

Samenvatting Logica

Kyndylan Nienhuis

14 mei 2008

1 Propositielogica

Formules De formules zijn de elementen van de kleinste verzameling X die alle propositieletters en \perp en \top bevat, en die gesloten is onder de connectieven (dus als $\varphi, \psi \in X$ dan ook $\varphi \circ \psi \in X$). Die verzameling noemen we F_P .

Om aan te tonen dat χ geen formule is, maak je een verzameling Y waarvoor het vorige ook geldt, en waar χ niet inzit. Omdat F_P de kleinste is, geldt $F_P \subseteq Y$ en zie je dat χ geen formule is (zie §2).

Unieke leesbaarheid Een formule heeft slechts één constructieboom. (Is te bewijzen met haakjes tellen.)

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 $V_1(\varphi) = V_2(\varphi)$. Dit geeft aanleiding tot waarheidstafels.

Geldigheid Als φ voor alle valuaties waar is, heet φ een tautologie, en schrijft men $\models \varphi$. Twee formules φ en ψ zijn equivalent als $\varphi \leftrightarrow \psi$ een tautologie is. Verder schrijven we $\Phi \models \psi$ als voor iedere valuatie V , waarvoor voor alle $\varphi \in \Phi$ geldt dat $V(\varphi) = 1$, geldt dat $V(\psi) = 1$.

Om aan te tonen dat $\Phi \models \psi$ (of $\Phi \not\models \psi$) zijn semantische tableaux zeer geschikt (zie §4.3). Je probeert hierbij een valuatie te vinden, zodat alle $\varphi \in \Phi$ waar zijn, maar ψ onwaar. Lukt dit, dan heb je een tegenspraak. Lukt dit niet, dan concludeer je $\Phi \models \psi$.

Inductie naar de complexiteit van φ Een veel terugkomende bewijsmethode is inductie naar de complexiteit van φ . In de inductiebasis wordt gesteld dat φ een propositieletter is, gevolgd door een bewijs van de bewering in dit geval. In de tweede inductiestap wordt gesteld dat φ van de vorm $F(\varphi_1, \dots, \varphi_n)$ is (met F een connectief), en kan je gebruiken dat de bewering geldt voor φ_1 t/m φ_n om aan te tonen dat de bewering geldt voor φ .

Waarheidsfuncties Zij φ een formule die geen andere propositieletters bevat dan p_0, p_1, \dots, 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 geldt dat $f(V(p_0), V(p_1), \dots, V(p_{n-1})) = V(\varphi)$.

Omgekeerd, zij $f : \{0, 1\}^n \rightarrow \{0, 1\}$ een waarheidsfunctie. Dan is er een formule φ zo dat $\varphi^{(n)} = f$.

Disjunctieve normaalvorm Een formule is in disjunctieve normaalvorm als het een disjunctie van conjuncties van propositieletters en negaties van propositieletters is. Elke formule is equivalent met een formule in disjunctieve normaalvorm (zie §5.5 om te zien hoe je die formule kan vinden).

Functionele volledigheid Een connectief is een symbool voor een waarheidsfunctie. Laat C een verzameling connectieven zijn. Dan is $F_P[C]$ de kleinste verzameling X van uitdrukkingen die de propositieletters bevat, en die gesloten is onder alle connectieven in C (als $F \in C$ n -plaatsig is, en $\varphi_1, \dots, \varphi_n \in X$, dan ook $F(\varphi_1, \dots, \varphi_n) \in X$).

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

Om aan te tonen dat een stelsel C niet functioneel volledig is, kan je proberen aan te tonen dat voor alle φ geldt dat $\varphi^{(n)}(0, \dots, 0) = 0$ (of $\varphi^{(n)}(1, \dots, 1) = 1$). Je ziet nu dat bijvoorbeeld negatie niet uitdrukbaar is. Als dit niet werkt moet je een andere f zoeken die je niet kan uitdrukken met een $\varphi^{(n)}$.

