemma. Zij $\mathcal{L}'$ een subvocabulaire van $\mathcal{L}$, **A** een structuur voor $\mathcal{L}$, met $\mathcal{L}'$-reduct $\mathbf{A}' := \mathbf{A}\lceil\mathcal{L}'$, en ***b*** een bedeling in **A**.
(a) Als **t** een term is over $\mathcal{L}'$, dan $\mathbf{t}^{\mathbf{A}'}[\boldsymbol{b}] = \mathbf{t}^{\mathbf{A}}[\boldsymbol{b}]$.
(b) Als φ een formule is over $\mathcal{L}'$, dan $\varphi^{\mathbf{A}'}[\boldsymbol{b}] = \varphi^{\mathbf{A}}[\boldsymbol{b}]$.

Bewijs. (a) Inductie over $\mathcal{L}'$-termen.
(b) Inductie over $\mathcal{L}'$-formules. ⊠

15:3 Oefening. Voer het hierboven gesuggereerde bewijs uit.

15.8.3 Definitie. Laat $\mathbf{A} = \langle A, I\rangle$ en $\mathbf{B} = \langle B, J\rangle$ structuren zijn voor een vocabulaire $\mathcal{L}$. Dan heet **B** een *substructuur* van **A**, notatie $\mathbf{B} \leq \mathbf{A}$, en **A** een *uitbreiding* of *superstructuur* van **B**, als
1° B een subuniversum is van het operationele reduct van **A**;
2° voor iedere $n \geq 0$ geldt, voor elke n-plaatsige predikaatletter $P \in \mathcal{L}$,

$$J(P) = I(P) \cap B^n,$$

en voor elk n-plaatsig operatiesymbool $Q \in \mathcal{L}$,

$$J(Q) = I(Q)\lceil B^n.$$

15.8.4 Lemma. Laat **A** en **B** structuren zijn voor een vocabulaire $\mathcal{L}$, $\mathbf{B} \leq \mathbf{A}$, ***b*** een bedeling, en φ een quantorvrije $\mathcal{L}$-formule. Dan $\varphi^{\mathbf{B}}[\boldsymbol{b}] = \varphi^{\mathbf{A}}[\boldsymbol{b}]$.

15:4 Oefening. Bewijs dit. [Een bedeling in **B** is ook een bedeling in **A**. Bewijs eerst met inductie over termen dat voor elke term **t** over $\mathcal{L}$, $\mathbf{t}^{\mathbf{B}}[\boldsymbol{b}] = \mathbf{t}^{\mathbf{A}}[\boldsymbol{b}]$ (cf. 9:6); doe vervolgens inductie over φ.]

15.9 Substitutie

Substitutie in vergelijkingen is besproken in §8.7. We zullen de daar gegeven definitie nu uitbreiden naar alle formules (over een willekeurig vocabulaire $\mathcal{L}$).

15.9.1 Definitie. Laat σ een substitutie zijn van $\mathcal{L}$-termen voor variabelen, en φ een $\mathcal{L}$-formule. Dan is $\sigma\varphi$ gedefinieerd als volgt.
(i) Als φ een vergelijking is, zeg $\varphi = (\mathbf{s}_1 \approx \mathbf{s}_2)$, dan $\sigma\varphi = (\sigma\mathbf{s}_1 \approx \sigma\mathbf{s}_2)$, als in §8.7.
(ii) Als $\varphi = P\mathbf{s}_1 \ldots \mathbf{s}_n$, dan $\sigma\varphi = P(\sigma\mathbf{s}_1,\ldots, \sigma\mathbf{s}_n)$.
(iii) Als $\varphi \in \{\bot, \top\}$, dan $\sigma\varphi = \varphi$.
(iv) Als $\varphi = \neg\psi$, dan $\sigma\varphi = \neg\sigma\psi$.
(v) Als $\varphi = \psi \circ \chi$, voor een tweeplaatsig connectief $\circ$, dan $\sigma\varphi = \sigma\psi \circ \sigma\chi$.
(vi) Zij $\varphi = \mathrm{Q}x\psi$, voor een quantor Q. Laat $\sigma' = \sigma(x/x)$, de substitutie die x onveranderd laat, en op alle andere variabelen werkt als σ. Dan $\sigma\varphi = \mathrm{Q}x\sigma'\psi$.

Als $\psi = [\mathbf{t}_1/x_1,\ldots, \mathbf{t}_k/x_k]\varphi$, dan schrijft men φ als $\varphi(x_1,\ldots,x_k)$, en ψ als $\psi(\mathbf{t}_1,\ldots, \mathbf{t}_k)$. (Cf. 5.7 en 8.7.)

Het quantorgeval is bijzonder, door de bijzondere rol van gebonden variabelen. Een vrije variabele heeft een eigen, nader te bepalen betekenis; een gebonden variabele niet. Een substitutie *is*, in beginsel, een nadere betekenisbepaling, en als zodanig niet van toepassing op gebonden variabelen.

De aanpassing van σ in clausule (vi) is nodig, maar niet voldoende, om onbedoelde veranderingen in betekenis te voorkomen. Zo hebben we in de structuur $\mathbf{Z} = \langle \mathbb{Z}, < \rangle$ voor elke bedeling $\boldsymbol{b}$:

$$(\forall v_0 \exists v_1\, v_0 < v_1)^{\mathbf{Z}}[\boldsymbol{b}] = 1,$$

en je zou kunnen verwachten dat weglaten van de quantificatie $\forall v_0$ en substitutie voor v_0 tot ware formules leidt:

$$(\exists v_1\, x < v_1)^{\mathbf{Z}}[\boldsymbol{b}] = 1;$$

maar succes is niet verzekerd! Neem $x = v_1$; $\exists v_1\, v_1 < v_1$ is in $\mathbf{Z}$ *onwaar*. Om zulke verrassingen uit te sluiten, hebben we een nieuw begrip nodig.

15.9.2 Definitie. Zij φ een formule, x een variabele, en $\mathbf{t}$ een term. Dan is $\mathbf{t}$ *substitueerbaar* voor x in φ als x in φ niet vrij voorkomt binnen het bereik van een quantificatie over een variabele die voorkomt in $\mathbf{t}$. Een substitutie σ is *toelaatbaar* in φ als voor elke variabele x, σx substitueerbaar is voor x in φ.

15.9.3 Substitutiestelling. Zij φ een formule, over zeker vocabulaire $\mathcal{L}$, ρ een substitutie van $\mathcal{L}$-termen voor variabelen die toelaatbaar is in φ, en $\mathbf{A}$ een $\mathcal{L}$-structuur. Dan geldt voor elke bedeling $\boldsymbol{b}$ in $\mathbf{A}$: $(\rho\varphi)^{\mathbf{A}}[\boldsymbol{b}] = \varphi^{\mathbf{A}}[\boldsymbol{b}^* \circ \rho]$.

Bewijs. Met inductie naar φ.

Als φ een vergelijking is: pas Gevolg 9.4.2(ii) toe.

Als $\varphi = P\mathbf{s}_0 \ldots \mathbf{s}_{n-1}$, dan $(\rho\varphi)^{\mathbf{A}}[\boldsymbol{b}] = 1$ dan en slechts dan als

$$P^{\mathbf{A}}((\rho\mathbf{s}_0)^{\mathbf{A}}[\boldsymbol{b}], \ldots, (\rho\mathbf{s}_{n-1})^{\mathbf{A}}[\boldsymbol{b}]),$$

wat wegens gevolg 9.4.2(i) hetzelfde is als $P^{\mathbf{A}}(\mathbf{s}_0^{\mathbf{A}}[\boldsymbol{b}^* \circ \rho], \ldots, \mathbf{s}_{n-1}^{\mathbf{A}}[\boldsymbol{b}^* \circ \rho])$, dat is, $\varphi^{\mathbf{A}}[\boldsymbol{b}^* \circ \rho] = 1$.

Als $\varphi = \neg\psi$, dan
$$\begin{aligned} (\rho\varphi)^{\mathbf{A}}[\boldsymbol{b}] &= \neg((\rho\psi)^{\mathbf{A}}[\boldsymbol{b}]) \\ &= \neg(\psi^{\mathbf{A}}[\boldsymbol{b}^* \circ \rho]) \text{ volgens inductiehypothese} \\ &= \varphi^{\mathbf{A}}[\boldsymbol{b}^* \circ \rho]. \end{aligned}$$

Als $\varphi = (\psi \circ \chi)$, voor een tweeplaatsig connectief $\circ$, dan
$$\begin{aligned} (\rho\varphi)^{\mathbf{A}}[\boldsymbol{b}] &= (\rho\psi)^{\mathbf{A}}[\boldsymbol{b}] \circ (\rho\chi)^{\mathbf{A}}[\boldsymbol{b}] \\ &= \psi^{\mathbf{A}}[\boldsymbol{b}^* \circ \rho] \circ \chi^{\mathbf{A}}[\boldsymbol{b}^* \circ \rho] \text{ volgens inductiehypothese} \\ &= \varphi^{\mathbf{A}}[\boldsymbol{b}^* \circ \rho]. \end{aligned}$$

Als $\varphi = \forall y\, \psi$, dan
$$\begin{aligned} (\rho\varphi)^{\mathbf{A}}[\boldsymbol{b}] &= \bigwedge_{a \in A} (\rho(y/y)\psi)^{\mathbf{A}}[\boldsymbol{b}(a/y)] \\ &= \bigwedge_{a \in A} \psi^{\mathbf{A}}[\boldsymbol{b}(a/y)^* \circ \rho(y/y)] \text{ volgens inductiehypothese.} \end{aligned}$$

Maar $(\boldsymbol{b}(a/y)^* \circ \rho(y/y))(y) = \boldsymbol{b}(a/y)^*(y) = a$; en als $x \neq y$, en $x \in \mathrm{Vr}(\psi)$, dan komt y niet voor in $\rho(x)$, dus $(\boldsymbol{b}(a/y)^* \circ \rho(y/y))(x) = \boldsymbol{b}(a/y)^*(\rho(x)) = \boldsymbol{b}^*(\rho(x))$. Dus volgens Lemma .8.1, $\psi^{\mathbf{A}}[\boldsymbol{b}(a/y)^* \circ \rho(y/y)] = \psi^{\mathbf{A}}[(\boldsymbol{b}^* \circ \rho)(a/y)]$, voor alle a. Dus

$$(\rho\varphi)^{\mathbf{A}}[\boldsymbol{b}] = \bigwedge_{a \in A} \psi^{\mathbf{A}}[(\boldsymbol{b}^* \circ \rho)(a/y)] = \varphi^{\mathbf{A}}[\boldsymbol{b}^* \circ \rho].$$

Het geval $\varphi = \exists y\, \psi$ gaat analoog, of met behulp van de De Morgan-wet. ☒

15.9.4 Gevolg. Laat φ een formule zijn, over zeker vocabulaire $\mathcal{L}$, x een variabele, $\mathbf{A}$ een $\mathcal{L}$-structuur, en $\boldsymbol{b}$ een bedeling in $\mathbf{A}$.

(a) Als $\mathbf{t}$ een $\mathcal{L}$-term is, substitueerbaar voor x in φ, en $\mathbf{t}^{\mathbf{A}}[\boldsymbol{b}] = a$, dan $([\mathbf{t}/x]\varphi)^{\mathbf{A}}[\boldsymbol{b}] = \varphi^{\mathbf{A}}[\boldsymbol{b}(a/x)]$.

(b) Als $\mathbf{t}_0$ en $\mathbf{t}_1$ $\mathcal{L}$-termen zijn, substitueerbaar voor x in φ, zo dat $\mathbf{t}_0^{\mathbf{A}}[\boldsymbol{b}] = \mathbf{t}_1^{\mathbf{A}}[\boldsymbol{b}]$, dan $([\mathbf{t}_0/x]\varphi)^{\mathbf{A}}[\boldsymbol{b}] = ([\mathbf{t}_1/x]\varphi)^{\mathbf{A}}[\boldsymbol{b}]$.

Bewijs. (a) Bedenk dat $\boldsymbol{b}(a/x) = \boldsymbol{b}(\mathbf{t}^{\mathbf{A}}[\boldsymbol{b}]/x) = \boldsymbol{b}^* \circ [\mathbf{t}/x]$. ☒

15:5 Oefening. Completeer het bovenstaande bewijs.

15.9.5 α-Conversiestelling. Laat x en y verschillende variabelen zijn, φ een formule over zeker vocabulaire $\mathcal{L}$, $y \notin \mathrm{Vr}(\varphi)$ en substitueerbaar voor x in φ, $\mathbf{A}$ een $\mathcal{L}$-structuur, en $\boldsymbol{b}$ een bedeling in $\mathbf{A}$. Dan $(\forall x\varphi)^{\mathbf{A}}[\boldsymbol{b}] = (\forall y[y/x]\varphi)^{\mathbf{A}}[\boldsymbol{b}]$ en $(\exists x\varphi)^{\mathbf{A}}[\boldsymbol{b}] = (\exists y[y/x]\varphi)^{\mathbf{A}}[\boldsymbol{b}]$.

Bewijs. Zij $a \in A$. Er geldt dat $[y/x]x = y$ en $[y/x]v = v$ als $v \neq x$. Dus
$\varphi^{\mathbf{A}}[\boldsymbol{b}(a/x)] = \varphi^{\mathbf{A}}[\boldsymbol{b}(a/y)(a/x)]$ volgens het eerste eindigheidslemma, want $y \notin \mathrm{Vr}(\varphi)$
$= \varphi^{\mathbf{A}}[\boldsymbol{b}(a/y)^{*}\circ y/x]$, want $\boldsymbol{b}(a/y)(a/x) = \boldsymbol{b}(a/y)^{*}\circ y/x$
$= [y/x]\varphi^{\mathbf{A}}[\boldsymbol{b}(a/y)]$ volgens de Substitutiestelling.
Dus $(\forall x\varphi)^{\mathbf{A}}[\boldsymbol{b}] = \bigwedge_{a\in A} \varphi^{\mathbf{A}}[\boldsymbol{b}(a/x)] = \bigwedge_{a\in A} [y/x]\varphi^{\mathbf{A}}[\boldsymbol{b}(a/y)] = (\forall y[y/x]\varphi)^{\mathbf{A}}[\boldsymbol{b}]$.

Het geval $\varphi = \exists y\psi$ gaat analoog, of met behulp van de De Morgan-wet. ☒

15.10 Het kan ook voorkomen dat we een formule willen substitueren voor een subformule van een gegeven formule. Analoog aan Gevolg .9.4 stellen we de situatie voor als twee substituties van formules voor een propositieletter (nulplaatsige predikaatletter) p. De werking van de substitutie-operator $[\varphi/p]$ is simpel, als in Oefening 2:2: vervang overal p door φ.

