Aanvullende syllabus Discrete Structuren (Gerard Renardel, november 2003)

Deze syllabus is een kleine aanvulling op het boek *Discrete Mathematics* van Ross en Wright (verder aangeduid door [R&W]). Het eerste deel gaat over een bepaalde notatie van wiskundige bewijzen ter aanvulling op Chapter 2, het tweede deel is een overzicht van de wetten van de predikatenlogica ter aanvulling op Chapter 13 (Chapter 11 in de 4e editie). Aan het einde van de onderdelen staan enkele opgaven, met achterin de uitwerkingen.

1 Geannoteerde lineaire bewijzen

Het *geannoteerde lineaire bewijs* (kortweg GLB) is een redelijk precies omschreven bewijsvorm die houvast biedt bij het maken van bewijzen. Verder leidt het gebruik van het GLB-formaat tot bewijzen die goed nagelezen en gecontroleerd kunnen worden.

1.1 Vorm van een GLB

De algemene vorm van een GLB is als volgt:

$$\begin{array}{lll} & \varphi_1 & \\ \Rightarrow & & \{\text{reden waarom } \varphi_1 \Rightarrow \varphi_2\} \\ & \varphi_2 & \\ \Rightarrow & & \{\text{reden waarom } \varphi_2 \Rightarrow \varphi_3\} \\ \vdots & \vdots & \vdots \\ \Rightarrow & & \{\text{reden waarom } \varphi_{n-1} \Rightarrow \varphi_n\} \\ & \varphi_n & \\ \\ \multicolumn{3}{l}{\text{Conclusie: } \varphi_1 \Rightarrow \varphi_n.} \end{array}$$

Je ziet: alle bewijsstappen staan op één (verticale) lijn, en daarom spreken we van een *lineair* bewijs. De rechtvaardiging van elk van de bewijsstappen wordt tussen accolades vermeld: dat is de *annotatie*. De rechtvaardiging kan bestaan uit een logische equivalentie (zie bv. [R&W], p. 62; in de 4e editie p. 85) of logische implicatie ([R&W], p. 63; in de 4e editie p. 86), die dan in de annotatie vermeld wordt. Bijvoorbeeld 9: contrapositie ($p \to q \Rightarrow \neg q \to \neg p$), of 19: modus ponens ($[p \wedge (p \to q)] \Rightarrow q$). We voegen daar de volgende logische equivalenties aan toe:

28a.	$\neg \mathbf{1} \Longleftrightarrow \mathbf{0}$	0-1-wetten
b.	$\neg \mathbf{0} \Longleftrightarrow \mathbf{1}$	
29a.	$(p \wedge (p \vee q)) \Longleftrightarrow p$	absorptie
b.	$(p \vee (p \wedge q)) \Longleftrightarrow p$	

De rechtvaardiging kan ook een basisprincipe uit de wiskunde zijn, bijvoorbeeld commutativiteit van de optelling ($x + y = y + x$), transitiviteit van $\leq$ ($x \leq y \wedge y \leq z \Rightarrow x \leq z$) of de eigenschap $xy = 0 \Longleftrightarrow (x = 0 \vee y = 0)$.

Enige speciale gevallen:

- $\varphi_1 = \mathbf{1}$: de conclusie van het bewijs is dan φ_n.
- $\varphi_n = \mathbf{0}$: in dat geval is de conclusie $\neg\varphi_1$

Het spreekt vanzelf dat één of meer $\Rightarrow$'s door $\Longleftrightarrow$ mogen worden vervangen, mits we de bijbehorende equivalentie $\varphi_i \Longleftrightarrow \varphi_{i+1}$ kunnen rechtvaardigen. Als *alle* $\Rightarrow$'s door $\Longleftrightarrow$ zijn vervangen, dan hebben we zelfs een GLB voor $\varphi_1 \Longleftrightarrow \varphi_n$.

Voorbeeld uit de propositielogica: bewijs van 5a, idempotentie van $\vee$, gebruik makend van andere logische equivalenties.

$$\begin{array}{lll}
 & p \vee p & \\
\Longleftrightarrow & & \{\text{8a: De Morgan}\} \\
 & \neg(\neg p \wedge \neg p) & \\
\Longleftrightarrow & & \{\text{5b: idempotentie van } \wedge\} \\
 & \neg\neg p & \\
\Longleftrightarrow & & \{\text{1: dubbele negatie}\} \\
 & p &
\end{array}$$

Conclusie: $(p \vee p) \Longleftrightarrow p$. Anders gezegd: $(p \vee p) \leftrightarrow p$ is een tautologie.

