Tentamentips

Tomas Klos

14 december 2010

Samenvatting

In dit document vind je een aantal tentamen tips. Het gaat om fouten die ik op tentamens veel gemaakt zie worden, en die ik je liever niet zie maken. Ik geef in de appendix aan het eind van dit document, ten behoeve van je voorbereiding op het tentamen, ook de uitwerkingen van bepaalde opgaven uit de hoofdstukken over de boommethode (zowel propositie- als predicatenlogica), en over meta-beweringen. Ik raad je ook aan oude tentamenopgaven te maken, en niet enkel naar de uitwerkingen te kijken en te constateren: "ja, dat snap ik wel." Het is een hele andere vaardigheid zelf correcte antwoorden te bedenken dan te verifiëren dat gegeven antwoorden correct zijn.

1 Algemeen

Voorop het tentamenblad schrijf ik altijd dat je duidelijk moet zijn. Velen lijken dat niet te lezen, want regelmatig moet ik op zoek, bijvoorbeeld naar wat nou precies iemands antwoord is, bijvoorbeeld wanneer ik vraag of een bewering waar of onwaar is. Schrijf eerst op wat je denkt: waar of onwaar? Als je denkt waar, geef dan een bewijs. Als je denkt onwaar, geef dan een tegenvoorbeeld. Ik wil bij een tegenvoorbeeld ook altijd weten hoe je meent dat het tegenvoorbeeld de onwaarheid aantoont. Daar vraag ik dus ook altijd om, maar ook dat mist vaak, en dat kost kostbare punten.

Nog een algemene, niet zo belangrijke opmerking: een bewijs begint met het woord "Bewijs" en eindigt met "QED." Dat gebruik je dus niet als je onwaarheid van een bewering met een tegenvoorbeeld aantoont.

2 Boommethode

Net als bij andere vragen, is het dus ook bij vragen over de boommethode belangrijk dat je duidelijk bent, bijvoorbeeld over je antwoord. Bedenk verder bij het maken van opgaven volgens de boommethode, dat op elke formule altijd **precies één regel toepasbaar** is.

De meeste gemaakte fout is het toepassen van regels van de boommethode op *echte subformules* van een formule. Wanneer je je een formule (zowel in de propositie- als in de predicatenlogica) voorstelt als een ontledingsboom, dan mag je alleen een regel toepassen die past bij het connectief dat (of de kwantor die) in de **bovenste knoop** staat, of in de één na bovenste wanneer de bovenste een negatie is. Hieronder volgt een aantal voorbeelden.

- Op een formule als $\neg A \to \neg B$ moet je een $\to$-regel toepassen, en deze formule herschrijven naar $\neg\neg A \vee \neg B$. Let op dat je deze regel (en anderen) *exact* toepast. De regel zegt dat een implicatie $A \to B$ moet worden herschreven naar $\neg A \vee B$, dus de disjunctie van de negatie van het antecedent en het consequent. In de formule hierboven is het antecedent $\neg A$ en het consequent $\neg B$, zodat de herschrijving wordt $\neg\neg A \vee \neg B$. Voor alle duidelijkheid: iets anders is fout.

- Op een formule als $\neg(A \to B)$ moet je de andere $\to$-regel toepassen, namelijk die voor de *negatie* van een implicatie. Deze formule wordt dus herschreven naar $A \wedge \neg B$, en **NIET** naar $\neg(\neg A \vee B)$. In dat tweede geval pas je namelijk de andere $\to$-regel toe op een *echte subformule* van de formule $\neg(A \to B)$, en dat is niet toegestaan.

- Op een formule als $(A \vee B) \vee (B \to \neg C)$ moet je een $\vee$-regel toepassen, waarbij je dus de tak splitst en $A \vee B$ in één tak zet, en $B \to \neg C$ in de andere tak. Pas daarna mag je de eerste tak opnieuw splitsen met A en B in aparte takken, en in de tweede tak $B \to \neg C$ herschrijven naar $\neg B \vee \neg C$.

- Op een formule als $\neg(\neg A \vee C)$ moet je de andere $\vee$-regel toepassen, en deze formule herschrijven naar $\neg\neg A \wedge \neg C$ (dus **NIET** naar $A \wedge \neg C$, is het je duidelijk waarom niet?).

- Op een formule als $\neg\neg A \wedge (B \to A)$ moet je een $\wedge$-regel toepassen, en de beide subformules $\neg\neg A$ en $B \to A$ op afzonderlijke regels plaatsen. *Daarna* pas mag je $\neg\neg A$ herschrijven naar A, en $B \to A$ naar $\neg B \vee A$, doe dat niet tegelijkertijd.

Wat hierboven staat geldt ook als de formules A, B, en C zelf weer staan voor gekwantificeerde formules.

- Op een formule als $\neg\forall x(P(x) \to Q(x)) \vee \exists y B(y)$ bijvoorbeeld, moet je een $\vee$-regel toepassen, waarbij je de tak splitst en $\neg\forall x(P(x) \to Q(x))$ in de ene tak zet en $\exists y B(y)$ in de andere. Daarna mag je de formule in de eerste tak herschrijven naar $\exists x \neg(P(x) \to Q(x))$ etc., en de formule in de tweede tak naar $B(a)$ of $B(b)$ of zo, zolang je voor y maar een *nieuwe naam* gebruikt.

- Op een formule als $\exists x(A(x) \vee B(x))$ moet je een $\exists$-regel toepassen: je moet een *nieuwe naam* voor x invullen, omdat deze formule zegt dat er een object in het domein bestaat waarvoor $A(x) \vee B(x)$ geldt, en dan mag je niet veronderstellen dat dit geldt voor een object waarover je (in *deze* tak van de boom) al iets anders hebt aangenomen. Als je dus al een keer $x := a$ hebt gebruikt, moet je nu $x := b$ of $x := c$ of zo gebruiken: $A(b) \vee B(b)$.