Om aan te tonen dat een stelsel C wel functioneel volledig is, kan je soms een ander stelsel C' gebruiken waarvan bekend is dat het functioneel volledig is (bijvoorbeeld $\{\neg, \vee, \wedge\}$). Je gaat voor alle $G \in C$ op zoek naar een $\varphi \in F_P[C']$ met $G = \varphi^{(n)}$. Vervolgens gebruik je stelling 5.7.4 om te concluderen dat C functioneel volledig is.

Simultane substitutistelling Zijn $\varphi_0, \dots, \varphi_{n-1}, \psi \in F_P[C]$ en V een valuatie. We schrijven $\psi(\varphi_0, \dots, \varphi_{n-1})$ voor $[\varphi_0/p_0, \dots, \varphi_{n-1}/p_{n-1}]\psi$. Er geldt $V(\psi(\varphi_0, \dots, \varphi_{n-1})) = \psi^{(n)}(V(\varphi_0), \dots, V(\varphi_{n-1}))$.

Natuurlijke deductie Een afleiding is een rijtje formules, waarvoor geldt dat de formules of aannames zijn (gesloten of open), of volgen uit de vorige formules volgens een afleidingsregel. Een afleiding met de open aannames $\varphi_1, \dots, \varphi_n$ en eindigend met ψ heet een afleiding van ψ uit $\varphi_1, \dots, \varphi_n$. We schrijven $\varphi_1, \dots, \varphi_n \vdash \psi$ als er een afleiding van ψ uit $\varphi_1, \dots, \varphi_n$ bestaat.

De afleidingsregels zijn herhaling, introductie of eliminatie van \wedge, \vee of \rightarrow , ex falso sequitur quodlibet, en reductio ad absurdum. In het intuïtionistische deductiesysteem mag reductio ad absurdum niet gebruikt worden (we noteren $\varphi_1, \dots, \varphi_n \vdash_I \psi$ voor afleidbaarheid binnen dit systeem).

2 Termlogica

Algebra's Een algebra \mathfrak{A} van type \mathcal{F} bestaat uit een universum A , en een interpretatie I die aan ieder n -plaatsig symbool $F \in \mathcal{F}$ de operatie $F^{\mathfrak{A}} : A^n \rightarrow A$ toekent.

Een reduct van een algebra is een algebra met een kleiner type, en een expansie is een algebra met een groter type.

Een subalgebra van een algebra is een algebra met een kleiner universum, en een superalgebra is een algebra met een groter universum. De operaties moeten hierbij wel zodanig geïnterpreteerd worden dat wanneer ze toegepast worden binnen het kleinere universum de waarde binnen het kleinere universum blijft.

Termalgebra's De verzameling $T_{\mathcal{F}}(W)$ van termen over \mathcal{F} is de kleinste verzameling X die de variabelen $v \in W$ bevat, en waarvoor voor alle $Q \in \mathcal{F}$ geldt dat als $t_1, \dots, t_n \in X$ dan $Qt_1 \dots t_n \in X$.

Voor elk type \mathcal{F} is er een termalgebra \mathfrak{T} van dat type. Het universum daarvan is $T_{\mathcal{F}}(Var)$, en een $Q \in \mathcal{F}$ wordt geïnterpreteerd als $Q^{\mathfrak{T}}(t_1, \dots, t_n) = Qt_1 \dots t_n$.

Bedelingen Een homomorfisme $a : T_{\mathcal{F}}(Var) \rightarrow A$ noemen we een bedeling in A , en we noteren $t^{\mathfrak{A}}[a]$ voor $a(t)$. Voor bedelingen geldt het eindigheidslemma eveneens. (Een bedeling is een uitbreiding van een functie $Var \rightarrow A$).

Substituties Zijn t_1, \dots, t_k termen, en s een term of een vergelijking. We schrijven $s(t_1, \dots, t_k)$ voor $[t_1/x_1, \dots, t_k/x_k]s$ (en $s(x_1, \dots, x_k)$ voor s). Een substitutie is een bedeling van $T_{\mathcal{F}}(Var)$ naar $T_{\mathcal{F}}(Var)$.