Equivalentiestelling. Laat φ, ψ en χ formules zijn over een vocabulaire $\mathcal{L}$, $p \in \mathcal{L}$ een nulplaatsige predikaatletter, en $\mathbf{A}$ een structuur voor $\mathcal{L}$, zo dat voor elke bedeling $\boldsymbol{b}$ in $\mathbf{A}$, $\varphi^{\mathbf{A}}[\boldsymbol{b}] = \psi^{\mathbf{A}}[\boldsymbol{b}]$. Dan $([\varphi/p]\chi)^{\mathbf{A}}[\boldsymbol{b}] = ([\psi/p]\chi)^{\mathbf{A}}[\boldsymbol{b}]$, voor elke bedeling $\boldsymbol{b}$ in $\mathbf{A}$.

Bewijs. Inductie naar χ, geschreven als $\chi(p)$.

Als $\chi = p$ is er niets te bewijzen; evenmin als p niet in χ voorkomt.

Als $\chi = \neg\chi'$, dan $\chi(\varphi)^{\mathbf{A}}[\boldsymbol{b}] = \neg(\chi'(\varphi)^{\mathbf{A}}[\boldsymbol{b}]) = \neg(\chi'(\psi)^{\mathbf{A}}[\boldsymbol{b}]) = \chi(\psi)^{\mathbf{A}}[\boldsymbol{b}]$, per definitie en volgens inductiehypothese.

Evenzo, als $\chi = (\chi_1 \circ \chi_2)$, voor een tweeplaatsig connectief $\circ$, dan
$\chi(\varphi)^{\mathbf{A}}[\boldsymbol{b}] = (\chi_1(\varphi)^{\mathbf{A}}[\boldsymbol{b}]) \circ (\chi_2(\varphi)^{\mathbf{A}}[\boldsymbol{b}]) = (\chi_1(\psi)^{\mathbf{A}}[\boldsymbol{b}]) \circ (\chi_2(\psi)^{\mathbf{A}}[\boldsymbol{b}]) = \chi(\psi)^{\mathbf{A}}[\boldsymbol{b}]$.

Als $\chi = \forall x\chi'$, dan $\chi(\varphi)^{\mathbf{A}}[\boldsymbol{b}] = \bigwedge_{a\in A} \chi'(\varphi)^{\mathbf{A}}[\boldsymbol{b}(a/x)] = \bigwedge_{a\in A} \chi'(\varphi)^{\mathbf{A}}[\boldsymbol{b}(a/x)]$
$= \chi(\psi)^{\mathbf{A}}[\boldsymbol{b}]$.
Het geval dat $\chi = \exists x\chi'$ gaat analoog, of met de Wet van De Morgan. ☒

In combinatie met de α-Conversiestelling rechtvaardigt deze stelling dat we niet-vrije variabelen in een gegeven formule χ stelselmatig vervangen door andere: een subformule $Qx\varphi$ mogen we veranderen in $Qy[y/x]\varphi$, mits y niet vrij voorkomt in φ en substitueerbaar is voor x in φ; het resultaat χ' is equivalent met χ, in de zin dat voor elke geschikte structuur $\mathbf{A}$ en elke bedeling $\boldsymbol{b}$ in $\mathbf{A}$, $\chi^{\mathbf{A}}[\boldsymbol{b}] = (\chi')^{\mathbf{A}}[\boldsymbol{b}]$. Dus onder meer:

Gevolg. Laat χ een $\mathcal{L}$-formule zijn en X een eindige verzameling variabelen. Dan is er een formule χ' waarin geen variabelen uit X bindend voorkomen, en zo dat voor elke $\mathcal{L}$-structuur $\mathbf{A}$ en elke bedeling $\boldsymbol{b}$ in $\mathbf{A}$, $\chi^{\mathbf{A}}[\boldsymbol{b}] = (\chi')^{\mathbf{A}}[\boldsymbol{b}]$.

De variabelenconventie. In het bijzonder kun je bij een gegeven formule φ altijd een equivalente formule φ' vinden waarin een gegeven term $\mathbf{t}$ substitueerbaar is — laat X bestaan uit de variabelen die in $\mathbf{t}$ voorkomen. Bijvoorbeeld, als je $v_0 + v_1$ wilt substitueren voor v_2 in $\varphi =$

$$\forall v_0 v_1 (v_0 < v_1 \to v_0 \cdot v_2 \leq v_1 \cdot v_2),$$

dan substitueer je in een equivalente formule, zeg

$$\forall v_3 v_4 (v_3 < v_4 \to v_3 \cdot v_2 \leq v_4 \cdot v_2).$$

Nu gebruiken we in de weergave van formules meestal geen officiële variabelen v_0, v_1, v_2,…, maar *onbepaalde* variabelen x, y, v_i,… De variabelenconventie is de afspraak dat, zonder tegenbericht, onbepaalde bindende variabelen altijd zo gekozen zijn dat alle substituties die we willen uitvoeren verantwoord zijn.

Zo kunnen we ook het satisfactiebegrip vereenvoudigen. Als v_{i_0},…, $v_{i_{k-1}}$ de variabelen bevat die vrij zijn in φ, dan definiëren we $\varphi^{\mathbf{A}}[a_0 \ldots a_{k-1}]$ door v_{i_j}, voor $j < k$, te laten verwijzen naar a_j; en in het quantorgeval stipuleren we

$$(\forall x \psi)^{\mathbf{A}}[a_0 \ldots a_{k-1}] = \bigwedge_{a \in A} \psi^{\mathbf{A}}[a_0 \ldots a_{k-1} a],$$

aannemend dat de index van x groter is dan i_{k-1}.

15:6 Oefening. Laat φ, ψ en χ formules zijn over een vocabulaire $\mathcal{L}$, $p \in \mathcal{L}$ een propositieletter, $\mathbf{A}$ een structuur voor $\mathcal{L}$, en $\boldsymbol{b}$ een bedeling in $\mathbf{A}$, zo dat $\varphi^{\mathbf{A}}[\boldsymbol{b}] = \psi^{\mathbf{A}}[\boldsymbol{b}]$. Stel dat p in χ niet voorkomt binnen het bereik van een quantificatie over een variabele die vrij voorkomt in φ of ψ. Bewijs dat

$$([\varphi/p]\chi)^{\mathbf{A}}[\boldsymbol{b}] = ([\psi/p]\chi)^{\mathbf{A}}[\boldsymbol{b}].$$

15.11 Definitie. Laat $\mathbf{A}$ en $\mathbf{B}$ structuren zijn van hetzelfde type $\mathcal{L}$. Een homomorfisme f: $\mathbf{A}\lceil Op_{\mathcal{L}} \longrightarrow \mathbf{B}\lceil Op_{\mathcal{L}}$ (zie §7.10) is een homomorfisme van $\mathbf{A}$ naar $\mathbf{B}$ als voor ieder natuurlijk getal n, voor elk n-plaatsig relatiesymbool $R \in \mathcal{L}$, voor alle $a_0,\ldots, a_{n-1} \in A$,

(*) $\qquad R^{\mathbf{A}}(a_0,\ldots, a_{n-1})$ impliceert dat $R^{\mathbf{B}}(f(a_0),\ldots,f(a_{n-1}))$.

We noteren f: $\mathbf{A} \longrightarrow \mathbf{B}$, voor '$f$ is een homomorfisme van $\mathbf{A}$ naar $\mathbf{B}$'. Een homomorfisme f van $\mathbf{A}$ naar $\mathbf{B}$ is *gesloten* als de omkering van (*) ook geldt:

(**) $\qquad R^{\mathbf{B}}(f(a_0),\ldots,f(a_{n-1}))$ impliceert dat $R^{\mathbf{A}}(a_0,\ldots, a_{n-1})$.

Een gesloten homomorfisme dat bijectief is, heet (cf. §7) een *isomorfisme*, en we noteren f: $\mathbf{A} \cong \mathbf{B}$, voor '$f$ is een isomorfisme van $\mathbf{A}$ naar $\mathbf{B}$'. Structuren $\mathbf{A}$ en $\mathbf{B}$ zijn *isomorf*, notatie $\mathbf{A} \cong \mathbf{B}$, als er een isomorfisme van $\mathbf{A}$ naar $\mathbf{B}$ bestaat.

Structuren van hetzelfde type zullen we *vergelijkbaar* noemen.

15:7 Oefening. Laat f: $\mathbf{A} \longrightarrow \mathbf{B}$ en g: $\mathbf{B} \longrightarrow \mathbf{C}$ homomorfismen zijn. Bewijs:
(a) de samengestelde $g \circ f$ is een homomorfisme van $\mathbf{A}$ naar $\mathbf{C}$;
(b) als f en g gesloten zijn, dan is $g \circ f$ ook gesloten.
(c) als f en g isomorfismen zijn, dan is $g \circ f$ ook een isomorfisme.

15:8 Oefening. Bewijs: als f: $\mathbf{A} \longrightarrow \mathbf{B}$ een isomorfisme is, dan is de inverse functie f^{-1} een isomorfisme van $\mathbf{B}$ naar $\mathbf{A}$.

15:9 Oefening. Laat $\mathbf{A}$, $\mathbf{B}$ en $\mathbf{C}$ vergelijkbare structuren zijn. Ga na dat
(i) $\mathbf{A} \cong \mathbf{A}$;
(ii) als $\mathbf{A} \cong \mathbf{B}$, dan $\mathbf{B} \cong \mathbf{A}$;
(ii) als $\mathbf{A} \cong \mathbf{B}$ en $\mathbf{B} \cong \mathbf{C}$, dan $\mathbf{A} \cong \mathbf{C}$.
(Als we willen afzien van de complicatie dat de structuren geen *verzameling* vormen, is isomorfie dus een equivalentierelatie.)

15:10 Oefening. Laat f: $\mathbf{A} \cong \mathbf{B}$ een isomorfisme zijn van $\mathcal{L}$-structuren, en φ een $\mathcal{L}$-formule. Bewijs dat voor elke bedeling $\boldsymbol{b}$ in $\mathbf{A}$, $\varphi^{\mathbf{A}}[\boldsymbol{b}] = \varphi^{\mathbf{B}}[f \circ \boldsymbol{b}]$.

15.12 Definitie. Structuur **A** is een *homomorf beeld* van structuur **B** als er een surjectief homomorfisme van **B** naar (*op*) **A** bestaat; een *gesloten homomorf beeld* als er een *gesloten* surjectief homomorfisme van **B** op **A** bestaat.

15:11 Oefening. (a) Bewijs dat $\langle \mathbb{N}, \leq \rangle$ een homomorf beeld is van $\langle \mathbb{Z}, \leq \rangle$.
(b) Is $\langle \mathbb{N}, \leq \rangle$ een *gesloten* homomorf beeld van $\langle \mathbb{Z}, \leq \rangle$?

15.13 Definitie (satisfactie). Een veelgebruikte notatie voor '$\varphi^{\mathbf{A}}[\boldsymbol{b}] = 1$' is:

$$\mathbf{A} \models \varphi[\boldsymbol{b}],$$

voor te lezen als: ***b*** *vervult* φ, of φ *is waar onder bedeling* ***b***, in **A**. Het tegendeel is $\mathbf{A} \not\models \varphi[\boldsymbol{b}]$ ($\varphi^{\mathbf{A}}[\boldsymbol{b}] = 0$).

Als Φ een verzameling van formules is, dan noteren we

$$\mathbf{A} \models \Phi[\boldsymbol{b}]$$

($\boldsymbol{b}$ vervult Φ in **A**) wanneer $\mathbf{A} \models \varphi[\boldsymbol{b}]$ voor alle $\varphi \in \Phi$.

15.14 Definitie (vervulbaarheid). Zij Φ een verzameling formules, en **A** een geschikte structuur (zo dat alle elementen van Φ in **A** geïnterpreteerd kunnen worden). Dan heet Φ *vervulbaar in* **A** als er een bedeling in **A** is die Φ vervult; en *vervulbaar* als er een structuur bestaat waarin Φ vervulbaar is.

Een enkele formule φ is vervulbaar als $\{\varphi\}$ vervulbaar is.

15.15 Definitie (geldigheid in een structuur). Een formule φ is *geldig* in een structuur **A**, notatie $\mathbf{A} \models \varphi$, als $\mathbf{A} \models \varphi[\boldsymbol{b}]$ voor elke bedeling $\boldsymbol{b}$ in **A**.

Als Φ een verzameling van formules is, dan noteren we $\mathbf{A} \models \Phi$ wanneer $\mathbf{A} \models \varphi$ voor alle $\varphi \in \Phi$.

Een formule zonder vrije variabelen heet een *zin*. Uit het eindigheidslemma .8.1 volgt dat voor een zin geldigheid en vervulbaarheid, in een gegeven structuur, hetzelfde zijn.

15.16 Definitie. Een *predikaatlogische theorie* (of *eerste orde-theorie*) bestaat uit een vocabulaire $\mathcal{L}$ en een verzameling formules over $\mathcal{L}$.

We kunnen een predikaatlogische theorie dus beschrijven als een paar

$$\mathcal{T} = \langle \mathcal{L}, \Phi \rangle$$

van een type $\mathcal{L}$ en een verzameling Φ van formules over $\mathcal{L}$, de *axioma's* van $\mathcal{T}$.

15.17 Voorbeelden
(i) Equationele theorieën: zie §8.4-5.
(ii) De theorie van de gelijkheid: $\mathrm{EQ} = \langle \emptyset, \emptyset \rangle$.
(iii) De theorie PO van de (partiële) ordening, met vocabulaire $\{\leq\}$ (binaire relatie, infix geschreven) en axioma's

$x \leq x$	(reflexiviteit)
$x \leq y \wedge y \leq x \rightarrow x \approx y$	(antisymmetrie)

$x \leq y \wedge y \leq z \to x \leq z$ (transitiviteit)

(iv) De theorie SO van de stricte (partiële) ordening, met vocabulaire $\{<\}$ (binaire relatie, infix geschreven) en axioma's

$\neg(x < x)$ (irreflexiviteit)

$x < y \wedge y < z \to x < z$ (transitiviteit)

(v) De theorie N van de natuurlijke getallen heeft vocabulaire $\{<, +. \cdot, S, 0\}$ en axioma's

N1. $Sx \not\approx 0$

N2. $Sx \approx Sy \to x \approx y$

N3. $x + 0 \approx x$

N4. $x + Sy \approx S(x + y)$

N5. $x \cdot 0 \approx 0$

N6. $x \cdot Sy \approx (x \cdot y) + x$

N7. $\neg(x < 0)$

N8. $x < Sy \leftrightarrow x < y \vee x \approx y$

N9. $x < y \vee x \approx y \vee y < x$.