- Op een formule als $\neg\exists x(A(x) \vee B(x))$ moet je de andere $\exists$-regel toepassen, namelijk die waarbij je $\neg\exists x(A(x) \vee B(x))$ vervangt door $\forall x \neg(A(x) \vee B(x))$.

- Op een formule als $\forall x(P(x) \to Q(x))$ moet je een $\forall$-regel toepassen, namelijk die waarbij je voor x een term invult, bijvoorbeeld $P(a) \to Q(a)$, of $P(b) \to Q(b)$ of nog iets anders. Je mag bij deze regel de term invullen die je wil, ook als die al eerder in de tak is gebruikt: de formule zegt namelijk dat de formule geldt *voor alle* x.

- Op een formule als $\neg\forall x(A(x) \vee B(x))$ moet je de andere $\forall$-regel toepassen, namelijk die voor de negatie van een $\forall$. Als er wordt gezegd dat *niet voor alle* x een uitspraak geldt, dan moet er een x bestaan waarvoor de uitspraak niet geldt (anders zou de uitspraak *wel* voor alle x gelden).

Het is handig om zoveel mogelijk eerst ∃-regels toe te passen, en nieuwe namen voor variabelen te substitueren. Daarna mag je die naam ook substitueren voor universeel gekwantificeerde variabelen (∀-regel), omdat zo'n formule zegt dat een uitspraak *voor alle* elementen in het domein geldt, en dus ook voor het element dat je bij $\exists x$ hebt gesubstitueerd. Als je kunt kiezen en je past eerst de ∀-regel toe, bijvoorbeeld door $x := a$ te substitueren, moet je daarna bij het toepassen van een ∃-regel een nieuwe naam, bijvoorbeeld $x := b$ substitueren, en daarna nog een keer de ∀-regel toepassen en $x := b$ substitueren.

Ook is het handig om formules zoveel mogelijk in de stam van de boom af te breken tot literalen. Als je dat niet doet, kan het gebeuren dat je dezelfde herschrijvingen in verschillende takken moet herhalen. Soms is dat overigens niet te vermijden natuurlijk. Als je wil oefenen met het maken van bomen, geef ik aan het eind van dit document (in appendix A) de antwoorden voor opgave 5.3.2 uit het dictaat *Logica*, p. 65-66. De beweringen in opgave 5.3.1 zijn allemaal waar, zoals ook in de opgave staat. In appendix B geef ik de antwoorden voor opgave 11.4.1 over bomen voor predicaatlogische beweringen. (Mocht je het met een antwoord niet eens zijn, neem dan even contact met me op.)

3 Verzamelingen

Beweringen over verzamelingen zijn waar of onwaar. Geef altijd duidelijk aan wat je denkt dat het correcte antwoord is: waar of onwaar. Dat mist vaak, en soms is rest van het antwoord ook nog eens zo onduidelijk, dat ik niet eens weet wat er bedoeld wordt.

Als een bewering onwaar is, moet je **specifieke verzamelingen** geven die dat aantonen, en ook uitleggen hoe die verzamelingen onwaarheid aantonen. Beschouw bijvoorbeeld de volgende bewering.

Bewering. *Voor alle verzamelingen A en B geldt: Als $A \subseteq B$, dan $B \subseteq A$.*

Deze bewering is niet waar. De bewering is een implicatie, die onwaar is als het antecedent waar is, maar het consequent onwaar.[1] Dit wordt aangetoond door verzamelingen $A = \{0\}$ en $B = \{0, 1\}$. Voor deze verzamelingen geldt namelijk wel dat $A \subseteq B$, omdat alle elementen van A ook in B zitten, maar niet dat $B \subseteq A$, omdat het element 1 wel in B maar niet in A zit.

Als een bewering over verzamelingen wel waar is, moet een bewijs dat duidelijk maken. Hierbij moet je gebruik maken van de *definities* van de begrippen die in de beweringen worden gebruikt, bijvoorbeeld de deelverzamelingrelatie, de machtsverzameling, en operaties als doorsnede, vereniging en complement. Zorg dus dat je deze definities kent en kunt gebruiken. Als voorbeeld:

Bewering. *Als $A \subseteq B$, dan $B^c \subseteq A^c$.*

Deze bewering is waar. Het is een implicatie, die we bewijzen door het antecedent voor waar aan te nemen en te laten zien dat onder die aanname het consequent logisch volgt.

Ik wil in een bewijs over verzamelingen geen uitspraken tegenkomen als "dus is verzameling x *groter dan* verzameling y" of zo. Er zijn hele duidelijke definities van de verschillende begrippen, en die wordt je geacht te gebruiken, anders niets.

[1] Strikt genomen is de bewering een gekwantificeerde uitspraak, want hij zegt dat een implicatie waar is voor alle mogelijke verzamelingen A en B. Dat dit onwaar is, kan worden aangetoond door specifieke verzamelingen A en B te geven waarvoor de implicatie onwaar is; dan geldt de implicatie namelijk *niet voor alle* verzamelingen A en B.