Achterstevoren: een variant van GLB ontstaat als we *alle* $\Rightarrow$'s door $\Leftarrow$'s vervangen:

$$\begin{array}{lll}
 & \psi & \\
\Leftarrow & & \{\ldots\} \\
\vdots & \vdots & \vdots \\
\Leftarrow & & \{\ldots\} \\
 & \varphi &
\end{array}$$

Dit 'achterstevoren'-bewijs van $\varphi \Rightarrow \psi$ is vaak makkelijker te bedenken, zeker als ψ ingewikkelder is dan φ. Je kunt ψ dan gaandeweg vereenvoudigen.

Meer varianten: $\varphi \Rightarrow \psi$ kan ook nog op andere manieren mbv. een GLB bewezen worden. We geven een aantal daarvan schematisch weer:

$$\begin{array}{lllclllclll}
 & \neg\psi & & & & \varphi \wedge \neg\psi & & & & \varphi \rightarrow \psi & \\
\Rightarrow & & \{\ldots\} & & \Rightarrow & & \{\ldots\} & & \Leftarrow & & \{\ldots\} \\
\vdots & \vdots & \vdots & \text{of} & \vdots & \vdots & \vdots & \text{of} & \vdots & \vdots & \vdots \\
\Rightarrow & & \{\ldots\} & & \Rightarrow & & \{\ldots\} & & \Leftarrow & & \{\ldots\} \\
 & \neg\varphi & & & & \mathbf{0} & & & & \mathbf{1} &
\end{array}$$

Voor $\varphi \Longleftrightarrow \psi$ zijn ook diverse GLB's mogelijk:

$$\begin{array}{lllclllclll}
 & \psi & & & & \neg\varphi & & & & \varphi \leftrightarrow \psi & \\
\Longleftrightarrow & & \{\ldots\} & & \Longleftrightarrow & & \{\ldots\} & & \Leftarrow & & \{\ldots\} \\
\vdots & \vdots & \vdots & \text{of} & \vdots & \vdots & \vdots & \text{of} & \vdots & \vdots & \vdots \\
\Longleftrightarrow & & \{\ldots\} & & \Longleftrightarrow & & \{\ldots\} & & \Leftarrow & & \{\ldots\} \\
 & \varphi & & & & \neg\psi & & & & \mathbf{1} &
\end{array}$$

of de *ping-pong*-variant:

$$
\begin{array}{llll}
 & \varphi & \\
\Rightarrow & & \{\ldots\} \\
\vdots & \vdots & \vdots \\
\Rightarrow & & \{\ldots\} \\
 & \psi &
\end{array}
\quad \textbf{en} \quad
\begin{array}{llll}
 & \psi & \\
\Rightarrow & & \{\ldots\} \\
\vdots & \vdots & \vdots \\
\Rightarrow & & \{\ldots\} \\
 & \varphi &
\end{array}
$$

Voorbeeld uit de wiskunde: bepalen van de nulpunten van een vierdegraads vergelijking.

$$
\begin{array}{ll}
 & x^4 - 6x^3 + 5x^2 = 0 \\
\Longleftrightarrow & \quad \{\text{ontbinden in factoren}\} \\
 & x^2 \cdot (x-1) \cdot (x-5) = 0 \\
\Longleftrightarrow & \quad \{\text{produkt is } 0 \Longleftrightarrow \text{ minstens een factor is } 0\} \\
 & x = 0 \vee x - 1 = 0 \vee x - 5 = 0 \\
\Longleftrightarrow & \quad \{\text{rekenen}\} \\
 & x = 0 \vee x = 1 \vee x = 5
\end{array}
$$

1.2 Universele generalisatie

Om universele beweringen (dwz. van de vorm $\forall x \ldots$) te bewijzen, wordt vaak *universele generalisatie* gebruikt. Dit is de volgende bewijsvorm:

> Zij x een willekeurig object met eigenschap p, dwz. $p(x)$ geldt.
> Dan ... (volgt een redenering, bv. een LGB) ... $q(x)$.
> Conclusie: $\forall x(p(x) \rightarrow q(x))$.

Een eenvoudiger vorm ontstaat als we de conditie $p(x)$ weglaten, de conclusie wordt dan $\forall x\, q(x)$.

