RAF belangrijk te onthouden

Auteur: Daan Pape

Hoofdstuk 1

symbool	omschrijving		lees als
$\neg$	negatie (ontkenning)	$\neg p$	niet p het is niet zo dat p
$\wedge$	conjunctie	$p \wedge q$	p en q
$\vee$	disjunctie	$p \vee q$	p of q
$\Rightarrow$	implicatie	$p \Rightarrow q$	als p dan q p impliceert q p is voldoende voor q
$\Leftarrow$	gevolg	$p \Leftarrow q$	p volgt uit q p is nodig voor q
$\equiv$	equivalentie	$p \equiv q$	p is equivalent met q p als en slechts als q
$\not\equiv$	inequivalentie exclusieve of	$p \not\equiv q$	p is niet equivalent met q ofwel p ofwel q

Er geldt steeds:

$$p \Leftarrow q \equiv q \Rightarrow p$$

p	q	$p \Rightarrow q$
F	F	T
F	T	T
T	F	F
T	T	T

Aantonen dat gevolgtrekking geldig is: aantoneen dat als de permissen allemaal *waar* zijn dat de conclusie dan ook *waar* moet zijn. M.a.w de conjunctie van alle premissen impliceert de conclusie.

Hoofdstuk 2

Als men met kwantoren werkt is het zeer belangrijk om onderscheid te maken tussen twee soorten kwantoren:

1. *vrije veranderlijke*: deze staan voor objecten waarover de uitspraak iets zegt, verschillende waarden invullen kan leiden tot betekenisverandering en een andere waarheidswaarde.

2. *gebonden veranderlijke*: ook wel *dummy variabele* genoemd is enkel een letter die er staat ter verduidelijking van het idee. Meestal kan deze geëlimineerd worden of verander worden door een andere letter.

Een binaire relatie R in X is

1. reflexief als en slechts als $\forall x \in X \ . \ xRx$
2. antireflexief als en slechts als $\forall x \in X \ . \ \neg(xRx)$
3. symmetrisch als en slechts als $\forall x, y \in X \ . \ xRy \Rightarrow yRx$
4. antisymmetrisch als en slechts als $\forall x, y \in X \ . \ xRy \wedge yRx \Rightarrow x = y$
5. transitief als en slechts als $\forall x, y, z, \in X \ . \ xRy \wedge yRz \Rightarrow xRz$

Je kan bewijzen dat voor een strikt geordende verzameling geldt dat als die antireflexief en transitief is dat die ook antisymmetrisch:

(1) R is anti-reflexief: $\forall a \in S. \neg aRa$

(2) R is transitief: $\forall a, b, c \in S. aRb \wedge bRc \Rightarrow aRc$

We leveren een bewijs uit het ongerijmde: Stel dat R wel symmetrisch is dan geldt $\exists a, b \in S. aRb \wedge bRa$. Aangezien de verzameling transitief is moet ook gelden dat $aRb \wedge bRa \Rightarrow aRa$. Dit is echter strijdig met de opgelegde antireflexiviteit en dus moet S anti-symmetrisch zijn.

Er zijn verschillende soorten relaties:

1. *equivalentierelatie*: reflexief, symmetrisch, transitief
2. *partieel geordende relatie*: reflexief, antisymmetrisch, transitief
3. *totaal geordende relatie of ketting*: een partieel geordende relatie met bijkomende voorwaarde: $\forall x, y \in X \ . \ x \preceq y \vee y \preceq x$
4. *strikt geordende relatie*: elk koppel $(X, \prec)$ bestaande uit een niet lege verzameling X en een binaire relatie $\prec$ in X die antireflexief en transitief is.

In een *poset* partially ordered set, zijn er belangrijke dingen te definiren:

- b is een bovengrens voor A als en slechts als:

$$\forall a \in A \ . \ a \preceq b$$

- b is een ondergrens voor A als en slechts als:

$$\forall a \in A \ . \ b \preceq a$$

- b is het grootste element voor A als en slechts als:

$$b \in A \wedge b \text{ is een bovengrens voor } A$$

- b is het kleinste element voor A als en slechts als:

$$b \in A \wedge b \text{ is een ondergrens voor } A$$

- b is het supremum voor A, genoteerd als $\sup A = b$ als en slechts als:

$$b \text{ is een bovengrens voor } A \wedge \forall x \in X \ . \ (x \text{ is een bovengrens voor } A \Rightarrow b \preceq x)$$