Bewijs (nogal uitgebreid). Stel dat $A \subseteq B$, dus dat (definitie!) voor alle x geldt dat als $x \in A$, dan ook $x \in B$. Te bewijzen is dat $B^c \subseteq A^c$, dus dat (definitie!) voor alle x geldt dat als $x \in B^c$, dan ook $x \in A^c$. Een "voor alle" bewijs kunnen we geven door (bewijsmethode!) voor een willekeurig element te laten zien dat de implicatie geldt. Neem dus een willekeurig element $e \in B^c$, zodat $\neg(e \in B)$. We moeten nu laten zien dat $e \in A^c$. (Op het college heb ik aangegeven dat een voor de hand liggende bewijsmethode in de context van complementen, het bewijs uit het ongerijmde is.) Neem, ten behoeve van een bewijs uit het ongerijmde, aan dat $e \in A$. Volgens onze aanname dat $A \subseteq B$ geldt nu ook $e \in B$. Maar we hebben e willekeurig gekozen uit B^c, dus geldt $\neg(e \in B)$, wat een tegenspraak oplevert. Er kan dus niet gelden dat $e \in A$, zodat we concluderen dat $e \in A^c$. Omdat e willekeurig was gekozen uit B^c, geldt voor alle $x \in B^c$, dat $x \in A^c$, oftewel dat $B^c \subseteq A^c$. QED

4 Fitch

Tsja, Fitch .... Oefenen, oefenen, oefenen. Maar zonder dollen: de patronen die toegestaan bij de verschillende Fitch-regels zijn (wederom) heel duidelijk omschreven, dus als je die in je hoofd hebt, kan er weinig misgaan, behalve dat je het niet "ziet" (daarover hieronder meer). Het is echt als een puzzel: ik geef je een aantal premissen, en jij moet de juiste regels in de juiste volgorde zetten om op de conclusie uit te komen. Blijf zowel van boven naar beneden als van beneden naar boven denken: de premissen moet je gebruiken, dus daar moet je eliminatieregels op toepassen, en de conclusie moet je tevoorschijn toveren, dus daar moet je een introductie-regel (of $\neg$-introductie, oftewel bewijs uit het ongerijmde) op toepassen. Verder zijn er vaak meerdere mogelijkheden, maar voor alle geldige afleidingen geldt dat de regels op de juiste manier zijn toegepast.

Een andere goede richtlijn is dat je altijd moet beginnen met het openen van een hypothese-interval voor elke premisse, en dat je de conclusie moet afleiden binnen al die hypothese-intervallen: de conclusie staat op de laatste regel, en links van de conclusie staan zoveel verticale lijnen als de redenering premissen heeft. (Zie de uitgebreide beschrijving over de regels van Fitch op Blackboard: `http://www.st.ewi.tudelft.nl/~tomas/TI1300/TI1300fitchHandout.pdf` maar vooral de extra uitleg hier: `http://www.st.ewi.tudelft.nl/~tomas/TI1300/TI1300fitchExtra.pdf` en veel voorbeelden van afleidingen (ook uit het dictaat) hier: `http://www.st.ewi.tudelft.nl/~tomas/TI1300/TI1300fitchAfleidingen.pdf`.)

Nog een waarschuwing over oefenen: probeer eerst uit alle macht om afleidingen zelf te maken voordat je naar antwoorden gaat kijken: op het moment dat je een correcte afleiding ziet, heb je de kans verkeken om zelf de benodigde creativiteit aan de dag te leggen. Dat is vaak het belangrijkst: "het zien," of doorhebben hoe het moet. Dit inzicht volgt meestal pas na een aantal afleidingen. Net als iedereen kon ik dit zelf eerst ook niet, maar door het gewoon een aantal keer te doen, kreeg ik er gevoel voor, voor hoe je die regels in elkaar kunt steken om te bereiken wat je wil. De afleidingsstrategieën die in het dictaat staan (p. 79–80) kun je dus weliswaar gebruiken als je een afleiding gaat maken, maar beter is het als je zelf deze strategieën ontdekt op basis van je ervaring in het maken van afleidingen.

5 Meta-beweringen

Voor metabeweringen geldt in zekere zin hetzelfde als voor verzamelingen: het is erg belangrijk dat je je realiseert wat bepaalde symbolen of concepten betekenen, en dat je daar de definities van kent en er mee kunt redeneren.

Als voorbeeld de metabewering van het tentamen van November 2010.

Bewering. *Als* $\sim (A \models B)$, *dan* $A \models \neg B$.

Wat staat hier nou eigenlijk? Als $\sim (A \models B)$, dus als $A \models B$ niet waar is, oftewel als B geen logisch gevolg is van A, dan moet $\neg B$ logisch gevolg van A zijn .... Dat is toch zeker niet waar? Het kan toch wel zo zijn dat noch een formule, noch de negatie ervan uit een andere formule volgt?

Velen dachten dat deze bewering waar was, en dat kwam door verkeerd begrip van de notie van logisch gevolg $\models$. Wanneer $A \models B$, betekent dit dat alle valuaties die model zijn van A, ook model zijn voor B. Als dit niet waar is (dus als $\sim (A \models B)$ waar is), dan geldt dus *niet voor alle* valuaties dat als ze model zijn voor A, ze ook model zijn voor B. Dan moet er dus tenminste één valuatie voor A bestaan die geen model is voor B (en dus wel voor $\neg B$). Maar dat betekent nog niet dat *alle* valuaties die model zijn voor A ook model zijn voor $\neg B$! Toch is dit hoe velen de uitspraak $\sim (A \models B)$ hebben geïnterpreteerd.

Een andere foute interpretatie die ik veel tegenkwam is dat mensen het hadden over $v(A \models B) = 0$ of 1, of ook $v(\sim (A \models B)) = 1$ of zo. Valuaties zijn functies die waarheidswaarden toekennen aan propositievariabelen, en we hebben tijdens het college afgesproken dat we die ook gebruiken voor het toekennen van waarheidswaarden aan formules (waarvoor we oorspronkelijk de functie v^+ gebruikten). Maar $A \models B$ is geen formule! A en B zijn wel formules (of in elk geval metavariabelen die *staan voor* formules), dus het heeft *wel* zin om te spreken over $v(A)$ en $v(B)$, maar dus *niet* over $v(A \models B)$, $v(\models A \to B)$ of iets dergelijks.