Voorbeeld: bewijs van $(A - (B \cup C)) \subseteq (A - B)$.
Door toepassing van de definitie van $\subseteq$ zien we dat we moeten bewijzen: $\forall x(x \in (A - (B \cup C)) \rightarrow x \in (A - B))$. Dit is een universele bewering. Zij dus x een willekeurig element van $(A - (B \cup C))$. Dan:

$$
\begin{array}{ll}
 & x \in (A - (B \cup C)) \\
\Longleftrightarrow & \quad \{\text{definitie van } - \text{ en } \cup\} \\
 & x \in A \wedge \neg(x \in B \vee x \in C) \\
\Longleftrightarrow & \quad \{\text{De Morgan}\} \\
 & x \in A \wedge (\neg\, x \in B \wedge \neg\, x \in C) \\
\Longleftrightarrow & \quad \{\text{associativiteit}\} \\
 & (x \in A \wedge \neg x \in B) \wedge \neg\, x \in C \\
\Rightarrow & \quad \{\text{conjunctie-eliminatie } (\textit{simplification} \text{ in [R\&W]})\} \\
 & x \in A \wedge \neg x \in B \\
\Longleftrightarrow & \quad \{\text{definitie van } -\} \\
 & x \in (A - B)
\end{array}
$$

Conclusie: $\forall x(x \in (A - (B \cup C)) \rightarrow x \in (A - B))$
Dus (definitie van $\subseteq$): $(A - (B \cup C)) \subseteq (A - B)$.

1.3 Pas op! vaak gemaakte fouten in GLB's

Een bewijsstap kan bestaan uit het herschrijven van een *onderdeel* van een expressie mbv. een (logische) wet. **Dat mag alleen als die wet een equivalentie is!** En dus niet als het slechts een implicatie is: zulke wetten mogen alleen worden gebruikt voor het herschrijven van de *gehele* expressie. We laten zien wat er mis kan gaan als we ons hier niet aan houden.

Non-voorbeeld: foutief bewijs van $\mathbf{0}$.

$$
\begin{array}{lll}
 & \mathbf{1} & \\
\Longleftrightarrow & & \{ \text{ 28b: 0-1-wet } \} \\
 & \neg\mathbf{0} & \\
\Longleftrightarrow & & \{ \text{ 6c: } \mathbf{1} \wedge \mathbf{0} \Longleftrightarrow \mathbf{0} \ \} \\
 & \neg(\mathbf{1} \wedge \mathbf{0}) & \\
\Rightarrow ?? & & \{ \text{ 17: simplificatie } \} \\
 & \neg\mathbf{1} & \\
\Rightarrow & & \{ \text{ 28a: 0-1-wet } \} \\
 & \mathbf{0} &
\end{array}
$$

De fout zit natuurlijk in de derde stap: toepassing van simplificatie (een logische implicatie, geen logische equivalentie) op een onderdeel van de expressie.

Vraag: is het volgende een GLB met conclusie $\varphi_1 \Rightarrow \varphi_4$?

$$
\begin{array}{lll}
 & \varphi_1 & \\
\Rightarrow & & \{\cdots\} \\
 & \varphi_2 & \\
\Longleftrightarrow & & \{\cdots\} \\
 & \varphi_3 & \\
\Leftarrow & & \{\cdots\} \\
 & \varphi_4 &
\end{array}
$$

Antwoord: **nee**, want de pijl $\Leftarrow$ in de laatste bewijsstap loopt in de verkeerde richting. We mogen hier wel bv. concluderen $\varphi_1 \Rightarrow \varphi_3$ en $\varphi_4 \Rightarrow \varphi_2$.

1.4 Opgaven

1. Bewijs $p \wedge (\neg p \rightarrow q) \Longleftrightarrow p$.

2. Bewijs $p \Longleftrightarrow (\neg p \vee q) \rightarrow p$.

3. Bewijs dat $((p \rightarrow q) \rightarrow p) \rightarrow p$ een tautologie is.

2 Wetten van de predikatenlogica

In sectie 13.2: *Elementary Predicate Calculus* van [R&W] (11.2 in de 4e editie) worden enkele wetten van de predikatenlogica gegeven. Echter, een aantal belangrijke wetten ontbreekt: daarom hier een overzicht van alle wetten die tot de tentamenstof behoren. Evenals de wetten van de propositielogica (Chapter 2) hoef je deze wetten niet uit het hoofd te leren, voor zover nodig worden ze tijdens de toets en het tentamen ter beschikking gesteld.