Vergelijkingen Zijn t, s termen van type \mathcal{T} , dan heet $t \approx s$ een vergelijking over \mathcal{T} . Een bedeling a in \mathfrak{A} vervult $t \approx s$ als $t^{\mathfrak{A}}[a] = s^{\mathfrak{A}}[a]$, en we noteren $\mathfrak{A} \models (t \approx s)[a]$. Een vergelijking α is geldig in \mathfrak{A} als elke bedeling a vervult, en we schrijven $\mathfrak{A} \models \alpha$.

Als $\mathfrak{A} \models \alpha$ dan geldt er voor elke substitutie ρ dat $\mathfrak{A} \models \rho\alpha$ (zie §9.4).

Afleidingen Een equationele theorie \mathcal{E} bestaat uit een type \mathcal{F} en een stelsel vergelijkingen E over \mathcal{F} . Een afleiding in \mathcal{E} is een rijtje vergelijkingen over \mathcal{F} , waarvoor voor elke vergelijking α geldt dat het

of een aanname is,

of een instantie van een vergelijking uit E ,

of van de vorm $t \approx t$ is,

of verkregen is door vervangen van gelijken in eerdere vergelijkingen (als $s \approx t$ en $\beta(s)$ eerdere vergelijkingen zijn, en $\alpha = \beta(t)$).

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

Afgeleide regels zijn de symmetrieregels, de transitiviteitsregel, de compatibiliteitsregel, de substitutieregel en het snedelemma (zie §8.9).

Modellen Een model van een equationele theorie $\mathcal{E} = (\mathcal{T}, E)$ is een algebra van type \mathcal{T} waarin alle elementen van E geldig zijn. Als in ieder model van \mathcal{E} iedere bedeling die Γ vervult ook β vervult, dan is β een gevolg van Γ in \mathcal{E} , en schrijven we $\Gamma \models_{\mathcal{E}} \beta$.

Correctheid Als $\Gamma \vdash_{\mathcal{E}} \beta$ dan $\Gamma \models_{\mathcal{E}} \beta$.

Volledigheid Als $\Gamma \models_{\mathcal{E}} \beta$ dan $\Gamma \vdash_{\mathcal{E}} \beta$.

Congruëntierelaties Een equivalentierelatie is een congruentierelatie van \mathfrak{A} als de relatie compatibel is met \mathfrak{A} . Een relatie R is compatibel met \mathfrak{A} wanneer voor elke operatie Q van \mathfrak{A} geldt dat als $(a_1, b_1), \dots, (a_n, b_n) \in R$ dan ook $(Q(a_1, \dots, a_n), Q(b_1, \dots, b_n)) \in R$.

Zij \mathcal{E} een equationele theorie van type \mathcal{T} , en Γ een verzameling vergelijkingen van type \mathcal{T} . De door Γ in \mathcal{E} voortgebrachte congruentierelate $\Theta_{\mathcal{E}}(\Gamma)$ is gedefinieerd door $(t, s) \in \Theta_{\mathcal{E}}(\Gamma)$ dan en slechts dan als $\Gamma \vdash_{\mathcal{E}} t \approx s$.

Quotientalgebra's Zij \mathfrak{A} een algebra van type \mathcal{T} . Zij θ een congruentierelatie van \mathfrak{A} . Dan is \mathfrak{A}/θ , het quotient van \mathfrak{A} over θ , de algebra van type \mathcal{T} met als universum A/θ en als operaties $Q^{\mathfrak{A}/\theta}$ voor $Q \in \mathcal{T}$ gedefinieerd door $Q^{\mathfrak{A}/\theta}(a_1/\theta, \dots, a_n/\theta) = Q^{\mathfrak{A}}(a_1, \dots, a_n)/\theta$.

Zij \mathcal{E} een equationele theorie van type \mathcal{T} , en Γ een verzameling vergelijkingen over \mathcal{T} . Er geldt dat $T_{\mathcal{T}}(\text{Var})/\Theta_{\mathcal{E}}(\Gamma)$ een model is van \mathcal{E} . (Dit kan gebruikt worden om de volledigheidstelling te bewijzen.)