De bewering hierboven is zoals gezegd niet waar, en dat wordt aangetoond door een tegenvoorbeeld, waarbij je voor A en B **specifieke** formules uit $PROP$ neemt (net zoals je in een tegenvoorbeeld voor een onware bewering over verzamelingen zoals hierboven, de verzamelingen A en B voor **specifieke** verzamelingen laat staan—hierboven $A = \{0\}$ en $B = \{0, 1\}$). In het geval van deze metabewering wordt een tegenvoorbeeld gevormd door de formules $A = p$ en $B = q$. Zoals ik hierboven al meldde, vind ik het ook belangrijk dat je laat zien dat je begrijpt hoe bepaalde formules de onwaarheid van een bewering duidelijk maken, dus **uitleg hoort altijd bij een tegenvoorbeeld**! In dit geval leg je dan uit dat de gegeven formules het antecedent van de implicatie (wat de vorm van deze bewering is) waar maken, maar het consequent onwaar. Met $A = p$ en $B = q$ geldt wel dat $\sim (A \models B)$, want niet voor alle valuaties geldt nu dat als $v(A) = 1$, dan ook $v(B) = 1$. Neem bijvoorbeeld een valuatie w met $w(p) = 1$ en $w(q) = 0$: die is wel model voor A maar niet voor B. Voor deze formules $A = p$ en $B = q$ geldt alleen niet dat $A \models \neg B$, want niet voor alle valuaties geldt dat als $v(A) = 1$, dan ook $v(\neg B) = 1$. Neem bijvoorbeeld een valuatie s met $s(p) = s(q) = 1$: die valuatie is wel model voor A, maar niet voor $\neg B$, want $s(\neg q) = 1 - s(q) = 1 - 1 = 0$.

Als je wil oefenen met de meta-beweringen in het dictaat, probeer ze dan te maken. Aan het eind van dit document (in appendix C) kun je je antwoorden controleren, maar kijk er pas naar als je zelf een serieuze poging hebt gedaan om een bewijs of tegenvoorbeeld te leveren. Dek bovendien de antwoorden af met een papiertje, zodat je niet per ongeluk het antwoord op de volgende opgave ziet.

6 Inductie

6.1 Volledige Inductie

Dit ging dit jaar beter dan eerdere jaren. Ik heb dan ook veel nadruk gelegd op het voorkomen van de meest gemaakte fout die bij inductie wordt gemaakt, en dat is de volgende. Zowel in de basis- als in de inductiestap wordt vaak (foutief dus) hetgeen te bewijzen is voor waar aangenomen (in de inductiestap van het eerste inductiebewijs tijdens het college bijvoorbeeld dat $\sum_{i=1}^{k+1} i = \frac{(k+1)(k+2)}{2}$), en vervolgens met een aantal stappen aangetoond dat $1 = 1$ of zo, of dat een andere contradictie niet optreedt. Dat is niet de manier waarop dit hoort te verlopen.

Zowel in de basis- als in de inductiestap moet vaak een gelijkheid ($=$) of een ongelijkheid ($\leq$) worden bewezen. Dat doe je door te beginnen met dat wat aan de linkerkant van de (on)gelijkheid staat, en daar operaties op uit te voeren totdat je bij de rechterkant uitkomt. Als je in al die stappen alleen gelijkheden ($=$) gebruikt, heb je aangetoond dat de linkerkant gelijk is aan de rechterkant. Als je naast gelijkheden nog één of meerdere keren een ongelijkheid hebt gebruikt (maar wel steeds dezelfde, dus niet zowel $\leq$ als $\geq$), heb je aangetoond dat die ongelijkheid geldt tussen de linker- en de rechterkant. Als voorbeeld dat eerste bewijs van het college.

Stelling. *Voor alle natuurlijke getallen ≥ 1 geldt dat*

$$\sum_{i=1}^{n} i = \frac{n(n+1)}{2}.$$

(Dit was de formule waarmee Gauss volgens de legende zo snel de som oploste die de leraar hem en zijn klas gaf, namelijk om de getallen 1 t/m 100 bij elkaar op te tellen.)

Bewijs (nogal uitgebreid). We noemen $P(n)$ de eigenschap (P voor Predicaat—dit is een uitspraak in een eerste-ordetaal, dus in de predicatenlogica) dat de som van de eerste n getallen, oftewel $\sum_{i=1}^{n} i$, gelijk is aan $\frac{n(n+1)}{2}$. We willen bewijzen dat alle natuurlijke getallen groter dan of gelijk aan 1 die eigenschap hebben, oftewel dat $P(n)$ waar is voor alle $n \geq 1$.

Basis ($n = 1$): In de basisstap moeten we aantonen dat het basisgeval de genoemde eigenschap heeft, dus dat $P(n)$ geldt wanneer we $n = 1$ invullen. Is het dus zo dat $\sum_{i=1}^{n} i = \frac{n(n+1)}{2}$ waar is als $n = 1$? Wel, als $n = 1$ geldt

$$\sum_{i=1}^{n} i = \sum_{i=1}^{1} i = 1 = \frac{2}{2} = \frac{1 \cdot 2}{2} = \frac{1(1+1)}{2} = \frac{n(n+1)}{2}.$$

In de eerste 2 stappen (de eerste 2 '$=$' tekens dus) vul ik gewoon in dat $n = 1$ en werk ik de sommatie uit, daarna ga ik van 1 naar $\frac{2}{2}$ en verder, omdat ik alvast uitkijk naar waar ik wil uitkomen, namelijk bij $\frac{n(n+1)}{2}$.