Equivalenties:

30a.	$p \iff \forall x\, p$ (x niet vrij in p)	loze kwantificatie
ba.	$p \iff \exists x\, p$ (x niet vrij in p)	
31a.	$\forall x\, p(x) \iff \forall y\, p(y)$	herbenoemen van gebonden variabele
b.	$\exists x\, p(x) \iff \exists y\, p(y)$	
32a.	$\forall x\, \forall y\, p(x,y) \iff \forall y\, \forall x\, p(x,y)$	kwantorwisseling
b.	$\exists x\, \exists y\, p(x,y) \iff \exists y\, \exists x\, p(x,y)$	
33a.	$\forall x(p(x) \wedge q(x)) \iff \forall x\, p(x) \wedge \forall x\, q(x)$	$\forall(\wedge) \iff \forall \wedge \forall$ ($\forall$ distribueert over $\wedge$)
b.	$\exists x(p(x) \vee q(x)) \iff \exists x\, p(x) \vee \exists x\, q(x)$	$\exists(\vee) \iff \exists \vee \exists$ ($\exists$ distribueert over $\vee$)
c.	$\exists x(p(x) \to q(x)) \iff \forall x\, p(x) \to \exists x\, q(x)$	$\exists(\to) \iff \forall \to \exists$
34a.	$\forall x(p \vee q(x)) \iff p \vee \forall x\, q(x)$ (x niet vrij in p)	
b.	$\exists x(p \wedge q(x)) \iff p \wedge \exists x\, q(x)$ (x niet vrij in p)	
35a.	$\neg\forall x\, p(x) \iff \exists x\, \neg p(x)$	$\neg\forall \iff \exists\neg$ (De Morgan)
b.	$\neg\exists x\, p(x) \iff \forall x\, \neg p(x)$	$\neg\exists \iff \forall\neg$ (De Morgan)

Implicaties:

36.	$\forall x\, p(x) \Rightarrow \exists x\, p(x)$	$\forall \Rightarrow \exists$
37.	$\exists x\, \forall y\, p(x,y) \Rightarrow \forall y\, \exists x\, p(x,y)$	$\exists\forall \Rightarrow \forall\exists$
38a.	$\exists x(p(x) \wedge q(x)) \Rightarrow \exists x\, p(x) \wedge \exists x\, q(x)$	$\exists(\wedge) \Rightarrow \exists \wedge \exists$
b.	$\forall x(p(x) \to q(x)) \Rightarrow \forall x\, p(x) \to \forall x\, q(x)$	$\forall(\to) \Rightarrow \forall \to \forall$
c.	$\forall x\, p(x) \vee \forall x\, q(x) \Rightarrow \forall x(p(x) \vee q(x))$	$\forall \vee \forall \Rightarrow \forall(\vee)$

2.1 Opgaven

4. Bewijs $\exists x\, p(x) \to \forall x\, q(x) \Rightarrow \forall x(p(x) \to q(x))$
5. Bewijs $\forall x(p(x) \leftrightarrow q) \iff (\exists x p(x) \to q) \wedge (q \to \forall x p(x))$ (x komt niet vrij voor in q)

2.2 Uitwerkingen

1. Eenvoudig:

$$
\begin{array}{ll}
 & p \wedge (\neg p \rightarrow q) \\
\Longleftrightarrow & \quad \{ \text{ 11a } \} \\
 & p \wedge (p \vee q) \\
\Longleftrightarrow & \quad \{ \text{ 29a: absorptie } \} \\
 & p
\end{array}
$$

Conclusie: $p \wedge (\neg p \rightarrow q) \Longleftrightarrow p$.

2. We redeneren achterstevoren:

$$
\begin{array}{ll}
 & (\neg p \vee q) \rightarrow p \\
\Longleftrightarrow & \quad \{ \text{ 10a: implicatie } \} \\
 & \neg(\neg p \vee q) \vee p \\
\Longleftrightarrow & \quad \{ \text{ 8a: De Morgan } \} \\
 & (\neg\neg p \wedge \neg q) \vee p \\
\Longleftrightarrow & \quad \{\text{1: dubbele negatie}\} \\
 & (p \wedge \neg q) \vee p \\
\Longleftrightarrow & \quad \{\text{2a: commutativiteit}\} \\
 & p \vee (p \wedge \neg q) \\
\Longleftrightarrow & \quad \{\text{29b: absorptie}\} \\
 & p
\end{array}
$$

Conclusie: $p \Longleftrightarrow (\neg p \vee q) \rightarrow p$.