15.18 Definitie. Zij $\mathcal{T} = \langle \mathcal{L}, \Phi \rangle$ een eerste orde-theorie. Een *model* van $\mathcal{T}$ is een structuur van type $\mathcal{L}$ waarin alle elementen van Φ geldig zijn.

15.19 Voorbeelden

(i) De hierboven ingevoerde begrippen zijn uitbreidingen van begrippen uit Deel II. Een groep is dus ook in de zin van de zojuist gegeven definitie een model van de groepentheorie, enzovoort.

(ii) Elke niet-lege verzameling is een model van de theorie EQ van de gelijkheid. (Officieel is zo'n model natuurlijk een paar $\langle X, \emptyset \rangle$, maar de interpretatie voegt niets toe.)

(iii, iv) Laat $\mathcal{X}$ een niet-lege collectie verzamelingen zijn. Dan is $\langle \mathcal{X}, \subseteq \rangle$ een model van PO, en $\langle \mathcal{X}, \subset \rangle$ een model van SO. In het algemeen noemen we een model van PO een *geordende verzameling*; en een model van SO een *strict geordende verzameling*. Een model van PO waarin ook

$$x \leq y \vee y \leq x$$

geldt, heet een *lineair* of *totaal* geordende verzameling. Het overeenkomstige axioma voor SO is N9.

(v) De natuurlijke getallen, met hun stricte ordening, optelling, vermenigvuldiging, opvolger en nul vormen een model van N.

15.20 Definitie. Zij $\mathcal{T} = \langle \mathcal{L}, \Phi \rangle$ een eerste orde-theorie, en $\Phi \cup \{\psi\}$ een verzameling formules over $\mathcal{L}$. Dan is ψ een gevolg van Φ in $\mathcal{T}$, notatie

$$\Phi \models_{\mathcal{T}} \psi,$$

als in ieder model van $\mathcal{T}$, iedere bedeling die Φ vervult ook ψ vervult.

Als Φ eindig is, zeg $\Phi = \{\varphi_1, \ldots, \varphi_n\}$, dan schrijven we ook

$$\varphi_1, \ldots, \varphi_n \models_{\mathcal{T}} \psi,$$

en zeggen dat ψ volgt uit $\varphi_1, \ldots, \varphi_n$. In het bijzonder korten we $\emptyset \models_{\mathcal{T}} \psi$ af tot $\models_{\mathcal{T}} \psi$: ψ is *geldig in* $\mathcal{T}$.

15.21 *Voorbeeld*. $\models_{\mathrm{N}} SSx \not\approx 0$.

We kunnen ook van gevolgen en geldigheid spreken buiten de context van een theorie. Laten we '$\Phi \models_{\langle \mathcal{L}, \emptyset \rangle} \psi$' afkorten tot $\Phi \models_{\mathcal{L}} \psi$.

15.22 Propositie. Laat $\mathcal{L}$ en $\mathcal{L}'$ twee vocabulaires zijn, zo dat $\Phi \cup \{\psi\}$ zowel een verzameling $\mathcal{L}$-formules is als een verzameling $\mathcal{L}'$-formules. Dan

$$\Phi \models_{\mathcal{L}} \psi \Leftrightarrow \Phi \models_{\mathcal{L}'} \psi.$$

Bewijs. We mogen wel aannemen dat $\mathcal{L} \subseteq \mathcal{L}'$ (anders bekijken we eerst $\mathcal{L} \cap \mathcal{L}'$, of we verwisselen $\mathcal{L}$ en $\mathcal{L}'$).
($\Rightarrow$) Stel $\Phi \models_{\mathcal{L}} \psi$; zij $\mathbf{A}$ een $\mathcal{L}'$-structuur, en $\boldsymbol{b}$ een bedeling in $\mathbf{A}$ die Φ vervult. Dan vervult $\boldsymbol{b}$ de verzameling Φ ook in het $\mathcal{L}$-reduct $\mathbf{A}\lceil\mathcal{L}$. Dus $\boldsymbol{b}$ vervult ψ in $\mathbf{A}\lceil\mathcal{L}$. Volgens Lemma .8.2 geldt dan ook $\mathbf{A} \models \psi[\boldsymbol{b}]$.
($\Leftarrow$) Stel $\Phi \models_{\mathcal{L}'} \psi$; zij $\mathbf{A} = \langle A, I\rangle$ een $\mathcal{L}$-structuur, en $\boldsymbol{b}$ een bedeling in $\mathbf{A}$ die Φ vervult. Definieer een expansie $\mathbf{A}' = \langle A, I'\rangle$ van $\mathbf{A}$ die een $\mathcal{L}'$-structuur is.
(Hoe je dat doet, maakt niet uit. Het kan bijvoorbeeld zo: neem $I'(R) = \emptyset$ voor alle relatiesymbolen $R \in \mathcal{L}' - \mathcal{L}$. Als $\mathcal{L}' - \mathcal{L}$ ook operatiesymbolen bevat, kies dan $a_0 \in A$ willekeurig. Definieer voor $Q \in Op_{\mathcal{L}'} - \mathcal{L}$, voor alle $a_1, \ldots, a_n \in A$, waar n de plaatsigheid is van Q:

$$I'(Q)(a_1, \ldots, a_n) = a_0.)$$

Volgens Lemma .8.2 wordt Φ vervuld door $\boldsymbol{b}$ in $\mathbf{A}'$. Dus $\mathbf{A}' \models \psi[\boldsymbol{b}]$; en weer volgens Lemma .8.2, $\mathbf{A} \models \psi[\boldsymbol{b}]$. ☒

Ongebruikt vocabulaire speelt dus geen rol. In het vervolg betekent

$$\Phi \models \psi$$

(lees: ψ *volgt uit* Φ) dat in elke structuur die rijk genoeg is om alle betrokken formules te interpreteren, elke bedeling die Φ vervult ook ψ vervult. Als $\models \psi$, dat wil zeggen, ψ volgt uit de lege verzameling, dan heet ψ *universeel geldig*. Als $\models \psi \leftrightarrow \chi$, dan heten ψ en χ *logisch equivalent*. (Dit is hetzelfde equivalentiebegrip als in #9: zie Oefening 19.)

Als de axioma's van een theorie $\mathcal{T} = \langle \mathcal{L}, \Phi\rangle$ zinnen zijn, dan kunnen we gevolgtrekking in $\mathcal{T}$ reduceren tot 'absolute' gevolgtrekking; dan geldt namelijk dat

$$\Psi \models_{\mathcal{T}} \chi \text{ dan en slechts dan als } \Phi \cup \Psi \models \chi.$$

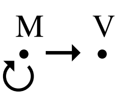
Als Φ een verzameling zinnen is, en $\mathbf{A} \models \Phi$, dan noemen we $\mathbf{A}$ ook een model van Φ.

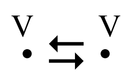
15.23 Voorbeelden

(i) Laat H de verzameling van alle mensen zijn, M die der mannen, V de verzameling der vrouwen, en O de collectie van alle mensenparen waarvan het eerste element de vader of moeder is van het tweede. Dan is

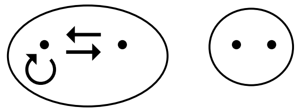
$$\langle H, M, V, O\rangle$$

een model van de ware zinnen in Oefening 13:1.
(ii) $\langle \mathbb{Z}, <\rangle$ is een model van de zinnen die corresponderen met de beweringen (i)-(iv) in opgave 13:2; idem $\langle \mathbb{N}, +, \cdot\rangle$ voor 13:4.
(iii) Kleine structuren voor eenvoudige talen kun je *uittekenen*. Hier zijn eenvoudige modellen voor de zinnen in respectievelijk 13:1(a) en (b):

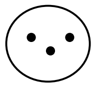


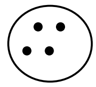


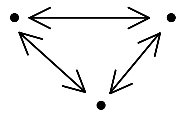
Het domein bestaat uit twee individuen, aangegeven met stippen; de eenplaatsige predikaten die op de individuen van toepassing zijn, staan erboven; en de ouderrelatie is aangegeven met pijlen.

Nog een paar voorbeelden:
Twee modellen van $\forall xy\,(Rxy \to Ryx)$: 

Dit waren toevallig ook modellen voor $\exists xy\, x \not\approx y$. Hier zijn er nog twee:





Een model van $\{\forall xy\,(\forall z(z \in x \leftrightarrow z \in x) \to x \approx y),$
$\forall xy\,\exists z(x \in z \wedge y \in z),$
$\forall x\ (x \notin x)\}$ 

(Om de verzamelingstheorie te axiomatiseren is dus nog meer nodig.)
(iv) Ook voor oneindige structuren kan een pictorale voorstelling nuttig zijn. Een model voor

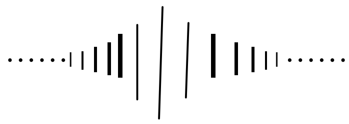
$$\{\forall xy\,(Sx \approx Sy \to x \approx y), \exists x \forall y\, x \not\approx Sy\}$$

kan men als volgt schetsen:

$\bullet \to \bullet \to \bullet \to \bullet \to \bullet \to \bullet \to \cdots\cdots$ (enzovoort);

of in perspectief:

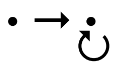
Het laatste is ook een geschikt beeld van $\langle \mathbb{N}, < \rangle$ (met de ordening van links naar rechts). In dezelfde stijl is $\langle \mathbb{Z}, < \rangle$:



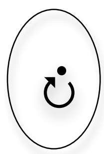
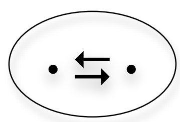
15:12 Vraag. Is ieder model van de formules (i)-(iv) van 13:2 isomorf met $\langle \mathbb{Z}, < \rangle$?

Oefeningen

15:13 Zij $\mathcal{L}$ het vocabulaire bestaande uit een enkele tweeplaatsige predikaatletter R.
(a) Geef een zin over $\mathcal{L}$ die



als enig model heeft (op isomorfie na).
(b) Geef ook een zin die als modellen, op isomorfie na, alleen

 en 

heeft.

15:14 Geef alle modellen (op isomorfie na) met hoogstens drie elementen van

$$\{\forall xy\,(Rxy \to \neg Ryx), \exists xy\, Rxy, \forall xy\,(Rxy \to \forall z(Rxz \to y \approx z))\}.$$

15:15 Bedenk voor alle $n \in \mathbb{N}$, over het lege vocabulaire:

(a) een zin μ_n die alleen waar is in structuren met *minstens n* elementen;

(b) een zin η_n die alleen waar is in structuren met *hoogstens n* elementen;

(b) een zin π_n die alleen waar is in structuren met *precies n* elementen.

15:16 Ga na dat $\models \forall x\,(\varphi \to \psi) \to \forall x\varphi \to \forall x\psi$.

15.24 Redeneringen en tegenvoorbeelden

Een tegenvoorbeeld bij een predikaatlogisch geanalyseerde redenering is een structuur met een bedeling die de premissen vervult, en de negatie van de conclusie. In het veel voorkomende geval van een redenering die geheel bestaat uit zinnen, is een tegenvoorbeeld een model van de premissen en de negatie van de conclusie.

Voorbeeld. Na betoogd te hebben dat het construeren van godsbewijzen niet per se zinloos is, zet Thomas van Aquino er twee uiteen die hij aan Aristoteles toeschrijft (Contra Gentiles, lib. 1 cap. 13 n. 3):
Quarum prima talis est: omne quod movetur, ab alio movetur. Patet autem sensu aliquid moveri, utputa solem. Ergo alio movente movetur. Aut ergo illud movens movetur, aut non. Si non movetur, ergo habemus propositum, quod necesse est ponere aliquod movens immobile. Et hoc dicimus Deum. Si autem movetur, ergo ab alio movente movetur. Aut ergo est procedere in infinitum: aut est devenire ad aliquod movens immobile. Sed non est procedere in infinitum. Ergo necesse est ponere aliquod primum movens immobile.
(*Waarvan het eerste zo gaat: al wat beweegt, wordt door iets anders bewogen. We nemen duidelijk waar dat er iets beweegt, de zon bijvoorbeeld. Die beweegt dus door iets anders dat hem beweegt. Òf dat bewegende wordt bewogen, òf niet. Als het niet wordt bewogen, hebben we de stelling, dat het noodzakelijk is iets onbeweeglijks te poneren dat beweegt. En dat noemen we God. Als het echter bewogen wordt, wordt het bewogen door iets anders dat het beweegt. Dan moeten we ofwel in het oneindige doorgaan: of uitkomen op iets onbeweeglijks dat beweegt. Maar in het oneindige doorgaan, dat bestaat niet. Dus is het noodzakelijk een onbeweeglijke eerste beweger te poneren*.)

In zijn geheel gaat deze redenering de eerste orde-logica te boven; we komen er nog op terug. In elk geval kunnen we opmerken dat het Latijn duidelijker is, niet alleen omdat Thomas zo'n voortreffelijk stilist is, maar ook doordat hij de intransitieve (mediale) betekenis van *bewegen* met het passivum weergeeft, waardoor het geheel overtuigender wordt. Hier is een gedeeltelijke analyse, waarin *Mxy* staat voor *x movet y*.

1° Omne quod movetur, ab alio movetur,

$$\forall x\,(\exists y\, Myx \to \exists y(y \neq x \wedge Myx)).$$

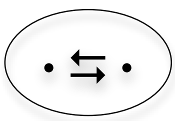
2° Patet aliquid moveri,

$$\exists xy\, Myx.$$

Gewenste conclusie: Est aliquod movens immobile,

$$\exists x\,(\exists y\, Mxy \wedge \neg\exists y Myx).$$

Een eenvoudig tegenvoorbeeld wordt gesuggereerd door



Dergelijke cykels zijn duidelijk niet de bedoeling. Je kunt ze uitsluiten met een

hulppredikaat M^*, geaxiomatiseerd door
3° $Mxy \to M^*xy$,
4° $M^*xy \wedge M^*yz \to M^*xz$,
5° $M^*xy \wedge M^*yx \to x \approx y$.

Als de wereld eindig is, volgt uit 1°-5° de gewenste conclusie. Anders is

$$\langle\{x \in \mathbb{Z} \mid x \leq 0\}, >\rangle$$

een tegenvoorbeeld. *Procedit in infinitum*: maar dat kunnen we in de eerste orde-logica niet uitsluiten. (Zie verder Appendix A.)