Inductiestap: Hier moeten we laten zien dat elk getal de eigenschap 'doorgeeft' aan het volgende getal—als dominostenen die omvallen, zoals ik op het college heb uitgelegd. Dat wil zeggen dat we voor elk getal $n \geq 1$ moeten laten zien dat **als** n de eigenschap heeft, **dan** $n + 1$ ook de eigenschap heeft. Met andere woorden, we moeten voor alle $n \geq 1$ de implicatie $P(n) \to P(n+1)$ bewijzen. Dit vraag om een 'voor alle' bewijs, dus we nemen een willekeurige $k \geq 1$, waarvoor we moeten bewijzen dat $P(k) \to P(k+1)$. We nemen dus aan dat $P(k)$ waar is, en leiden onder die aanname af dat $P(k+1)$ ook waar is. De aanname dat $P(k)$ waar is, is de **inductiehypothese**, *schrijf die altijd op en noem hem ook inductiehypothese of IH*. De inductiehypothese houdt in dat we aannemen dat $\sum_{i=1}^{k} i = \frac{k(k+1)}{2}$. Nu moeten we aantonen dat $P(k+1)$ ook waar is, oftewel dat $\sum_{i=1}^{k+1} i = \frac{(k+1)(k+2)}{2}$. Dat gaat als volgt, waarbij we dus beginnen met de linkerkant $\sum_{i=1}^{k+1} i$ en in een aantal gelijkheden moeten toewerken naar de rechterkant $\frac{(k+1)(k+2)}{2}$, en waarbij we gebruik zullen moeten maken van de IH:

$$
\begin{aligned}
\sum_{i=1}^{k+1} i &= \sum_{i+1}^{k} i + (k+1) && k+1 \text{ afgesplitst} \\
&= \frac{k(k+1)}{2} + (k+1) && \text{Inductiehypothese toegepast} \\
&= \frac{k(k+1)}{2} + \frac{(k+1)}{1} && k+1 \text{ als breuk geschreven} \\
&= \frac{k(k+1)}{2} + \frac{2(k+1)}{2} && \text{noemers van beide breuken gelijk gemaakt} \\
&= \frac{k(k+1)+2(k+1)}{2} && \text{breuken opgeteld} \\
&= \frac{(k+1)(k+2)}{2} && \text{in de teller } (k+1) \text{ buiten haakjes gehaald}
\end{aligned}
$$

In de eerste stap haal ik de laatste term van de optelling $\sum_{i=1}^{k+1} i$ af, omdat ik dan de sommatie $\sum_{i=1}^{k} i$ volgens de inductiehypothese kan vervangen door $\frac{k(k+1)}{2}$. Als ik dat niet doe, kan ik de inductiehypothese niet toepassen, en dat zal ik moeten doen omdat het bewijs anders niet kan werken. Zoiets dergelijks zul je eigenlijk altijd moeten doen in een inductiebewijs, omdat meestal het consequent van de implicatie *niet algemeen* geldig is, maar *alleen onder de voorwaarde dat het antecedent waar is*.

In nog meer detail: $\sum_{i=1}^{k+1} i = 1 + 2 + \ldots + (k-1) + k + (k+1)$ en wanneer ik de eerste k termen schrijf als $\sum_{i=1}^{k} i$ is dat gelijk aan $\sum_{i=1}^{k} i + (k+1)$.

Het vervolg van het bewijs is dat we nu, omdat k willekeurig was gekozen uit de verzameling getallen die ≥ 1 zijn, mogen concluderen dat voor *alle* getallen $n \geq 1$ geldt dat $P(n) \to P(n+1)$.

Omdat we de basis- en de inductiestap hebben bewezen, mogen we nu **volgens het principe van inductie** concluderen dat de eigenschap geldt voor alle getallen ≥ 1. (Deze laatste stap is noodzakelijk in een inductiebewijs, dus vergeet hem niet, want dat kost punten.) QED

Een ander probleem is dus dat vaak de inductiehypothese niet voor waar wordt aangenomen, of dat dit niet duidelijk wordt genoemd. De inductiestap is een (universeel gekwantificeerde) implicatie, dus die kun je bewijzen door een willekeurig element te nemen van de verzameling van elementen waarvoor je wil bewijzen dat de eigenschap geldt (dat zijn alle natuurlijke getallen groter dan of gelijk aan het basisgetal), en voor dat willekeurige element te bewijzen dat de implicatie inderdaad geldt. Een implicatie bewijzen doen we door het antecedent voor waar aan te nemen en onder die aanname het consequent af te leiden. Dan moet je dus wel eerst aannemen dat het antecedent waar is, dus dat de eigenschap geldt voor het willekeurige getal—en dat is de inductiehypothese!

Recapitulerend werkt namelijk een bewijs met inductie over de natuurlijke getallen als volgt: als je bewijst dat het basisgetal (meestal 0 of 1) een bepaalde eigenschap heeft (de basisstap), en dat *alle* getallen groter dan of gelijk aan het basisgetal die eigenschap doorgeven aan het volgende getal (de inductiestap), dan mag je volgens het principe (axioma) van inductie concluderen dat de eigenschap geldt voor alle getallen groter dan of gelijk aan het basisgetal.