Dualiteit De duale \mathfrak{B}^{∂} van een Boole-algebra \mathfrak{B} is een Boole-algebra waarbij \wedge en \vee , en 1 en 0 van rol verwisseld zijn (dus $\wedge^{\mathfrak{B}^{\partial}} = \vee^{\mathfrak{B}}$). Er geldt $(t^{\partial})^{\mathfrak{B}^{\partial}}[b] = t^{\mathfrak{B}}[b]$.

Boolese ringen Een Boolese ring is een commutatieve ring met multiplicatief eenheidselement waarin de vermenigvuldiging idempotent is, dat wil zeggen $x \cdot x \approx x$ voor alle x . In een Boolese ring geldt $x \approx -x$.

Laat $\mathfrak{B} = (B, \neg, \wedge, \vee, 1, 0)$ 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 $\mathfrak{B}^r := (B, +, 1_B, 0, \cdot, 1)$ een Boolese ring (1_B , hoe de $-$ geïnterpreteerd wordt, is de indentiteit op B).

Laat $\mathfrak{R} = (R, +, -, 0, \cdot, 1)$ 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 $\mathfrak{R}^a = (R, \neg, \wedge, \vee, 1, 0)$ een Boole-algebra.

Idealen Een deelring \mathfrak{I} (subalgebra) van een ring \mathfrak{R} is een ideaal als voor alle $x, y \in R$, $x \in I$ impliceert dat xy en yx tot I behoren.

Zij \mathfrak{R} een ring, en $X \subseteq R$. Er geldt X is een ideaal van \mathfrak{R} dan en slechts dan als (i) $X \neq \emptyset$, (ii) als $x \in X$ en $r \in R$ dan $x \cdot r, r \cdot x \in X$, (iii) $x, y \in X$ dan $x - y \in X$.

Laat I en J idealen zijn van een ring \mathfrak{R} . Dan (a) is $I + J$ een ideaal van R , en (b) als K een ideaal is van \mathfrak{R} , en $I \cup J \subseteq K$, dan $I + J \subseteq K$.

Zij \mathfrak{R} een commutatieve ring met 1, en $a \in R$. Dan is (a) Ra een ideaal van \mathfrak{R} , en (b) als I een ideaal is van \mathfrak{R} , en $a \in I$, dan $Ra \subseteq I$.

Priemidealen Een ideaal P van een commutatieve ring \mathfrak{R} is priem als $P \neq R$ en voor alle $x, y \in R$ geldt: als $xy \in P$, dan $x \in P$ of $y \in P$.

Zij P een priemideaal van een Boolese ring \mathfrak{R} . Dan geldt voor alle $r \in R$: of $r \in P$, of $r + 1 \in P$. Er geldt $\mathfrak{R}/P \cong \mathbb{Z}/2\mathbb{Z}$. Een priemideaal verdeelt zo de elementen van een Boolese ring in ware en onware.

Laat \mathfrak{B} een Boole-algebra zijn. Een ideaal van \mathfrak{B} is een ideaal van de Boolese ring \mathfrak{B}^r . Een ideaal van \mathfrak{B}^{∂} heet een filter van \mathfrak{B} ; een priemideaal van \mathfrak{B}^{∂} een priemfilter van \mathfrak{B} .

Priemideaalstelling en de priemfilterstelling Zij I een ideaal van een Boole-algebra \mathfrak{B} , en $x \in B - I$. Dan bestaat er een priemideaal P van \mathfrak{B} dat I omvat en waar x niet in zit. In de duale stelling moet ideaal door filter vervangen worden.

3 Predikaatlogica

Predikaatlogische formules Een type \mathcal{L} is een verzameling operatiesymbolen en predikaatletters. De predikaatlogische taal bepaald door \mathcal{L} wordt in drie stappen gemaakt.