Verdere opgaven

15:17 Geef tegenvoorbeelden bij de schema's
(i) $\forall x\,(Ax \vee Bx)\ /\ \forall x\,Ax \vee \forall x\,Bx$;
(ii) $\exists x\,Ax \wedge \exists x\,Bx\ /\ \exists x\,(Ax \wedge Bx)$;
(iii) $\forall x\,Ax \to \forall x\,Bx\ /\ \forall x\,(Ax \to Bx)$;
(iv) $\forall x\,\exists y\,(Ax \to By)\ /\ \exists y\,By$;
(v) $\forall xy\,(fx \approx fy \to x \approx y)\ /\ \exists xyz\,(x \not\approx y \wedge x \not\approx z \wedge y \not\approx z)$.

15:18 Laat $\Phi \cup \{\psi\}$ een verzameling formules zijn, x een variabele, en $\mathbf{t}$ een term substitueerbaar voor x in ψ. Ga na dat
(i) als $\Phi \models [\mathbf{t}/x]\psi$, dan $\Phi \models \exists x\psi$;
(ii) als $\Phi \models \forall x\psi$, dan $\Phi \models [\mathbf{t}/x]\psi$;
(iii) als $\Phi \models \psi$, en x komt niet vrij voor in Φ, dan $\Phi \models \forall x\psi$;
(iv) als $\Phi \models \exists x\psi$ en $\Phi \models \psi \to \chi$, en x komt niet vrij voor in $\Phi \cup \{\chi\}$, dan $\Phi \models \chi$.

15:19 (a) Bewijs: φ en ψ zijn logisch equivalent dan en slechts dan als voor iedere geschikte structuur **A** en iedere bedeling $\boldsymbol{b}$ in **A**, $\varphi^{\mathbf{A}}[\boldsymbol{b}] = \psi^{\mathbf{A}}[\boldsymbol{b}]$.
(b) Laat φ_0, φ_1 en ψ formules zijn, en p een propositieletter. Bewijs: als φ_0 en φ_1 logisch equivalent zijn, dan is $[\varphi_0/p]\psi$ logisch equivalent met $[\varphi_1/p]\psi$.

15:20 Neem aan dat $x \notin \mathrm{Vr}(\psi)$. Bewijs dat logisch equivalent zijn:
(i) $\psi \to \exists x\varphi$ en $\exists x(\psi \to \varphi)$;
(ii) $\forall x\,\varphi \to \psi$ en $\exists x(\varphi \to \psi)$;
(iii) $\psi \to \forall x\,\varphi$ en $\forall x\,(\psi \to \varphi)$;
(iv) $\exists x\,\varphi \to \psi$ en $\forall x\,(\varphi \to \psi)$.

15:21 Een formule φ is in *prænexvorm* als hij bestaat uit een rijtje quantificaties gevolgd door een quantorvrije formule (de *matrix* van φ). Bewijs dat elke predikaatlogische formule logisch equivalent is met een formule in prænexvorm. (Formule-inductie. Je kunt je beperken tot de connectieven $\to$ en $\perp$. Gebruik de voorafgaande oefeningen.)

15:22 Bewijs dat logisch equivalent zijn:
(i) $\forall x\,(\varphi \wedge \psi)$ en $\forall x\,\varphi \wedge \forall x\,\psi$;
(ii) $\exists x\,(\varphi \vee \psi)$ en $\exists x\varphi \vee \exists x\psi$.

15:23 Neem aan dat $x \notin \mathrm{Vr}(\psi)$. Bewijs dat logisch equivalent zijn:
(i) $\forall x\,(\varphi \vee \psi)$ en $\forall x\,\varphi \vee \psi$;
(ii) $\exists x\,(\varphi \wedge \psi)$ en $\exists x\varphi \wedge \psi$.

15:24 Als ψ logisch equivalent is met φ, en ψ is in prænexvorm, dan heet ψ *een prænexvorm van* φ. Construeer prænexvormen voor:
(i) $\forall y\,(\exists x\,Ax \to \forall x\,Rxy) \to \forall x Bx$;
(ii) $\forall x\,(\exists y\,Rxy \to \exists y(Rxy \wedge \forall u Ruy))$;

(iii) $\neg\exists y\,(\neg\forall x\,Rxy \wedge \exists z\,Rzy)$;
(iv) $\forall x\,\exists y\,((\exists x Rxz \to \forall z Rzx) \to Rxy)$;
(v) $\forall x\,Ax \vee \neg\exists xy\,(Rxy \wedge Ax)$;
(vi) $\forall x\,(\exists y\,Rxy \leftrightarrow \exists y\,Ryx)$.

15:25 Een *maximaal element* in een geordende verzameling is een element m dat voldoet aan $\forall x(m \leq x \to x \leq m)$. Een *grootste* element is een element g dat voldoet aan $\forall x\, x \leq g$. Bewijs: een geordende verzameling voldoet aan

$$\forall y(\forall x(y \leq x \to x \leq y) \to \forall x\, x \leq y)$$

dan en slechts dan als ze voldoet aan

$$\neg\exists y \forall x\, x \leq y \to \forall x \exists y(x \leq y \wedge y \nleq x).$$

15:26 (Generalisatie van #10). Definieer de substitutie van formules $\varphi(v_0,\ldots, v_{n-1})$ voor n-plaatsige predikaatletters, zo dat bijvoorbeeld

$$[\exists v_2(v_2 \not\approx 0 \wedge v_0 + v_2 \approx v_1)/R]\forall xy(Rxy \to \neg Ryx) = \\ \forall xy(\exists v_2(v_2 \not\approx 0 \wedge x + v_2 \approx y) \to \neg\exists v_2(v_2 \not\approx 0 \wedge y + v_2 \approx x)).$$

Zijn er beperkingen, zoals substitueerbaarheid bij de substitutie van termen?

15:27 Beschouw de structuur $\mathbf{R} = \langle \mathbb{R}, +, \cdot, -, |.|, f, 0, 1\rangle$: de ring der reële getallen met absolute waarde-operatie en een éénplaatsige functie f. Construeer formules die uitdrukken, voor $x, y, z \in \mathbb{R}$:
(a) $\lim_{x\to y} f(x) = z$;
(b) f is continu in x;
(c) f is continu;
(d) f is uniform continu;
(e) f is differentieerbaar in x.

15:28 Laat **N** de structuur zijn beschreven in #19(v), en n een natuurlijk getal. Definieer een uitbreiding van **N** met n nieuwe elementen die een model is van N.

§16 Natuurlijke deductie

We zullen nu de deductiesystemen van §6 en §8 uitbreiden met introductie- en eliminatieregels voor de quantoren.

Als context veronderstellen we, analoog aan §8.8, een eerste orde-theorie $\mathcal{T}$ = $\langle \mathcal{L}, T\rangle$. De instantiatieregel (2.) van §8.8 moet aangescherpt worden: $[\mathbf{t}_1/x_1,\ldots, \mathbf{t}_n/x_n]\varphi$ is alleen dan een geldige instantie van φ als voor alle i, $1 \leq i \leq n$, $\mathbf{t}_i$ substitueerbaar is voor x_i in φ.

16.1 Quantorintroductie- en -eliminatieregels. Men bewijst een algemene uitspraak $\forall x\varphi$ door φ te bewijzen voor *willekeurige* x. Dat x willekeurig is, wil zeggen dat we over x geen bijzondere informatie hebben. In natuurlijke deductie-termen: x komt niet vrij voor in de aannamen. Het resulterende schema voor *generalisatie* is

:
:
n. φ
:
:
n + m. $\forall x\varphi$ (∀-introductie op n) —mits x niet vrij voorkomt in (nog niet ingetrokken) aannamen.

De ∀-eliminatieregel is

:
:
n. $\forall x\varphi$
:
:
n + m. $[\mathbf{t}/x]\varphi$(∀-eliminatie op n) —mits **t** substitueerbaar is voor x in φ.

Even vanzelfsprekend als ∀-eliminatie is de ∃-introductieregel:

:
:
n. $[\mathbf{t}/x]\varphi$
:
:
n + m. $\exists x\varphi$(∃-introductie op n) —mits **t** substitueerbaar is voor x in φ.

16:1 Opgave. De noodzaak van de substitueerbaarheidseis bij ∀-eliminatie is geïllustreerd in §15.9. Geef zelf een voorbeeld waaruit de noodzakelijkheid blijkt van de substitueerbaarheidseis bij ∃-introductie.

De rechtvaardiging van de eliminatieregel voor ∃ lijkt op die voor ∨-eliminatie. $\exists x\varphi$ wil zeggen dat er een x is zo dat φ —waarvan we verder niets bijzonders weten. Als we nu ψ kunnen concluderen uit φ, zonder verdere aannamen over x — en x komt niet vrij voor in ψ — dan mogen we ψ concluderen uit $\exists x\varphi$. In een tweedimensionaal schema:

(∃-eliminatie) $\dfrac{\exists x\varphi \qquad \varphi \to \psi}{\psi}$ — mits x niet vrij voorkomt in ψ of in niet ingetrokken aannamen.

Dat x niet vrij mag zijn in ψ is te zien in de volgende pseudodeductie:

	1. $\exists x\, Ax$	(aanname)
	2. Ax	(A)
*	3. $Ax \to Ax$	(→-introductie)
	4. Ax	(*∃-eliminatie, 1, 3)
	5. $\forall x Ax$	(∀-introductie, 4)

Met andere woorden: uit $\exists xAx$ zou $\forall xAx$ volgen, en dat is bepaald niet de bedoeling.

16.2 ≈-eliminatie. De eliminatieregel voor gelijkheid is de voor de hand liggende generalisatie van de regel *vervanging van gelijken* in 8.8, onder voorwaarde van substitueerbaarheid:

(≈-eliminatie) $\dfrac{\mathbf{t}_1 \approx \mathbf{t}_2 \quad [\mathbf{t}_1/x]\varphi}{[\mathbf{t}_2/x]\varphi}$ —mits $\mathbf{t}_1$ en $\mathbf{t}_2$ substitueerbaar zijn voor x in φ.

16.3 Voorbeelden. (a) $\vdash_{SO} \neg\exists xy(x < y \wedge y < x)$.

1.	$\exists xy(x < y \wedge y < x)$	aanname
2.	$\exists y(x < y \wedge y < x)$	aanname
3.	$x < y \wedge y < x$	aanname
4.	$x < y \wedge y < x \rightarrow x < x$	instantie transitiviteit
5.	$x < x$	eliminatie $\rightarrow$ 4, 3
6.	$\neg(x < x)$	instantie irreflexiviteit
7.	$\perp$	eliminatie $\rightarrow$ 6, 5
8.	$\neg(x < y \wedge y < x)$	
9.	$\perp$	elim. $\exists$ 2, 8
10.	$\neg\exists y(x < y \wedge y < x)$	
11.	$\perp$	elim. $\exists$ 1, 10
12.	$\neg\exists xy(x < y \wedge y < x)$	

(b) $\vdash_N \forall x(x < SS0 \rightarrow x \approx 0 \vee x \approx S0)$.

1.	$x < SS0$	aanname
2.	$x < SS0 \leftrightarrow x < S0 \vee x \approx S0$	instantie N8
3.	$x < S0 \vee x \approx S0$	eliminatie $\leftrightarrow$ 2, 1
4.	$x < S0$	aanname
5.	$x < S0 \leftrightarrow x < 0 \vee x \approx 0$	instantie N8
6.	$x < 0 \vee x \approx 0$	eliminatie $\leftrightarrow$ 5, 4
7.	$\neg(x < 0)$	N7
8.	$x < 0$	aanname
9.	$\perp$	eliminatie $\rightarrow$ 7, 8
10.	$x \approx 0$	ex falso
11.	$x < 0 \rightarrow x \approx 0$	
12.	$x \approx 0$	aanname
13.	$x \approx 0 \rightarrow x \approx 0$	
14.	$x \approx 0$	eliminatie $\vee$ 6, 11, 13
15.	$x \approx 0 \vee x \approx S0$	introductie $\vee$ 14
16.	$x < S0 \rightarrow x \approx 0 \vee x \approx S0$	
17.	$x \approx S0$	aanname
18.	$x \approx 0 \vee x \approx S0$	introductie $\vee$ 17
19.	$x \approx S0 \rightarrow x \approx 0 \vee x \approx S0$	
20.	$x \approx 0 \vee x \approx S0$	eliminatie $\vee$ 3, 16, 19
21.	$x < SS0 \rightarrow x \approx 0 \vee x \approx S0$	
22.	$\forall x(x < SS0 \rightarrow x \approx 0 \vee x \approx S0)$	introductie $\forall$ 21

16:2 Oefening. Bewijs $\vdash_N SS0 + SS0 \approx SS0 \cdot SS0$

16.4 Notatie. Met '$\Phi \vdash_{\mathcal{T}} \chi$' drukken we uit, in aansluiting bij §6 en §8, dat er een afleiding van χ in $\mathcal{T}$ bestaat waarvan de niet-ingetrokken aannamen tot Φ behoren. We schrijven $\Phi \vdash \chi$ als er een vocabulaire $\mathcal{L}$ bestaat zo dat $\Phi \vdash_{\mathrm{I}(\mathcal{L})} \chi$, waar $\mathrm{I}(\mathcal{L}) = \langle \mathcal{L}, \emptyset \rangle$, als onder Oefening 9:2. We zullen in het vervolg zien dat $\mathcal{L}$ niet meer hoeft te bevatten dan de niet-logische symbolen in Φ en χ, maar vooralsnog spreekt dat niet vanzelf.

16.5 Universele afsluiting. Laat φ een formule zijn die precies de variabelen $x_1, \ldots, x_n$ vrij bevat. Een *universele afsluiting* van φ is dan een zin

$$\forall x_1 \ldots x_n \varphi.$$

Laat T een verzameling eerste orde-formules zijn, en T^U bestaan uit universele afsluitingen van alle formules in T. Dan

$\Phi \cup T^U \vdash \chi$ dan en slechts dan als
er een vocabulaire $\mathcal{L}$ bestaat zo dat $\Phi \vdash_{\langle \mathcal{L}, T \rangle} \chi$.

16.6 Verdere voorbeelden
(a) $\forall x \varphi \vdash \forall y [y/x]\varphi$, als y niet vrij voorkomt in $\forall x \varphi$, en substitueerbaar is voor x in φ.

1. $\forall x \varphi$ (aanname)
2. $[y/x]\varphi$ ($\forall$-eliminatie 1) (kan wegens substitueerbaarheid)
3. $\forall y [y/x]\varphi$ ($\forall$-introductie 2) (y is niet vrij in de aanname)

(b) $\exists x \varphi \vdash \exists y [y/x]\varphi$, onder de voorwaarden van (a).