6.2 Structurele Inductie

Een bewijs met structurele inductie is de naam die we gebruiken voor een bewijs dat alle formules in $PROP$ een bepaalde eigenschap hebben.[2] De verzameling $PROP$ is namelijk net als de verzameling natuurlijke getallen *recursief gedefinieerd*, dat wil zeggen: in termen van zichzelf. Een bewijs met inductie over de structuur van $PROP$ verloopt op soortgelijke manier als een bewijs met volledige inductie, met een paar wijzigingen:

- Meestal is de te bewijzen uitspraak uitgedrukt in functies die zelf ook recursief gedefinieerd zijn over $PROP$. Die recursieve functiedefinities moet je in je bewijs gebruiken.
- De basis is de individuele propositieletter p_i.
- In de inductiestap moet je aantonen dat de eigenschap behouden blijft in de constructie van nieuwe formules uit bestaande formules. Dit is overeenkomstig het idee bij volledige inductie, waar je ook aantoont dat de eigenschap behouden blijft bij constructie van een nieuw natuurlijk getal uit een bestaand, namelijk door er 1 bij op te tellen. Bij structurele inductie kun je op 2 verschillende manieren nieuwe formules uit bestaande maken, namelijk door

  1. voor een bestaande formule A een '$\neg$' te plaatsen en formule $\neg A$ te creëren, of
  2. tussen 2 bestaande formules A en B een tweeplaatsig connectief ($\vee$, $\wedge$, $\rightarrow$, of $\leftrightarrow$) te plaatsen, en haakjes om het geheel te plaatsen: $(A{\star}B)$, waar $\star \in \{\vee, \wedge, \rightarrow, \leftrightarrow\}$.

  De inductiestap van een bewijs met structurele inductie heeft dus ook altijd 2 delen: één voor formules van de vorm $\neg A$, en één voor formules van de vorm $(A \star B)$. Voorbeelden hiervan kun je terugvinden in (uitwerkingen van) oude tentamens.
- Het principe van inductie hoeft voor bewijzen met structurele inductie niet te worden aangeroepen. Dit komt door stelling 2.3.5 in het dictaat *Logica*, p. 20, waar *wel* het principe van inductie wordt aangeroepen.

Appendices

Op de volgende pagina's staan de antwoorden op opgaven 5.3.2 en 11.4.1 over de boommethode en 4.4.3 over meta-beweringen. Dek de antwoorden af met een papiertje (of scroll voorzichtig naar beneden) zodat je niet het antwoord ziet op een opgave die je nog moet doen. Ik geef voor elke opgave eerste het antwoord (waar of onwaar), en op de volgende regel eventueel een tegenvoorbeeld of een bewijs.

[2] Structurele inductie wordt ook wel gebruikt als de algemene naam voor inductie, omdat dit een bewijsmethode is voor het bewijzen van eigenschappen die alle elementen hebben in verzamelingen waarvan de structuur recursief gedefinieerd is. De natuurlijke getallen zijn bijvoorbeeld recursief gedefinieerd: 0 is een natuurlijk getal, en als n een natuurlijk getal is, is $n + 1$ dat ook. Dit is de *structuur* in de verzameling natuurlijke getallen, en die wordt nauwgezet gevolgd in een bewijs met volledige inductie, dus een bewijs met inductie over de structuur van de natuurlijke getallen. Ook de verzameling $PROP$ is recursief gedefinieerd: p_i (voor $i \in \mathbb{N}$) is een formule, en als A en B formules zijn, dan zijn ook $\neg A$ en $(A \star B)$ formules, waar $\star \in \{\vee, \wedge, \rightarrow, \leftrightarrow\}$. Je komt in de informatica nog veel meer recursief gedefinieerde verzamelingen objecten tegen, bijvoorbeeld in de context van (het vak) automaten en talen, reguliere expressies, grafen, etc. Ook bewijzen van eigenschappen die alle elementen in dergelijke verzamelingen hebben, vallen onder de noemer 'structurele inductie.'

A Logica, opgave 5.3.2

(a) onwaar.

Een tegenvoorbeeld is een valuatie v met $v(A) = v(B) = v(\neg C) = 1$.

(b) waar.

(c) onwaar.

Een tegenvoorbeeld is een valuatie v met $v(A) = v(B) = v(D) = v(\neg E) = 1$.

(d) waar.

(e) onwaar.

Tegenvoorbeelden zijn valuaties v met $v(A) = v(\neg B) = 1$ of $v(\neg A) = v(B) = 1$.

(f) waar natuurlijk.

Het is ook een leuke oefening voor metabeweringen om (d) als metabewering te bewijzen.

Bewijs van (d). De bewering zegt dat $\neg A \to A \models A$, dus dat alle modellen voor $\neg A \to A$ ook model zijn voor A. Dit bewijzen we door een willekeurig model voor $\neg A \to A$ te nemen, zeg de valuatie w (waarvoor dus geldt $w(\neg A \to A) = 1$), en te laten zien dat ook geldt dat $w(A) = 1$. Er geldt $w(\neg A \to A) = \max(1 - w(\neg A), w(A)) = \max(1 - (1 - w(A)), w(A)) = \max(1 - 1 + w(A), w(A)) = \max(w(A), w(A)) = 1$. Dit betekent dat $w(A) = 1$ moet gelden. Omdat w willekeurig was gekozen, geldt voor alle modellen van $\neg A \to A$ dat ze model zijn voor A, oftewel dat $\neg A \to A \models A$. QED

B Logica, opgave 11.4.1

(a) waar.

(b) waar.

(c) waar.

(d) onwaar.

Een tegenvoorbeeld is de structuur $\mathcal{D} = \langle D; R_0 \rangle$, waar $D = \{d_0, d_1\}$, $R_0 = C^{\mathcal{D}} = \{d_1\}$. In deze structuur is de conclusie onwaar, want voor object d_0 geldt weliswaar dat het object $d_1 \in R_0$ bestaat, zodat het antecedent van de implicatie waar is, maar er geldt niet dat $d_0 \in R_0$, zodat het consequent onwaar is, en de implicatie niet voor d_0, en dus *niet voor alle* x geldt.