3. We gaan aantonen dat $((p \rightarrow q) \rightarrow p) \rightarrow p$ logisch equivalent is met $\mathbf{1}$.

$$
\begin{array}{ll}
 & ((p \rightarrow q) \rightarrow p) \rightarrow p \\
\Longleftrightarrow & \quad \{\text{10a: implicatie (2 keer)}\} \\
 & (\neg(\neg p \vee q) \vee p) \rightarrow p \\
\Longleftrightarrow & \quad \{\text{8a: De Morgan}\} \\
 & ((\neg\neg p \wedge \neg q) \vee p) \rightarrow p \\
\Longleftrightarrow & \quad \{\text{1: dubbele negatie}\} \\
 & ((p \wedge \neg q) \vee p) \rightarrow p \\
\Longleftrightarrow & \quad \{\text{2a: commutativiteit en 29b: absorptie}\} \\
 & p \rightarrow p \\
\Longleftrightarrow & \quad \{\text{10a: implicatie}\} \\
 & \neg p \vee p \\
\Longleftrightarrow & \quad \{\text{2a: commutativiteit en 7a}\} \\
 & \mathbf{1}
\end{array}
$$

Conclusie: $((p \rightarrow q) \rightarrow p) \rightarrow p$ is een tautologie.

4. Achterstevoren:

$$\begin{array}{ll}
 & \forall x(p(x) \rightarrow q(x)) \\
\Longleftrightarrow & \quad \{\text{10a: implicatie}\} \\
 & \forall x(\neg p(x) \vee q(x)) \\
\Leftarrow & \quad \{\text{38a: } \forall \text{ over } \vee\} \\
 & \forall x\, \neg p(x) \vee \forall x\, q(x) \\
\Longleftrightarrow & \quad \{\text{35b: De Morgan}\} \\
 & \neg \exists x\, p(x) \vee \forall x\, q(x) \\
\Longleftrightarrow & \quad \{\text{10a: implicatie}\} \\
 & \exists x\, p(x) \rightarrow \forall x\, q(x)
\end{array}$$

Conclusie: $\exists x\, p(x) \rightarrow \forall x\, q(x) \Rightarrow \forall x(p(x) \rightarrow q(x))$.

5.

$$\begin{array}{ll}
 & \forall x(p(x) \leftrightarrow q) \\
\Longleftrightarrow & \quad \{ \text{ 13: equivalentie } \} \\
 & \forall x((p(x) \rightarrow q) \wedge (q \rightarrow p(x))) \\
\Longleftrightarrow & \quad \{ \text{ 33a: } \forall \text{ distribueert over } \wedge \} \\
 & \forall x(p(x) \rightarrow q) \wedge \forall x(q \rightarrow p(x)) \\
\Longleftrightarrow & \quad \{ \text{ 10b en 10a: implicatie } \} \\
 & \forall x\, \neg(p(x) \wedge \neg q) \wedge \forall x(\neg q \vee p(x)) \\
\Longleftrightarrow & \quad \{ \text{ 8c: De Morgan } \} \\
 & \neg \exists x(p(x) \wedge q) \wedge \forall x(\neg q \vee p(x)) \\
\Longleftrightarrow & \quad \{ \text{ 34b; } x \text{ niet vrij in } q \} \\
 & \neg(\exists x\, p(x) \wedge q) \wedge \forall x(\neg q \vee p(x)) \\
\Longleftrightarrow & \quad \{ \text{ 10b: implicatie } \} \\
 & (\exists x\, p(x) \rightarrow q) \wedge \forall x(\neg q \vee p(x)) \\
\Longleftrightarrow & \quad \{ \text{ 34a; } x \text{ niet vrij in } q \} \\
 & (\exists x\, p(x) \rightarrow q) \wedge (\neg q \vee \forall x\, p(x)) \\
\Longleftrightarrow & \quad \{ \text{ 10a: implicatie } \} \\
 & (\exists x\, p(x) \rightarrow q) \wedge (q \rightarrow \forall x\, p(x))
\end{array}$$

Conclusie: $\forall x(p(x) \leftrightarrow q) \Longleftrightarrow (\exists x\, p(x) \rightarrow q) \wedge (q \rightarrow \forall x\, p(x))$.