1. $\exists x \varphi$ (aanname)
2. φ (aanname)
3. $\exists y [y/x]\varphi$ ($\exists$-introductie 2) (want $\varphi = [x/y][y/x]\varphi$)
4. $\varphi \to \exists y [y/x]\varphi$
5. $\exists y [y/x]\varphi$ ($\exists$-eliminatie 1, 4)

(c) $\vdash_{\mathcal{T}} \exists x (x \approx \mathbf{t})$, als x niet voorkomt in $\mathbf{t}$.

1. $\mathbf{t} \approx \mathbf{t}$ (identiteitsaxioma)
2. $\exists x (x \approx \mathbf{t})$ ($\exists$-introductie 1)

16:3 Vraag: Waarom moet in het laatste voorbeeld geëist worden dat x niet voorkomt in $\mathbf{t}$?

16:4 Oefening. Laat zien dat, voor alle eerste orde-formules φ en ψ:
(i) $\forall x(\varphi \to \psi) \vdash \varphi \to \forall x \psi$, als x niet vrij voorkomt in φ, en
(ii) $\forall x(\psi \to \varphi) \vdash \exists x \psi \to \varphi$ onder dezelfde voorwaarde,
(iii) $\vdash x \approx y \to y \approx z \to x \approx z$
(iv) $\vdash x \approx y \to y \approx x$
(v) $\forall x \neg\varphi \vdash \neg\exists x \varphi$
(vi) $\exists x \neg\varphi \vdash \neg\forall x \varphi$
(vii) $\neg\forall x \varphi \vdash \exists x \neg\varphi$
(viii) $\neg\exists x \varphi \vdash \forall x \neg\varphi$
In (vii) en (viii) is *reductio ad absurdum* nodig.

16.7 Nog een voorbeeld. De oplossing van 13:6 was:

$$\forall x(Dx \to (\neg Sxx \leftrightarrow Sbx)) \,/\, \neg Db,$$

en dat is een geldige gevolgtrekking. We kunnen dat staven met een afleiding:

1. $\forall x(Dx \to (\neg Sxx \leftrightarrow Sbx))$ (aanname)
2. Db (aanname)
3. $Db \to (\neg Sbb \leftrightarrow Sbb)$ ($\forall$-eliminatie 1)
4. $\neg Sbb \leftrightarrow Sbb$ ($\to$-eliminatie 2, 3)
5. Sbb (aanname)
6. $\neg Sbb$ ($\leftrightarrow$-eliminatie 4, 5)
7. $\bot$ ($\to$-eliminatie 5, 6)
8. $\neg Sbb$
9. Sbb ($\leftrightarrow$-eliminatie 4, 8)
10. $\bot$ ($\to$-eliminatie 8, 9)
11. $\neg Db$

Verdere Oefeningen

16:5. Bewijs:
(i) $\forall x\,(Mx \to Vx), \forall x\,(Px \to Mx) \vdash \forall x\,(Px \to Vx)$;
(ii) $\forall x\,(Kx \to Mx), \exists x\,(Kx \wedge \neg Zx) \vdash \exists x\,(Mx \wedge \neg Zx)$.

16:6. Gebruik de $\bot$-regels om te laten zien dat $\psi \to \exists x\varphi \vdash \exists x(\psi \to \varphi)$, mits x niet vrij voorkomt in ψ.

16:7 We gebruiken $\vdash_I$, net als in §6, voor intuïtionistische afleidbaarheid — dat wil zeggen, zonder *reductio ad absurdum*. Laat zien:
(a) $\vdash_I \neg\neg\forall x\varphi \to \forall x\neg\neg\varphi$;
(b) $\vdash_I \exists x\neg\neg\varphi \to \neg\neg\exists x\varphi$.

16.8 De deductiestelling. In §6 is de strategie gepropageerd om afleidingen te beginnen met de aannamen die mogen blijven staan. Door de nieuwe regels die we hebben toegevoegd is dat echter niet altijd meer mogelijk. Uit Voorbeeld 6(a) volgt $\forall x\,Ax, Ay \vdash \forall y\,Ay$; maar als je begint met beide aannamen op te schrijven, zul je de conclusie niet bereiken.

Het resultaat van Oefening 6:5 lijkt hiermee ook minder vanzelfsprekend. Omdat we het nog nodig zullen hebben, geven we van het belangrijkste onderdeel een bewijs dat rekening houdt met het mogelijk vrij voorkomen van variabelen in aannamen.

Stelling. Als $\Phi \cup \{\varphi\} \vdash \psi$, dan $\Phi \vdash \varphi \to \psi$.

Bewijs. Laat ψ de conclusie zijn van een afleiding met openstaande aannamen $\varphi_1,\ldots,\varphi_n$, in volgorde; zij $\varphi = \varphi_i$. We kunnen de gegeven afleiding verlengen tot een afleiding van $\varphi_1 \to\ldots\to \varphi_n \to \psi$, zonder nog openstaande aannamen. Voeg nu de aannamen toe in de volgorde $\varphi_1,\ldots,\varphi_{i-1}, \varphi_{i+1},\ldots,\varphi_n, \varphi$; leid ψ af met $\to$-eliminatie; en trek de laatste aanname in. ⊠

16.9 Lemma. Laat $\Phi \cup \{\psi\}$ een verzameling eerste orde-formules zijn, en $\mathbf{t}_1$ en $\mathbf{t}_2$ termen die substitueerbaar zijn voor x in ψ. Als $\Phi \vDash [\mathbf{t}_1/x]\psi$ en $\Phi \vDash \mathbf{t}_1 \approx \mathbf{t}_2$, dan $\Phi \vDash [\mathbf{t}_2/x]\psi$.

Bewijs. Laat $\mathbf{A}$ een geschikte structuur zijn, en $\boldsymbol{b}$ een bedeling in $\mathbf{A}$ die Φ vervult. Dan $\mathbf{t}_1^{\mathbf{A}}[\boldsymbol{b}] = \mathbf{t}_2^{\mathbf{A}}[\boldsymbol{b}]$, dus volgens 15.9.4(b),

$$([\mathbf{t}_2/x]\psi)^{\mathbf{A}}[\boldsymbol{b}] = ([\mathbf{t}_1/x]\psi)^{\mathbf{A}}[\boldsymbol{b}] = 1.$$ ⊠

16.10 Correctheidsstelling. Laat $\Phi \cup \{\psi\}$ een verzameling eerste orde-formules zijn. Als $\Phi \vdash \psi$, dan $\Phi \models \psi$.

16:8 Oefening. Bewijs dit zelf. [Volg het stramien van 6.6.3. Lemma 6.6.2 geldt ook voor eerste orde-formules. Gebruik Lemma 9 voor de vervangingsregel, en opgave 15:18 voor de quantorregels.]

16.11 Volledigheid

De omkering van de correctheidsstelling is, net als bij de vorige gelegenheden, gecompliceerder. De meeste complicaties zijn echter al aan de orde geweest — zoals we zullen zien. De aanpak is precies als in §6.

De definities 6.6.4 (consistentie, inconsistentie) en 6.6.10 (maximale consistentie) zijn probleemloos toepasbaar op de predikaatlogische deductie.

16.11.1 Vervulbaarheidsstelling. Elke consistente verzameling formules is vervulbaar.

Het bewijs bestaat net als in §6 in de constructie van een omvattende maximaal consistente verzameling, die een structuur beschrijft. Een extra verwikkeling treedt op doordat we, wanneer we besluiten een formule $\exists x\varphi(x)$ op te nemen, ervoor moeten zorgen dat ook een instantie $\varphi(\mathbf{t})$ wordt vervuld.

Opmerking. We veronderstellen in het bewijs een aftelling $\langle \psi_n | n \in \mathbb{N} \rangle$ van alle formules van de predikaatlogische taal waar we mee werken. Zo'n aftelling bestaat voor talen over een eindig vocabulair; en zelfs over een oneindig vocabulair, mits dat een soortgelijke aftelling heeft (zie Appendix A). Niet elke verzameling is echter *aftelbaar*; de verzameling van alle reële getallen bijvoorbeeld niet. De formules van een predikaatlogische taal waarin ieder reëel getal een naam heeft, heeft bijgevolg geen aftelling. Weliswaar geldt voor zulke 'overaftelbare' talen de vervulbaarheidsstelling ook, maar het bewijs vereist zwaardere middelen.

16.11.2 Lemma. Zij Φ een consistente verzameling formules; stel dat oneindig veel variabelen in Φ niet voorkomen. Dan is Φ vervulbaar.

Bewijs. Laat $\mathcal{L}$ een geschikt vocabulaire zijn voor Φ; laat

$$\psi_0, \psi_1, \psi_2, \psi_3, \ldots$$

een opsomming zijn van alle formules over $\mathcal{L}$. We definiëren nu een keten

$$\Phi_0 \subseteq \Phi_1 \subseteq \Phi_2 \subseteq \Phi_3 \subseteq \ldots$$

van consistente verzamelingen waarin oneindig veel variabelen niet voorkomen, als volgt.

$\Phi_0 = \Phi$.

Stel Φ_n is geconstrueerd. Dan definiëren we:

$$\Psi_n := \begin{cases} \Phi_n \cup \{\psi_n\} \text{ als dat consistent is,} \\ \Phi_n \text{ anders.} \end{cases}$$

Als ψ_n begint met een existentiële quantor, zeg $\psi_n = \exists x\varphi(x)$, en $\psi_n \in \Psi_n$, laat dan y de eerste variabele zijn die in Ψ_n niet voorkomt, en definieer:

$$\Phi_{n+1} = \Psi_n \cup \{\varphi(y)\}.$$

Anders $\Phi_{n+1} = \Psi_n$.

Het is duidelijk dat er nog oneindig veel variabelen zijn die in Φ_{n+1} niet voorkomen, en dat Ψ_n consistent is. Ook als $\Phi_{n+1} \neq \Psi_n$, is Φ_{n+1} consistent. Want stel maar dat $\Phi_{n+1} \vdash \bot$. Door intrekking van de laatst toegevoegde formule (deductiestelling!) krijgen we $\Psi_n \vdash \neg\varphi(y)$; omdat y in Ψ_n niet voorkomt, en $\Psi_n \vdash \exists y\varphi(y)$ (Voorbeeld 6(b)), volgt met existentie-eliminatie $\Psi_n \vdash \bot$, en daarvan weten we dat het niet waar is.

Tenslotte nemen we de limiet:

$$\Phi_\infty = \bigcup_{n=0}^{\infty} \Phi_n.$$

Die is maximaal consistent, net als de limiet in het bewijs van Lemma 6.6.12. Dus $\Phi_\infty \vdash \varphi$ impliceert $\varphi \in \Phi_\infty$, voor $\mathcal{L}$-formules φ.

Als $\exists x\varphi(x) \in \Phi_\infty$, dan is er een variabele y zo dat $\varphi(y) \in \Phi_\infty$. Want $\exists x\varphi(x)$ staat ergens in de opsomming $\langle\psi_n\rangle_{n\in\mathbb{N}}$, zeg als ψ_m. Dan is $\Phi_m \cup \{\psi_m\}$ consistent, en de constructie zorgt dat er een y is zo dat $\varphi(y) \in \Phi_{m+1}$.

Beschouw de termalgebra $\mathbf{T} := \mathbf{T}_{\mathcal{L}}(\mathrm{Var})$. Omdat de predikaatlogische afleidingsregels de termlogische omvatten, volgt uit het bewijs van Stelling 9.12 dat de relatie

$$\theta := \{\langle \mathbf{s}, \mathbf{t}\rangle \mid \mathbf{s}, \mathbf{t} \in T \text{ en } (\mathbf{s} \approx \mathbf{t}) \in \Phi_\infty\}$$

een congruentie is. Definieer: $A = T/\theta$. Laat $\mathbf{A}$ de expansie zijn van $\mathbf{T}/\theta$ met relaties

$$R^{\mathbf{A}} = \{\langle a_1, \dots, a_n\rangle \mid \text{er zijn } \mathbf{t}_1 \in a_1, \dots, \mathbf{t}_n \in a_n \text{ zo dat } R\mathbf{t}_1 \dots \mathbf{t}_n \in \Phi_\infty\},$$

voor alle n, voor alle n-plaatsige predikaatletters $R \in \mathcal{L}$.

Merk op dat ieder element van A oneindig veel variabelen bevat. Voor elke term $\mathbf{t}$ komen in de opsomming $\langle\psi_n\rangle_{n\in\mathbb{N}}$ namelijk alle formules $\exists v_i(v_i \approx \mathbf{t})$ voor; die zijn afleidbaar, dus als $\exists v_i(v_i \approx \mathbf{t}) = \psi_m$, dan is er een variabele y_i die in Φ_m niet voorkomt en waarvoor $(y_i \approx \mathbf{t}) \in \Phi_{m+1}$.

Zij $\boldsymbol{b}$ de bedeling

$$x \mapsto x/\theta.$$

We weten uit het bewijs van Stelling 9.14 dat $\boldsymbol{b}$ alle vergelijkingen in Φ_∞ vervult; en alle vergelijkingen die *niet* tot Φ_∞ behoren, en die dan ook niet uit Φ_∞ afleidbaar zijn, niet. We zullen nu verifiëren dat voor andere formules hetzelfde geldt:

(*) $$\mathbf{A} \models \varphi[\boldsymbol{b}] \text{ dan en slechts dan als } \varphi \in \Phi_\infty.$$

Als we (*) hebben bewezen, zijn we klaar: dan wordt Φ_∞, en dus ook Φ, vervuld door $\boldsymbol{b}$.

Als $\varphi = R\mathbf{t}_1 \dots \mathbf{t}_k$, dan $\mathbf{A} \models \varphi[\boldsymbol{b}] \Leftrightarrow \langle \mathbf{t}_1^{\mathbf{A}}[\boldsymbol{b}], \dots, \mathbf{t}_k^{\mathbf{A}}[\boldsymbol{b}]\rangle \in R^{\mathbf{A}}$. Uit het bewijs van Stelling 9.14 weten we dat $\mathbf{t}_i \in \mathbf{t}_i^{\mathbf{A}}[\boldsymbol{b}]$; dus volgens de definitie van $R^{\mathbf{A}}$,

$$\mathbf{A} \models \varphi[\boldsymbol{b}] \Leftrightarrow R\mathbf{t}_1 \dots \mathbf{t}_k \in \Phi_\infty.$$

De connectiefgevallen kunnen we nagenoeg letterlijk overnemen uit het bewijs van Lemma 6.6.13. Een universeel gequantificeerde formule $\forall x\psi$ is, bewijsbaar en logisch, equivalent met $\neg\exists x\neg\psi$ (cf. Oefening 4). Daarmee blijft slechts één geval over.