Allereerst heb je de termen: de variabelen zijn termen, en als t_1, \dots, t_n termen zijn en Q een operatiesymbool, dan is $Qt_1 \dots t_n$ een term.

Daarnaast heb je de atomaire formules: als t_1, \dots, t_n termen zijn en R een predikaatletter, dan is $Rt_1 \dots t_n$ een atomaire formule. De predikaatletter \approx wordt altijd in \mathcal{L} gedacht, en heeft zijn vaste betekenis.

Als laatste heb je de formules: atomaire formules zijn formules, als φ een formule is, dan zijn $\forall x\varphi$ en $\exists x\varphi$ formules, en als $\varphi_1, \dots, \varphi_n$ formules zijn en C een connectief, dan is $C\varphi_1 \dots \varphi_n$ een formule. De connectieven bestaan uit $\top, \perp, \neg, \wedge, \vee \rightarrow$ en \leftrightarrow .

Structuren Een structuur bestaat uit een universum, en een interpretatie die aan elk operatiesymbool een operatie op het universum toekent, en aan elke predikaatletter een relatie op het universum (met inachtneming van de plaatsigheid).

Bedelingen Zij $a \in A$, b een bedeling en x een variabele. We schrijven $(a/x); b$ voor de bedeling die a toekent aan x , en $b(v)$ aan een variabele $v \neq x$. We korten $(t^{\mathfrak{A}}[b]/x); b$ af tot $(t/x)b$.

De waarheidswaarde $\varphi^{\mathfrak{A}}[b]$ van φ in \mathfrak{A} onder b is op de gebruikelijke manier gedefinieerd, met de toevoeging dat $(\forall x\varphi)^{\mathfrak{A}}[b] = \bigwedge_{a \in A} \varphi^{\mathfrak{A}}[(a/x); b]$ en $(\exists x\varphi)^{\mathfrak{A}}[b] = \bigvee_{a \in A} \varphi^{\mathfrak{A}}[(a/x); b]$. Bij het evalueren mag gebruikt worden dat $\neg \bigwedge_{m \in M} f(m) = \bigvee_{m \in M} \neg f(m)$.

Eindigheidslemma's Voor bedelingen a en b die hetzelfde toekennen aan de variabelen in φ geldt $\varphi^{\mathfrak{A}}[a] = \varphi^{\mathfrak{A}}[b]$.

Zij \mathfrak{A} een structuur met reduct \mathfrak{A}' . Er geldt $\varphi^{\mathfrak{A}}[a] = \varphi^{\mathfrak{A}'}[a]$.

Zijn $\mathfrak{B} \leq \mathfrak{A}$ structuren, en φ een quantorvrije formule. Dan $\varphi^{\mathfrak{B}}[a] = \varphi^{\mathfrak{A}}[a]$.

Substitutie Een substitutie heeft geen invloed op gebonden variabelen. Om te zorgen dat quantificaties ook geen invloed hebben op variabelen in een gesubstitueerde term, is het begrip substitueerbaar ingevoerd. Een term t is substitueerbaar voor x in φ als x in φ niet vrij voorkomt binnen het bereik van een quantificatie over een variabele die voorkomt in t .

Zij t een voor x in φ substitueerbare term. Er geldt $([t/x]\varphi)^{\mathfrak{A}}[a] = \varphi^{\mathfrak{A}}[(t/x)a]$. Bij een term t en een formule φ is altijd een equivalente formule φ' te vinden waarin t substitueerbaar is (dit heet α -conversie).

Homomorfismen Een functie f is een homomorfisme van \mathfrak{A} naar \mathfrak{B} als voor alle operatiesymbolen Q geldt dat $f(Q^{\mathfrak{A}}(a_1, \dots, a_n)) = Q^{\mathfrak{B}}(f(a_1), \dots, f(a_n))$ en er voor elke relatiesymbool R geldt dat $(a_1, \dots, a_n) \in R^{\mathfrak{A}}$ impliceert dat $(f(a_1), \dots, f(a_n)) \in R^{\mathfrak{B}}$. Een homomorfisme is gesloten als de omkering ook geldt.