(e) onwaar.

Dit is ook wel duidelijk als je erover nadenkt. Hoewel de implicatie 'van links naar rechts' waar is, is hij dat andersom niet: als er een object met eigenschap A bestaat, en een (ander) object met eigenschap B, dan hoeft dat nog niet te betekenen dat er ook een object met beide eigenschappen bestaat. Een tegenvoorbeeld is de structuur $\mathcal{E} = \langle D; R_0, R_1 \rangle$, waar $D = \{d_0, d_1\}$, $R_0 = A^{\mathcal{E}} = \{d_0\}$, en $R_1 = B^{\mathcal{E}} = \{d_1\}$. In deze structuur is het dus wel waar dat $d_0 \in R_0$ en dat $d_1 \in R_1$, maar er bestaat geen element dat in zowel R_0 als R_1 zit.

(f) waar.

(g) onwaar.

Een tegenvoorbeeld is de structuur $\mathcal{G} = \langle D; R_0, R_1 \rangle$, waar $D = \{d_0, d_1\}$, $R_0 = A^{\mathcal{G}} = \{d_1\}$, en $R_1 = B^{\mathcal{G}} = \{d_0\}$. Nu geldt wel het antecedent, want voor $d_0 \notin R_0$ is de implicatie daarin waar, maar niet het consequent van de conclusie van de bewering. Het antecedent van de implicatie in dat consequent is wel waar omdat $d_1 \in R_0$, maar het consequent (van de implicatie in het consequent van de conclusie van de bewering als geheel) is niet waar, want $d_1 \notin R_1$.

(h) waar.

(i) waar.

(j) onwaar.

Een tegenvoorbeeld is de structuur $\mathcal{J} = \langle D; R_0, R_1 \rangle$, waar $D = \{d_0, d_1\}$, $R_0 = A^{\mathcal{J}} = \emptyset$ en $R_1 = R^{\mathcal{J}} = \{(d_0, d_1)\}$. In deze structuur geldt namelijk wel de premisse van de redenering, want zowel voor object d_0 als voor d_1 geldt dat ze met zichzelf niet in relatie R_1 zitten, en dus is voor beide objecten de implicatie waar. De conclusie van de bewering is alleen niet waar, want voor object d_0 geldt weliswaar dat het met object d_1 in relatie R_1 zit, maar niet dat $d_0 \in R_0$.

C Logica, opgave 4.3.3

(a) waar.

Bewijs. Stel dat $\models A \wedge B$. Dan geldt voor alle valuaties dat $v(A \wedge B) = \min(v(A), v(B)) = 1$, dus moet voor alle valuaties gelden dat $v(A) = v(B) = 1$. QED

(b) waar.

Bewijs. Stel dat $\models \neg A$, dus dat voor alle valuaties geldt dat $v(\neg A) = 1$. Neem een willekeurige valuatie w. Hiervoor geldt dus ook dat $w(\neg A) = 1 - w(A) = 1$, dus dat $w(A) = 0$. Deze valuatie toont aan dat niet voor alle valuaties geldt dat $v(A) = 1$, dus dat $\sim\models A$. QED

(c) onwaar.

Tegenvoorbeeld: $A = p$. Als $A = p$, is het wel waar dat A geen tautologie is, dus dat $\sim\models A$, want voor elke valuatie met $v(p) = 0$ geldt niet dat $v(A) = 1$, dus geldt niet voor alle valuaties dat $v(A) = 1$. Maar er geldt niet dat $\neg A$ een tautologie is, want voor elke valuatie met $v(p) = 1$ is $v(\neg A) = 1 - v(A) = 1 - 1 = 0$, dus geldt niet voor alle valuaties dat $v(\neg A) = 1$.

(d) waar.

Bewijs. Stel dat $\models A$ of $\models B$ waar is. We moeten aantonen dat voor alle valuaties $v(A \vee B) = 1$. Neem een willekeurige valuatie, zeg w, waarvoor we nu moeten laten zien dat $w(A \vee B) = 1$. We maken op basis van de aanname een gevalsonderscheid.

$\models A$: Voor alle valuaties, dus ook voor w, geldt dus dat $v(A) = 1$. Dan geldt ook dat $w(A \vee B) = \max(w(A), w(B)) = \max(1, w(B)) = 1$, ongeacht $w(B)$.

$\models B$: Voor alle valuaties, dus ook voor w, geldt dus dat $v(B) = 1$. Dan geldt ook dat $w(A \vee B) = \max(w(A), w(B)) = \max(w(A), 1) = 1$, ongeacht $w(A)$.

In beide gevallen, dus in het algemeen, is $w(A \vee B) = 1$. Omdat w willekeurig was gekozen, geldt voor alle valuaties dat $v(A \vee B) = 1$, oftewel dat $\models A \vee B$. QED

(e) waar.

Bewijs. Stel dat $\models A \to B$. We moeten bewijzen dat “als $\models A$ dan $\models B$.” Dit is een implicatie, waarvan we kunnen bewijzen dat hij waar is door het antecedent voor waar aan te nemen, en het consequent af te leiden. Stel dus dat $\models A$. Nu moeten we bewijzen dat $\models B$, dus neem een willekeurige valautie, zeg w, waarvoor we nu moeten laten zien dat $w(B) = 1$. Vanwege de aannames weten we dat $w(A \to B) = w(A) = 1$, dus dat $w(A \to B) = \max(1 - w(A), w(B)) = \max(1 - 1, w(B)) = \max(0, w(B)) = 1$. Dan moet dus gelden dat $w(B) = 1$. Omdat w willekeurig was gekozen, geldt voor alle valuaties dat $v(B) = 1$, dus dat $\models B$. QED

(f) onwaar.