Zij $\varphi = \exists x\psi$. Dan $\mathbf{A} \models \varphi[\boldsymbol{b}] \Leftrightarrow$ er een $a \in A$ is zo dat $\mathbf{A} \models \psi[\boldsymbol{b}(a/x)]$. Stel $\mathbf{A} \models \psi[\boldsymbol{b}(a/x)]$. Als $y \in a$, dan $\boldsymbol{b}(y) = a$. Omdat a oneindig is, kunnen we $y \in a$

vinden substitueerbaar voor x in ψ. De Substitutiestelling impliceert dan (zie 15.9.4(a)) dat $\mathbf{A} \models [y/x]\psi[\boldsymbol{b}]$. Dan volgens inductiehypothese $[y/x]\psi \in \Phi_\infty$; dus $\Phi_\infty \vdash \varphi$. Omgekeerd, als $\varphi \in \Phi_\infty$ dan is er een y zo dat $[y/x]\psi \in \Phi_\infty$; dan volgens inductiehypothese $\mathbf{A} \models [y/x]\psi[\boldsymbol{b}]$, en daaruit volgt $\mathbf{A} \models \varphi[\boldsymbol{b}]$. ☒

Bewijs van de Vervulbaarheidsstelling. Laat Φ een consistente verzameling formules zijn. Als oneindig veel variabelen niet in Φ voorkomen, dan is Φ vervulbaar volgens het zojuist bewezen lemma. Zij anders, voor elke formule α, α' het resultaat van simultane vervanging van elke variabele (vrij of gebonden) door de variabele met de dubbele index: dus v_0 blijft, v_1 wordt v_2, v_2 wordt v_4, enzovoort. Laat $\Phi' = \{\varphi' \mid \varphi \in \Phi$. Dan voldoet Φ' aan de voorwaarden van het lemma; laat $\mathbf{A}$ een structuur zijn en $\boldsymbol{b}$ een bedeling zo dat $\mathbf{A} \models \Phi'[\boldsymbol{b}]$. Definieer een bedeling $\boldsymbol{b}'$ door

$$\boldsymbol{b}'(v_i) = \boldsymbol{b}(v_{2i}).$$

Beschouw nu een willekeurige formule $\varphi \in \Phi$. In §15.10 zagen we dat we een formule χ kunnen vinden waarin geen variabelen uit φ of φ' bindend voorkomen, en die logisch equivalent is met φ. Construeer nu χ^* uit χ door de indices van de *vrije* variabelen te verdubbelen; dan is χ^* logisch equivalent met φ'. Laat nu $\boldsymbol{b}^*$ de bedeling zijn die $\boldsymbol{b}(v_{2i})$ toekent aan v_i als v_i vrij voorkomt in χ, en verder overeenkomt met $\boldsymbol{b}$. Dan $\chi^{\mathbf{A}}[\boldsymbol{b}'] = \chi^{\mathbf{A}}[\boldsymbol{b}^*]$ volgens het eerste eindigheidslemma (15.8.1). In χ is de substitutie van v_{2i} voor v_i (simultaan voor alle i) toelaatbaar; dus $\chi^{\mathbf{A}}[\boldsymbol{b}^*] = (\chi^*)^{\mathbf{A}}[\boldsymbol{b}]$ volgens de Substitutiestelling. Maar $\varphi^{\mathbf{A}}[\boldsymbol{b}'] = \chi^{\mathbf{A}}[\boldsymbol{b}']$, en $(\chi^*)^{\mathbf{A}}[\boldsymbol{b}] = (\varphi')^{\mathbf{A}}[\boldsymbol{b}]$; daarmee is bewezen dat $\varphi^{\mathbf{A}}[\boldsymbol{b}'] = (\varphi')^{\mathbf{A}}[\boldsymbol{b}]$, en algemeen, dat $\mathbf{A} \models \Phi[\boldsymbol{b}']$. ☒

16.11.3 Volledigheidsstelling. Als $\Phi \models \psi$, dan $\Phi \vdash \psi$.

Bewijs. Met contrapositie. Stel $\Phi \nvdash \psi$; dan is $\Phi \cup \{\neg\psi\}$ consistent. (Als

$$\Phi \cup \{\neg\psi\} \vdash \bot,$$

dan leiden we ψ af uit Φ met reductio ad absurdum.) Dus $\Phi \cup \{\neg\psi\}$ is vervulbaar. Laat $\mathbf{A}$ een structuur zijn, en $\boldsymbol{b}$ een bedeling in $\mathbf{A}$, zo dat $\mathbf{A} \models \Phi[\boldsymbol{b}]$ en $\mathbf{A} \models \neg\psi[\boldsymbol{b}]$. Dan vormen $\mathbf{A}$ en $\boldsymbol{b}$ een bewijs dat $\Phi \not\models \psi$. ☒

Uit de Vervulbaarheidsstelling volgt net als in §6:

Compactheidsstelling. Elke eindig vervulbare verzameling predikaatlogische formules is vervulbaar.

16:9 Oefening. De stappen in bovenstaande bewijzen zijn niet altijd minimaal, en de toepasbaarheid van aangehaalde stellingen is niet altijd per se meteen duidelijk. Vul ontbrekende stappen aan tot je het betoog helemaal begrijpt.

❀ 16.12 Onvolledigheid en Onbeslisbaarheid

We zagen in §4 dat de waarheidstafelmethode gegarandeerd, zij het niet altijd snel, uitsluitsel geeft over de geldigheid van propositielogische gevolgtrekkingsschema's. De predikaatlogica gaat naar minstens twee kanten verder: de atomaire proposities hebben een interne structuur waar we rekening mee willen houden, en naast de connectieven hebben we quantoren. Daardoor wordt het verifiëren van de geldigheid van gevolgtrekkingsschema's onvergelijkbaar veel moeilijker. Hoe dat komt, dat zullen we hieronder oppervlakkig schetsen; wie echt wil weten hoe het zit, moet de literatuur raadplegen.

In de vorige subparagraaf is bewezen dat ons deductiesysteem voor de predikaatlogica volledig is, in de zin dat je er elk geldig gevolgtrekkingsschema mee kunt bewijzen. Er zijn echter meerdere opzichten waarin iets volledig kan zijn; in het bijzonder noemt men *een predikaatlogische theorie* 'volledig' als ze een volledige beschrijving geeft van een of andere structuur. Preciezer: $\mathcal{T}$ is volledig als er een structuur **A** bestaat voor de taal van $\mathcal{T}$ zo dat een *zin* φ in die taal afleidbaar is in $\mathcal{T}$ dan en slechts dan als $\mathbf{A} \models \varphi$. Of zonder een structuur te noemen: $\mathcal{T}$ is volledig als voor iedere zin φ in de taal van $\mathcal{T}$ geldt: ofwel $\vdash_{\mathcal{T}} \varphi$, òf $\vdash_{\mathcal{T}} \neg\varphi$. (En niet allebei, $\mathcal{T}$ moet dus consistent zijn.)

Het is niet moeilijk om volledige theorieën te definiëren ('neem als axioma's van $\mathcal{T}$ alle ware zinnen van **A**'), maar daarmee weet je nog niet wat erin zit. Noem een theorie $\mathcal{T}$ *effectief geaxiomatiseerd* als je een hanteerbaar procédé hebt om axioma's te herkennen. De stellingen van $\mathcal{T}$ hebben dan een als zodanig herkenbare afleiding. (Voorbeelden van effectief geaxiomatiseerde theorieën: die met eindig veel axioma's, zoals N; of theorieën met axiomaschema's als: $S^{n+1}x \not\approx x$ voor alle $n \geq 0$.) In 1931 bewees Kurt Gödel dat iedere effectief geaxiomatiseerde consistente predikaatlogische theorie die, echt of via een werkelijk uitvoerbare vertaling, een minimaal stukje getaltheorie omvat (de theorie N van 15.17(v) is ruim voldoende) onvolledig is.

In de theorie N kun je rijtjes coderen als getallen. (Denk aan unieke priemfactorontbinding, waarbij de exponenten van de successieve priemfactoren staan voor de elementen van het rijtje — er is een truc om zoiets zonder expliciete machtsverheffing te doen.) Je kunt zelfs een formule $A(x, y)$ construeren zo dat $\vdash_{\mathrm{N}} A(S^k0, S^m0)$ als k een afleiding codeert van de formule met code m, en $\vdash_{\mathrm{N}} \neg A(S^k0, S^m0)$ als dat niet het geval is. Gödel bedacht een formule ψ, met codegetal q, zo dat $\vdash_{\mathrm{N}} \psi \leftrightarrow \neg\exists x\, A(x, S^q0)$. Deze ψ kan niet bewijsbaar zijn, als N consistent is; en als N *waar* is, i.e. als de bewering in 15.19(v) juist is, is ook $\neg\psi$ niet afleidbaar. (Latere verfijningen hebben laten zien dat het beroep op waarheid vermeden kan worden.)

Voor de beslisbaarheid van de predikaatlogica is iets anders van belang, namelijk dat Gödel's bewijs aannemelijk maakt dat wanneer een eigenschap B beslisbaar is, voor de bijbehorende N-formule β geldt dat $\vdash_{\mathrm{N}} \beta(S^k0)$ als het object met code k de eigenschap heeft, en $\vdash_{\mathrm{N}} \neg\beta(S^k0)$ in het tegenovergestelde geval. Stel nu dat je een effectieve methode had om te beslissen of een predikaatlogische zin universeel geldig is of niet. Volgens de volledigheidsstelling kun je 'universeel geldig' vervangen door 'afleidbaar zonder blijvende aannamen'. Laat ν de conjunctie zijn van de universele afsluitingen van de axioma's van N. Dan kun je voor elke zin φ van de taal van N beslissen of $\vdash \nu \to \varphi$ of $\nvdash \nu \to \varphi$, en daarmee of $\vdash_{\mathrm{N}} \varphi$ of $\nvdash_{\mathrm{N}} \varphi$. Maar dan zou je voor elke formule in N kunnen bewijzen, ofwel dat hij bewijsbaar is, of dat hij niet bewijsbaar is; en we weten dat dat niet kan.

16:10 Oefening (Behmann). De *unaire predikaatlogica* is de predikaatlogica zonder gelijkheid of operatiesymbolen, en met alleen *unaire* predikaatletters. Bewijs dat de unaire predikaatlogica beslisbaar is. [Laat m het aantal predikaatletters zijn dat voorkomt in φ. Laat zien dat $\models \varphi$ als $\mathbf{A} \models \varphi$ voor alle **A** waarvan het universum precies 2^m elementen bevat.]

§17 Quantoreliminatie

Onder een *theorie* verstaan we in deze § een verzameling zinnen van de eerste orde-logica, over één of ander vocabulaire $\mathcal{L}$, die gesloten is onder afleidbaarheid; dat wil zeggen, als T een theorie is over $\mathcal{L}$, en φ een zin van $\mathcal{L}$, dan geldt:

$$\text{als } T \vdash \varphi, \text{ dan } \varphi \in T.$$

Een theorie T is *beslisbaar* als er een welomschreven, effectieve procedure bestaat om uit te maken of $\varphi \in T$ of niet; en anders *onbeslisbaar*. We zagen in §16 dat zelfs de theorie bestaande uit alle universeel geldige zinnen over $\mathcal{L}$ onbeslisbaar kan zijn. In deze § zullen we van een paar theorieën de beslisbaarheid bewijzen.

De propositielogica is beslisbaar (§4). Een voor de hand liggende strategie om een eerste orde-theorie T te beslissen is dan ook te proberen een verzameling B van handzame *basisformules* te definiëren, en dan te bewijzen dat in T elke formule equivalent is met een boolese combinatie van basisformules. Precies gezegd: voor elke formule φ over $\mathcal{L}$ moeten we een formule $\psi(p_0\ldots, p_{n-1})$ van de propositielogica vinden, en basisformules $\beta_0,\ldots, \beta_{n-1}$ zo dat

$$T \vdash \varphi \leftrightarrow \psi(\beta_0,\ldots, \beta_{n-1}).$$

Wanneer dat kan, voor een gegeven theorie T, dan zeggen we dat T *quantoreliminatie toelaat* over B.

17.1 Lemma. Zij T een eerste orde-theorie over een vocabulaire $\mathcal{L}$; en B een verzameling $\mathcal{L}$-formules (de basisformules). Laat B^+ de vereniging zijn van B met de verzameling der atomaire $\mathcal{L}$-formules. Dan laat T quantoreliminatie toe over B dan en slechts dan als voor elke variabele v en elk rijtje $\alpha_0,\ldots, \alpha_{n-1}$ van elementen van B^+ en negaties daarvan waar v in voorkomt, geldt dat er een boolese combinatie β bestaat van elementen van B zo dat

$$T \vdash \exists v(\alpha_0 \wedge\ldots\wedge \alpha_{n-1}) \leftrightarrow \beta.$$

Bewijs. Zij φ een formule over $\mathcal{L}$. Volgens de Prænexvormstelling (15:21) is φ logisch equivalent met een formule van de vorm

$$Q_1x_1\ldots\, Q_nx_n\gamma,$$

waarin $Q_1,\ldots, Q_n$ quantoren zijn, en γ, de propositionele matrix, quantorvrij is. Dus γ is zeker een boolese combinatie van elementen van B^+.

We mogen aannemen dat $Q_n = \exists$. Anders vervangen we $\forall x_n$ door $\neg\exists x_n\neg$: de tweede $\neg$ verdwijnt meteen in de propositionele matrix, en de eerste volgt na eliminatie van $\exists x_n$.

Schrijf γ in disjunctieve normaalvorm (§5), met de atomaire formules en de basisformules als atomaire proposities; zeg $\gamma \models\!\!\!\dashv \delta_1 \vee\ldots\vee \delta_k$, met δ_i $(1 \leq i \leq k)$ een conjunctie van (negaties van) elementen van B^+. Er geldt:

$$\exists x_n(\delta_1 \vee\ldots\vee \delta_k) \models\!\!\!\dashv \exists x_n\delta_1 \vee\ldots\vee \exists x_n\delta_k.$$

Zeg δ_i is $\alpha_0 \wedge\ldots\wedge \alpha_{m-1}$, met α_j $(0 \leq j < m)$ in B^+. Laat $\alpha_n,\ldots, \alpha_{m-1}$ de conjuncten zijn waar v niet in voorkomt. Dan is $\exists v(\alpha_0 \wedge\ldots\wedge \alpha_{m-1})$ logisch equivalent met $\exists v(\alpha_0 \wedge\ldots\wedge \alpha_{n-1}) \wedge \alpha_n \wedge\ldots\wedge \alpha_{m-1}$. Nu volstaat dat we

$\exists v(\alpha_0 \wedge \ldots \wedge \alpha_{n-1})$ kunnen vervangen door een boolese combinatie van basisformules. ⊠

17.2 Voorbeeld. Laat T de verzameling zijn van alle zinnen over het vocabulaire $\{0, S\}$ die afleidbaar zijn uit de axioma's

(1) $\quad x \not\approx 0 \leftrightarrow \exists y\, Sy \approx x,$

(2) $\quad Sx \approx Sy \to x \approx y,$

$(3+n)$ $\quad S^{n+1}x \not\approx x \qquad (n \in \mathbb{N}).$

(We laten buitenste universele quantoren weg.) Merk op dat de axioma's van T waar zijn in de structuur $\mathbf{N} = \langle \mathbb{N}, 0, S\rangle$ van de natuurlijk getallen met 0 en opvolgeroperatie: je zou je kunnen afvragen hoe T zich verhoudt tot de theorie $\mathrm{Th}(\mathbf{N})$ van alle zinnen die waar zijn in $\mathbf{N}$. In elk geval $T \subseteq \mathrm{Th}(\mathbf{N})$.

We zullen nu laten zien dat T quantoreliminatie toelaat. De basisformules zijn de atomaire formules.

Laat v een variabele zijn, en $\alpha_0, \ldots, \alpha_{n-1}$ atomaire formules, of negaties daarvan, waar v in voorkomt. We zoeken een quantorvrije formule β zo dat

$$T \vdash \exists v(\alpha_0 \wedge \ldots \wedge \alpha_{n-1}) \leftrightarrow \beta.$$

We mogen aannemen dat v in geen van de (on)gelijkheden α_i aan twee kanten voorkomt. Een gelijkheid $S^m v \approx S^n v$ kunnen we namelijk weglaten als $m = n$, want dan is ze afleidbaar, en we kunnen haar vervangen door $\perp$ als $m \neq n$, want dan is $S^m v \not\approx S^n v$ een stelling van T; voor een ongelijkheid geldt het omgekeerde. Stel nu dat v voorkomt in een atomaire α_i; zeg (zonder verlies van algemeenheid) α_0 is $S^m v \approx S^n a$; a is 0 of een variabele. Op grond van axioma (2) mogen we aannemen dat ofwel $m = 0$, of $n = 0$ en $m > 0$. In het eerste geval is $\exists v(\alpha_0 \wedge \ldots \wedge \alpha_{n-1})$ equivalent, in T, met $[S^n a/v](\alpha_1 \wedge \ldots \wedge \alpha_{n-1})$. (Ook als $n = 1$; de lege conjunctie is $\top$.) Neem aan dat we in het tweede geval verkeren: α_0 is $S^m v \approx a$. Als $\alpha_i = (S^r v \approx \mathbf{s})$, dan is α_i in T equivalent met $S^r S^m v \approx S^m \mathbf{s}$; en

$$\exists v(\alpha_0 \wedge \alpha_i)$$

is equivalent met $a \not\approx 0 \wedge \ldots \wedge a \not\approx S^{m-1}0 \wedge S^r a \approx S^m \mathbf{s}$. Zo elimineer je v uit alle gelijkheden in de conjunctie.

Tenslotte, als alle α_i ongelijkheden zijn, dan $T \models \exists v(\alpha_0 \wedge \ldots \wedge \alpha_{n-1})$. Want, zij $\alpha_i = (S^{m_i} v \not\approx \mathbf{t}_i)$. Laat $\boldsymbol{b}$ een bedeling zijn in een model $\mathbf{A}$ van T, en $a_i = \mathbf{t}_i^{\mathbf{A}}[\boldsymbol{b}]$, voor alle $i < n$. Dan zijn $0^{\mathbf{A}}, S^{\mathbf{A}}(0^{\mathbf{A}}), \ldots, (S^{\mathbf{A}})^n(0^{\mathbf{A}})$ allemaal verschillend (zo volgt uit (3)-$(3+n)$); minstens één daarvan moet dus verschillen van alle a_i $(i < n)$. ⊠

We concluderen dat iedere *zin* over het vocabulaire $\{0, S\}$ in T equivalent is met een boolese combinatie van gelijkheden $S^m 0 \approx S^n 0$. Die zijn in T zeker bewijsbaar of weerlegbaar, en daarmee kun je de waarheidswaarde van de boolese combinatie berekenen.

We zien nu ook dat $T = \mathrm{Th}(\mathbf{N})$. Want als $\varphi \in \mathrm{Th}(\mathbf{N})$, dan $\neg\varphi \notin \mathrm{Th}(\mathbf{N})$, dus $\neg\varphi \notin T$; maar als φ niet weerlegbaar is in T, dan is hij bewijsbaar, dus $\varphi \in T$.

Oefeningen.

17:1 Laat $T \cup \{\varphi, \psi\}$ een verzameling zinnen zijn over een vocabulaire $\mathcal{L}$. Bewijs (gebruik natuurlijke deductie):

(a) als $T \vdash \varphi$, dan $T \vdash \varphi \wedge \psi \leftrightarrow \psi$;

(b) als $T \vdash \neg\varphi$, dan $T \vdash \varphi \wedge \psi \leftrightarrow \perp$.

17:2* Een theorie U is *eindig axiomatiseerbaar* als er een eindige deelverzameling U_0 van U bestaat waar alle formules in U uit kunnen worden afgeleid. Is de theorie T van Voorbeeld 2 eindig axiomatiseerbaar?

17.3 Voorbeeld. Laat T de verzameling zijn van alle universeel geldige zinnen over het lege vocabulaire. De atomaire formules zijn dus gelijkheden tussen variabelen.

We willen bewijzen dat T quantoreliminatie toelaat. Als basisformules zullen de atomaire formules deze keer niet volstaan: het is immers op voorhand duidelijk dat T niet volledig is. Bijvoorbeeld, $\forall v_0 v_1\ v_0 \approx v_1$ is in sommige structuren waar, en in andere niet. Naast de atomaire formules gebruiken we zinnen $\sigma_1, \sigma_2, \ldots$; σ_m drukt uit dat er meer dan m dingen zijn. Een geschikte definitie is

$$\sigma_m = \forall v_0 \ldots v_{m-1} \exists v_m (v_m \not\approx v_0 \wedge \ldots \wedge v_m \not\approx v_{m-1}).$$

Laat $\alpha_0, \ldots, \alpha_{n-1}$ basisformules of negaties daarvan zijn, en v een variabele. We zoeken een boolese combinatie β van basisformules zo dat

$$\vdash \exists v(\alpha_0 \wedge \ldots \wedge \alpha_{n-1}) \leftrightarrow \beta.$$

We mogen aannemen dat elke α_i een gelijkheid of ongelijkheid is, want

$$\vdash \exists v(\sigma_m \wedge \varphi) \leftrightarrow \sigma_m \wedge \exists v \varphi.$$

Als v in α_{n-1} niet voorkomt, dan

$$\vdash \exists v(\alpha_0 \wedge \ldots \wedge \alpha_{n-1}) \leftrightarrow \exists v(\alpha_0 \wedge \ldots \wedge \alpha_{n-2}) \wedge \alpha_{n-1}$$

(enzovoort). Neem nu aan dat v in $\alpha_0, \ldots, \alpha_{n-1}$ wèl voorkomt.

We mogen aannemen dat v in geen van de (on)gelijkheden α_i aan twee kanten voorkomt. Een gelijkheid $v \approx v$ kunnen we namelijk weglaten, want die is afleidbaar, en een ongelijkheid $v \not\approx v$ kunnen we vervangen door $\perp$. Stel nu dat v positief voorkomt; zeg α_0 is $v \approx x$. Dan kunnen we in $\alpha_1, \ldots, \alpha_{n-1}$ overal v vervangen door x, α_0 schrappen, en de existentiële quantificatie weglaten.

Als laatste beschouwen we de mogelijkheid dat v uitsluitend in ongelijkheden voorkomt. Laat X de verzameling zijn van alle variabelen die in $\alpha_0, \ldots, \alpha_{n-1}$ voorkomen. Omdat

$$\exists v \varphi \mathrel{\vDash\!\!\!\!\dashv} \exists v(\varphi \wedge (x \approx y \vee x \not\approx y)) \mathrel{\vDash\!\!\!\!\dashv} \exists v(\varphi \wedge x \approx y) \vee \exists v(\varphi \wedge x \not\approx y)$$

mogen we aannemen dat voor alle $x, y \in X$, $x \approx y$ of $x \not\approx y$ één van de conjuncten is. Als $\exists v(\alpha_0 \wedge \ldots \wedge \alpha_{n-1})$ geen tegenspraak is, dan is

$$\{\langle x, y\rangle \mid \text{er is een } i < n \text{ zo dat } \alpha_i = (x \approx y)\}$$

een equivalentierelatie op X. Laat r het aantal der equivalentieklassen zijn van deze relatie — één van die klassen is $\{v\}$. Laat δ de conjunctie zijn van alle α_i waar v niet in voorkomt. Dan

$$\vdash \exists v(\alpha_0 \wedge \ldots \wedge \alpha_{n-1}) \leftrightarrow \sigma_{r-1} \wedge \delta. \qquad \boxtimes$$

We concluderen dat iedere *zin* over het lege vocabulaire logisch equivalent is met een boolese combinatie van basiszinnen σ_m ($m = 1, 2, \ldots$).

Merk op dat $\vdash \sigma_{m+1} \rightarrow \sigma_m$. We kunnen nu gemakkelijk een katalogus maken van alle volledige uitbreidingen van T. Ze worden geaxiomatiseerd door, respectievelijk,

$\neg\sigma_1$,
$\sigma_1 \wedge \neg\sigma_2$,
$\sigma_2 \wedge \neg\sigma_3$,
…
$\sigma_m \wedge \neg\sigma_{m+1}$,
…
$\{\sigma_1, \sigma_2, \sigma_3, \ldots\}$.

De laatste regel valt hier nogal uit de toon: een oneindige verzameling in plaats van een eindige, en dan nog wel een waarvan ieder individueel element overbodig is. De vraag dringt zich op of dat niet bondiger kan.

Het antwoord is *nee*. Stel dat deze theorie T_∞, de gelijkheidstheorie van oneindige verzamelingen, geaxiomatiseerd kon worden door een eindig stel axioma's in plaats van de boven omschreven verzameling Σ — dat we dan meteen kunnen conjungeren tot een enkel axioma φ. Dan geldt voor alle m

$$\varphi \models \sigma_m,$$

en omgekeerd $\Sigma \models \varphi$; uit de volledigheidsstelling volgt dat het laatste impliceert dat voor zekere $m_0, \ldots, m_{k-1}$,

$$\sigma_{m_0}, \ldots, \sigma_{m_{k-1}} \models \varphi,$$

en zelfs, als n de grootste is van $m_0, \ldots, m_{k-1}$, $\sigma_n \models \varphi$. Maar dan zou

$$\sigma_n \models \sigma_{n+1};$$

en dat is zeker niet het geval.

17:3 Oefening. Laat v een variabele zijn; δ een conjunctie van gelijkheden en ongelijkheden tussen variabelen die vervulbaar is in verzamelingen met meer dan m elementen, en niet in verzamelingen met m of minder elementen; en δ_0 wat overblijft van δ als je de (on)gelijkheden weglaat waar v in voorkomt.
Bewijs:
(a) Als $\models \delta \to v \approx w$ voor een variabele w verschillend van v, dan

$$\models \exists v\delta \leftrightarrow [w/v]\delta.$$

(b) Als $\models \delta \to v \not\approx w$ voor alle variabelen w verschillend van v die in δ voorkomen, dan $\models \exists v\delta \leftrightarrow \sigma_m \wedge \delta_0$.

17:4* Oefening. Laat T de theorie zijn van de *dichte lineaire orde zonder begin- of eindpunt*, de theorie over $\{<\}$ die wordt geaxiomatiseerd door

$x \nless x$,
$x < y \to y < z \to x < z$,
$x < y \vee x \approx y \vee y < x$
$x < z \to \exists y(x < y \wedge y < z)$,
$\exists y\, x < y$,
$\exists x\, x < y$.

(a) Laat zien dat T quantoreliminatie toelaat.
(b) Concludeer dat $T = \mathrm{Th}(\mathbb{Q}, <)$, de volledige theorie van de geordende verzameling der rationale getallen.
(c) Bewijs dat alle aftelbare modellen van T isomorf zijn.

Appendix A

Het keuze-axioma is de bewering

(AC) als $\mathcal{A}$ een collectie van niet-lege verzamelingen is, dan bestaat er een functie $f\colon \mathcal{A} \longrightarrow \bigcup\mathcal{A}$ zo dat voor alle $A \in \mathcal{A}, f(A) \in A$.

Een dergelijke f heet een *keuzefunctie* voor $\mathcal{A}$.

De status van dit axioma is niet onbetwist: het heeft verrassende gevolgen, en er bestaan andere aantrekkelijke axioma's over verzamelingen die ermee in strijd zijn. Twee eenvoudige gevolgen van het keuze-axioma zijn in het voorafgaande zonder bewijs aangeroepen. We zullen ze hieronder bewijzen. Vervolgens laten we zien dat de Priemideaalstelling (§11) voor aftelbare Boolealgebra's ook zonder het keuze-axioma bewijsbaar is; en we besluiten met een opmerking over opsommingen.

Het Lemma van Zorn

In het bewijs van de Priemideaalstelling in §11 wordt het Lemma van Zorn gebruikt. Dit is een uitspraak over geordende verzamelingen $\mathbf{X} = \langle X, \leq\rangle$. Een element b van X heet een *bovengrens* (in $\mathbf{X}$) van een verzameling $Y \subseteq X$ als $y \leq b$ voor alle $y \in Y$. Een *keten* in $\mathbf{X}$ is een verzameling $Y \subseteq X$ die totaal geordend is door $\leq$, dat wil zeggen, voor alle $y_1, y_2 \in Y$ geldt

$$y_1 \leq y_2 \text{ of } y_2 \leq y_1.$$

In het bijzonder is $\emptyset$ een keten, en ieder element van X is een bovengrens van $\emptyset$. Een element m is *maximaal* in $\mathbf{X}$ als $m \leq x$ alleen als $m = x$. Het Lemma luidt:

• Een geordende verzameling waarin elke keten een bovengrens heeft, bevat een maximaal element.

Laat $\mathbf{X}$ zo'n geordende verzameling zijn, en $\mathcal{K}$ de collectie van alle ketens in $\mathbf{X}$. Het is voldoende te laten zien dat de ordening $\langle\mathcal{K}, \subseteq\rangle$ een maximaal element heeft. Immers, laat M zo'n maximale keten zijn; M heeft een bovengrens m, en als m niet maximaal is, zeg omdat $m' > m$, dan is $M \cup \{m'\}$ een keten die M uitbreidt.