Als we voor A een tautologie kiezen, moet B ook een tautologie zijn om het antecedent waar te maken. Maar dan is het consequent ook waar, en dat moet juist onwaar zijn om de onwaarheid van de bewering aan te tonen. A mag dus geen tautologie zijn, en B ook niet. Als A een contradictie is, is het consequent ook altijd waar, dus A moet een contingentie zijn, de simpelste is $A = p$, dus laten we dat proberen. B mag geen tautologie zijn, laten we $B = \neg p$ proberen (als we ook $B = p$ nemen, is het consequent weer waar). Nu geldt dus dat, omdat A geen tautologie is, het antecedent waar is. Maar het consequent is niet waar, want $p \to \neg p$ is geen tautologie. Neem namelijk een valuatie v met $v(p) = 1$, dan is $v(A \to B) = v(p \to \neg p) = \max(1 - v(p), v(\neg p)) = \max(1 - v(p), 1 - v(p)) = \max(1 - 1, 1 - 1) = 0$, dus geldt niet voor alle valuaties dat $v(A \to B) = 1$.

(g) onwaar.

Als $A \vee B$ een tautologie is en A geen tautologie, dan is B een tautologie. Het lijkt op het eerste gezicht wel plausibel, maar let goed op het verschil tussen deze bewering en (h). Hier zit hem de kneep in de interpretatie van $\sim\models A$: dit zegt **niet** dat *voor alle valuaties* geldt dat $v(A) = 0$, maar dat *niet voor alle valuaties* geldt dat $v(A) = 1$. (Het verband tussen $\sim\models A$ en $\models \neg A$ heb je bij b en c al onderzocht.) Er bestaat dus een valuatie waarvoor $v(A) = 0$, maar dat zegt niets over alle valuaties, en over of ze B waar maken.

Een tegenvoorbeeld kan dit aantonen. Het antecedent moet waar zijn, dus A mag geen tautologie zijn, en het consequent moet onwaar zijn, dus B mag ook geen tautologie zijn. Om $\models A \vee B$ waar te maken, kunnen A en B bijvoorbeeld elkaars complement zijn, dus laten we voor $A = p$ nemen, en voor $B = \neg p$. Dan geldt inderdaad dat $\models A \vee B$, want voor alle valuaties geldt $v(A \vee B) = v(p \vee \neg p) = \max(v(p), v(\neg p)) = \max(v(p), 1 - v(p)) = 1$, ongeacht of $v(p) = 0$ of $v(p) = 1$. Er geldt ook dat $\sim\models A$, maar niet dat $\models B$.

(h) waar.

Bewijs. Stel dat $\models A \vee B$ en $\models \neg A$. Te bewijzen is dat $\models B$. Neem dus een willekeurige valuatie, zeg w, waarvoor we moeten bewijzen dat $w(B) = 1$. Voor alle valuaties, dus ook voor w, geldt dat $w(A \vee B) = 1$ en dat $w(\neg A) = 1 - w(A) = 1$, dus dat $w(A) = 0$. Dus $w(A \vee B) = \max(w(A), w(B)) = \max(0, 1(B)) = 1$, wat betekent dat $w(B) = 1$. Omdat w willekeurig was gekozen, geldt voor alle valuaties dat $v(B) = 1$, oftewel dat $\models B$. QED

(i) waar.

Bewijs. Stel dat $\models A$. Te bewijzen is dat $\models A \to A$. Hiervoor hebben we zelfs de aanname niet nodig, want voor een willekeurige valuatie, zeg w, geldt dat $w(A \to A) = \max(1 - w(A), w(A))$, en dat is gelijk aan 1, ongeacht of $w(A) = 0$ of 1. QED

(j) onwaar.

Als tenminste één van A en $\neg A$ waar is, hoeft het niet zo te zijn dat dat altijd A is. Neem bijvoorbeeld voor A een contingentie zoals $A = p$, dan geldt inderdaad dat $\models A \vee \neg A$, maar niet dat $\models A$.

(k) waar.

Bewijs. We bewijzen de beide richtingen van de bi-implicatie.

(⇒): Stel dat $A \models (B \to A)$. Te bewijzen is dat $B \models (A \to A)$. Volgens stelling (i) geldt $\models (A \to A)$, dus zijn alle valuaties, ook diegenen die model zijn voor B, model voor $A \to A$, oftewel $B \models A \to A$.

(⇐): Stel dat $B \models (A \to A)$. Te bewijzen is dat $A \models (B \to A)$, dus dat alle modellen voor A ook model zijn voor $B \to A$. Neem dus een willekeurig model voor A, d.w.z. een willekeurige valuatie die A waar maakt. Noem deze valuatie w. We moeten nu dus laten zien dat $w(B \to A) = \max(1 - w(B), w(A)) = 1$. We maken een gevalsonderscheid.

$w(B) = 0$**:** Nu is $\max(1 - w(B), w(A)) = \max(1 - 0, w(A)) = 1$.

$w(B) = 1$**:** Omdat w een model voor A is geldt nu dat $\max(1 - w(B), w(A)) = \max(1 - w(B), 1) = 1$.

In beide gevallen, dus in het algemeen, geldt dat $w(B \to A) = 1$. Omdat w een willekeurig model voor A was, geldt voor alle modellen voor A dat ze model voor $B \to A$ zijn, oftewel dat $A \models B \to A$.

QED