Neem een keuzefunctie f voor $\mathcal{P}X - \{\emptyset\}$. Definieer voor $K \in \mathcal{K}$:

$$U_K = \{x \in X \setminus K \mid K \cup \{x\} \in \mathcal{K}\}.$$

Laat $\mathbb{C}$ de collectie zijn van alle collecties $\mathcal{A} \subseteq \mathcal{K}$ die voldoen aan
1° $\emptyset \in \mathcal{A}$;
2° als $\mathcal{B} \subseteq \mathcal{A}$ en $\bigcup\mathcal{B}$ is een keten, dan $\bigcup\mathcal{B} \in \mathcal{A}$;
3° als $K \in \mathcal{A}$ en $U_K \neq \emptyset$, dan $K \cup \{f(U_K)\} \in \mathcal{A}$.
De collectie $\mathbb{C}$ is niet leeg, want $\mathcal{K} \in \mathbb{C}$. Dus $\bigcap\mathbb{C}$ bestaat; men verifieert eenvoudig dat $\bigcap\mathbb{C} \in \mathbb{C}$.

We bewijzen nu dat $\bigcap\mathbb{C}$ een keten van verzamelingen is. Definieer:

$$\mathcal{D} := \{K \in \bigcap\mathbb{C} \mid \text{voor alle } C \in \bigcap\mathbb{C}, C \subseteq K \text{ of } K \subseteq C\}.$$

Ons doel is, te bewijzen dat $\mathcal{D} \in \mathbb{C}$: dat impliceert dat $\bigcap\mathbb{C} \subseteq \mathcal{D}$.

Het is niet moeilijk in te zien dat $\mathcal{D}$ voldoet aan de voorwaarden 1° en 2°. Wat 3° betreft, veronderstel dat $K \in \mathcal{D}$ en $U_K \neq \emptyset$. Kort af:

$$K^+ := K \cup \{f(U_K)\}.$$

We moeten bewijzen dat $K^+ \in \mathcal{D}$. Daartoe definiëren we:

$$\mathcal{E} := \{C \in \bigcap\mathbb{C} \mid C \subseteq K^+ \text{ of } K^+ \subseteq C\}.$$

We willen bewijzen dat $\mathcal{E} \in \mathbb{C}$, want dan $\bigcap\mathbb{C} \subseteq \mathcal{E}$, en dus $K^+ \in \mathcal{D}$.

De verificatie van de voorwaarden 1° en 2° is weer eenvoudig. Voor 3° veronderstellen we dat $C \in \mathcal{E}$ en $U_C \neq \emptyset$. We schrijven:

$$C^+ := C \cup \{f(U_C)\}.$$

We moeten bewijzen dat $C^+ \in \mathcal{E}$. Uit $C \in \bigcap\mathbb{C}$ volgt $C^+ \in \bigcap\mathbb{C}$; omdat $K \in \mathcal{D}$ weten we

$$C^+ \subseteq K \text{ of } K \subseteq C^+.$$

In het eerste geval hebben we $C^+ \subseteq K^+$ en zijn we klaar. We nemen voor het vervolg dus aan dat $K \subseteq C^+$.

Omdat $C \in \mathcal{E}$ weten we dat $C \subseteq K^+$ of $K^+ \subseteq C$. In het tweede geval hebben we $K^+ \subseteq C^+$ en zijn we klaar. We houden dus het geval over dat

$$K \subseteq C^+ \text{ en } C \subseteq K^+.$$

Omdat $K \in \mathcal{D}$, $C \subseteq K$ of $K \subseteq C$. In het eerste geval, $C \subseteq K \subseteq C^+$. Dan $K = C$ (en $K^+ = C^+$); of $K = C^+$, dus $C^+ \subseteq K^+$. Het andere geval, $K \subseteq C \subseteq K^+$, gaat analoog.

Beschouw nu $M := \bigcup\bigcap\mathbb{C}$. Als $x, y \in M$, dan zijn er $K, L \in \bigcap\mathbb{C}$ zo dat $x \in K$ en $y \in L$. Maar $\bigcap\mathbb{C}$ is een keten, dus $L \subseteq K$ of $K \subseteq L$; en in beide gevallen, $x \leq y$ of $y \leq x$. Dus M is een keten. Dus (2°) $M \in \bigcap\mathbb{C}$. Als M niet maximaal is, dan $U_M \neq \emptyset$, en $M^+ := M \cup \{f(U_M)\} \in \bigcap\mathbb{C}$. Maar dan $M^+ \subseteq M$, een tegenspraak. ⊠

Het bovenstaande lemma werpt overigens een nieuw licht op Thomas' godsbewijs (15.24) in een oneindige wereld [G]. De inverse van een ordening is weer een ordening; de formulering voor de omgekeerde ordening is

• Een geordende verzameling waarin elke keten een benedengrens heeft, bevat een minimaal element.

Definieer nu $x \leq y$ als: $x \approx y \vee M^*xy$. Dan is $\leq$ een ordening. Versterk nu de eerste premisse (1°): *als* een keten van oorzaken oneindig terugloopt, dan heeft die keten als geheel een oorzaak. Dan heeft elke $\leq$-keten een benedengrens; er is dus een minimaal element, iets dat geen oorzaak heeft buiten zichzelf.

König's Lemma

In Oefening 4:6 wordt aangeraden om König's Lemma te gebruiken. Er zijn verschillende formuleringen van dit Lemma; het handigst voor de oefening is een in termen van bomen.

Een *boom* definiëren we als een geordende verzameling $\mathbf{X} = \langle X, \leq \rangle$
— die een kleinste element heeft, de *wortel*; en
— waarin de voorgangers van ieder element een eindige keten vormen.
Typische voorbeelden zijn verzamelingen van eindige rijtjes, geordend door de beginsegment-relatie, waarbij het lege rijtje de wortel is. Van deze aard zijn de (volledige) binaire boom $2^{<\omega}$ (rijtjes van nullen en enen); de binaire boom

van rijtjes van hoogstens vier nullen en hoogstens zes enen; en de Baire-boom $\mathbb{N}^{<\omega}$ (rijtjes van willekeurige natuurlijke getallen).

Een maximale keten in een boom noemen we een *tak*. Een boom is *eindig vertakkend* als elk element slechts eindig veel onmiddellijke opvolgers heeft. Het Lemma luidt:

• Een oneindige eindig vertakkende boom bevat een oneindige tak.

Laat $\mathbf{X}$ zo'n boom zijn. Laat voor elke $x \in X$, S_x de verzameling zijn van alle onmiddellijke opvolgers van x; en laat X' bestaan uit alle elementen van $\mathbf{X}$ met oneindig veel opvolgers. Als $x \in X'$, dan $S_x \cap X' \neq \emptyset$. Immers, x heeft eindig veel onmiddellijke opvolgers; en als geen daarvan oneindig veel opvolgers heeft, dan heeft ook x slechts eindig veel opvolgers. Laat f een keuzefunctie zijn voor $\{S_x \cap X' \,|\, x \in X'\}$. Definieer nu:

x_0 is de wortel van $\mathbf{X}$;

als $x_n \in X'$, dan $x_{n+1} = f(S_{x_n} \cap X')$.

Dan is x_n gedefinieerd voor elke $n \in \mathbb{N}$; want $x_0 \in X'$, en als $x_n \in X'$, dan ook $x_{n+1} \in X'$. Omdat steeds $x_{n+1} \in S_{x_n}$, en onze definitie van bomen uitsluit dat $\mathbf{X}$ een element bevat dat volgt op alle x_n, is $\{x_n \,|\, n \in \mathbb{N}\}$ de gezochte oneindige tak.

Maximale idealen in aftelbare ringen

Er is een belangrijk geval waarin we de Priemideaalstelling kunnen bewijzen *zonder* Zorn's Lemma te gebruiken. Neem aan dat de ring $\mathbf{R}$ *aftelbaar* is, dat wil zeggen, er is een opsomming

(*) $$r_0, r_1, r_2, \ldots$$

van alle elementen van $\mathbf{R}$. (De Boolese ring van bewijsbare equivalentie-klassen van formules van de propositielogica is van dit type.) We kunnen een maximaal ideaal construeren door gebruik te maken van deze opsomming.

Lemma. Zij $\mathbf{R}$ een ring. De doorsnede van een collectie van idealen van $\mathbf{R}$ is een ideaal.

Bewijs. Laat $\mathcal{I}$ bestaan uit idealen van $\mathbf{R}$; zij $D = \bigcap \mathcal{I}$. Dan $D \neq \emptyset$, want 0 behoort tot alle elementen van $\mathcal{I}$; als x, $y \in D$, dan geldt voor elke $I \in \mathcal{I}$ dat $x, y \in I$, dus $x - y \in I$, dus $x - y \in D$; en als $x \in D$ en $r \in R$, dan $x \in I$ voor elke $I \in \mathcal{I}$, dus xr en rx behoren tot I, dus xr en rx zijn elementen van D. ⊠

In het bijzonder is de doorsnede van alle idealen die een gegeven verzameling X omvatten, een ideaal, het ideaal *voortgebracht door* X, dat we noteren als $\mathrm{Id}(X)$. In 10.5.2 is bewezen dat, als I en J idealen zijn, $\mathrm{Id}(I \cup J) = I + J$; en in 10.5.3, dat voor een element a van een commutatieve ring $\mathbf{R}$ met 1, $\mathrm{Id}(a) = Ra$.

Laat nu $\mathbf{R}$ een ring zijn, opgesomd als in (*), en $x \in R - \{0\}$. Dan construeren we een maximaal ideaal M dat x niet bevat als vereniging van een keten

$$I_0 \subseteq I_1 \subseteq I_2 \subseteq \ldots$$

van idealen, die we als volgt definiëren:
$I_0 = \{0\}$. Laat I_n gedefinieerd zijn, zo dat $x \notin I_n$. Beschouw het ideaal $J := \mathrm{Id}(I_n \cup \{r_n\})$. Als $x \in J$, dan $I_{n+1} = I_n$; anders $I_{n+1} = J$.

De vereniging $M = \bigcup_{n \in \mathbb{N}} I_n$ is een ideaal dat x niet bevat. Stel dat $J \supset M$ een ideaal is. Zeg $r_k \in J - M$. Kennelijk $r_k \notin I_{k+1}$; dus $x \in \mathrm{Id}(I_k \cup \{r_k\}$. Maar dan zeker $x \in J$. ⊠

Opsommingen

Je kunt een verzameling formules, bijvoorbeeld FP, lexicografisch ordenen, zoals de woorden in een woordenboek. De ordening van de woorden volgt uit een gegeven ordening van de letters. Dat de propositielogica oneindig veel letters heeft is op zichzelf geen probleem. Wèl een probleem is dat je met eindig veel letters al oneindig veel formules kunt maken. Als p_0 in het alfabet na de connectieven komt (en de haakjes), dan gaan er oneindig veel formules aan p_0 vooraf — de formules zijn dan geordend, maar niet op de goede manier.

Een methode om het gewenste ordetype te bereiken, is de formules op te splitsen in eindige verzamelingen $\Phi_0, \Phi_1, \Phi_2, \ldots$, die dan ieder voor zich op een of andere manier, bijvoorbeeld lexicografisch, geordend worden. Je kunt bijvoorbeeld de connectieven en haakjes allemaal gewicht 1 geven, en p_i gewicht $i + 1$; en elke formule de som van de gewichten van de samenstellende symboolvoorkomens; $(\bot \to \bot)$ heeft dan gewicht 5, en $\neg p_0$ gewicht 2. In de opsomming komen eerst de formules van gewicht 1; dan de formules van gewicht 2; enzovoort.

Op analoge wijze kun je de formules van een predikaatlogische taal opsommen.

Als $X = \{x_0, x_1, x_2, \ldots\}$ een aftelbaar oneindige verzameling is, en R een equivalentierelatie van X, dan construeren we uit de gegeven opsomming van X een opsomming

$$X_0, X_1, X_2, \ldots$$

van X/R als volgt. Neem $X_0 = x_0/R$. Laat x_{k_1} het eerste element zijn in de opsomming van X dat niet tot X_0 behoort. Dan $X_1 = x_{k_1}/R$. Vervolgens zoeken we het eerste element dat niet tot $X_0 \cup X_1$ behoort. Laat dat x_{k_2} zijn; dan $X_2 = x_{k_2}/R$. Enzovoort. Als je op een gegeven moment geen nieuwe elementen van X meer kunt vinden, is de opsomming van equivalentieklassen eindig.

Appendix B

Boole schrijft [B, p.21]:

“To express the Proposition, Some *X*s are *Y*s.

If some *X*s are *Y*s, there are some terms common to the classes X and Y. Let those terms constitute a separate class V, to which there shall correspond a separate elective symbol v, then

$$v = xy$$

And as v includes all terms common to the classes X and Y, we can indifferently interpret it, as Some *X*s, or Some *Y*s.”

Elders geeft hij een lijstje:

Elke Y is X	$y = vx$
Geen Y is X	$y = v(1 - x)$
Minstens één Y is X	$vy = vx$
Minstens één Y is niet X	$vy = v(1 - x)$

Literatuur

(Een kort en tamelijk willekeurig lijstje, van een paar titels die in de tekst genoemd zijn en een paar suggesties voor verdere studie.)

[A] Thomas van Aquino: Summa contra Gentiles. 1264, beschikbaar op het Internet.

[B] George Boole: The Mathematical Analysis of Logic. Cambridge, 1847.

[C] Lewis Carroll: Through the looking-glass, and what Alice found there. Londen, 1872.

[D] Dirk van Dalen: Logic and structure. Berlijn, 1980.

[DM] Eric Temple Bell: The development of mathematics. New York 1940.

[G1] Semen Grigor'evich Gindikin: Algebraic logic. Vertaling van Алгебра логики в задачах door Robert H. Silverman. Наука 1972/ Springer 1985.

[G2] Jan de Graaf: *Waarheid, spel of taal?* Nieuw Archief voor Wiskunde, serie 5, deel 9, no. 1, 12-17.

[K1] Richard Kaye: The Mathematics of Logic. Cambridge, 2007.

[K2] Richard Kaye: *Circularity in Soundness and Completeness*. The Bulletin of Symbolic Logic 20 (2014), 24-38.

[Y] Marguerite Yourcenar: L'Œuvre au Noir. Parijs, 1968. Vertaald (met voorbehoud, *cela va de soi*: zover de doeltaal toelaat) als *Het Hermetisch Zwart*.