- b is het infimum voor A, genoteerd als $\inf A = b$ als en slechts als:

$$b \text{ is een ondergrens voor } A \wedge \forall x \in X \ . \ (x \text{ is een ondergrens voor } A \Rightarrow x \preceq b)$$

- b is een maximaal element voor A als en slechts als:

$$b \in A \wedge \forall x \in A \ . \ b \preceq x \Rightarrow x = b$$

- b is een minimaal element voor A als en slechts als:

$$b \in A \wedge \forall x \in A \ . \ x \preceq b \Rightarrow x = b$$

Hoofdstuk 3

Pythagorees drietal: als $x, y, z \in \mathbb{N}$ en er geldt $x^2 + y^2 = z^2$ dan wordt (x, y, z) een pythagorees drietal genoemd.

Eigenlijke breuk: $\frac{a}{b}$ is een eigenlijke breuk als a en b geen gemeenschappelijke priemfactoren hebben.

Existentiestelling: een stelling waarin het bestaan van minimum één geval wordt aangetoont.

Bewijsmogelijkheden:

1. **Universele veralgemening**: het wordt voor een willekeurig iets bewezen, dus het geldt voor alles.
2. **Universele instantiatie**: een andere benaming voor $\forall$-eliminatie.
3. **Existentiële veralgemening**: men concludeert dat het te bewijzen waar is op basis van de wetenschap dat er een specifiek geval bestaat. Dit kan enkel toegepast worden als er moet bewezen worden dat er minimum één geval bestaat. Dit komt neer op $\exists$-introductie.
4. **Existentiële instantiatie**: het is geweten dat er zo'n getal bestaat en er wordt één zo'n getal gekozen in het bewijs, meestal een nieuwe letter.

Bewijstechnieken:

1. **Bewijs door aanname van het antecedent**: er wordt aangenomen dat het antecedent waar is en vervolgens wordt direct bewezen dat het consequent dan ook waar is.
2. **Bewijs door contrapositie**: Deze methode steunt op het feit dat $p \Rightarrow q \equiv \neg q \Rightarrow \neg p$ en dat we dus het laaste kunnen bewijzen als bewijs voor het eerste.
3. **Bewijs uit het ongerijmde of bewijs door contradictie**: Er wordt aangenomen dat het te bewijzen niet geldt om zo tot een strijdigheid te komen.
4. **Bewijs door gevallenonderzoek**: het te bewijzen wordt opgesplitst en de delen worden bewezen samen met het bewijs dat alle gevallen samen de volledige mogelijkhedenverzameling bestrijkt.

5. **Bewijs door wederzijdse implicatie**: Bewijs van de nodige voorwaarde en voldoende voorwaarde appart.

Het **axioma van de goede ordening** stelt dat elke niet lege deelverzameling van $\mathbb{N}$ een kleinste element heeft in de poset $(\mathbb{N}, \leq)$.

Hoofdstuk 4

Het **axioma van de goede ordening** stelt dat elke niet lege deelverzameling van $\mathbb{N}$ een kleinste element heeft in de poset $(\mathbb{N}, \leq)$. De strikte orderelatie $<$ in $\mathbb{N}$ wordt om die reden een **goede ordening** genoemd. Inductie kan ook in andere posets $(X, \preceq)$ worden toegepast die uitgerust zijn met een orderelatie $\preceq$ die niet noodzakelijk totaal is.

Inductie is enkel geldig als de verzameling **goed gefundeerd** is, m.a.w. elke niet ledige deelverzameling een minimaal element bezit. Sterker zelfs, een poset $(X, \preceq)$ is goed gefundeerd als en slechts als inductie over $(X, \preceq)$ een geldige bewijstechniek is.

Een goed gefundeerde verzameling die daarnaast oook nog totaal geordend is wordt **goed geordend** genoemd. $(\mathbb{N}, \leq)$ is goed geordend als en slechts als $(\mathbb{N}, \leq)$ sterke inductie toelaat.

Er zijn twee soorten inductie:

1. *zwakke inductie*: deze vorm van inductie gaat terug op volgende rekenregel:

$$\forall n \in \mathbb{Z}_{\geq n_0} \,.\, P(n) \equiv P(n_0) \wedge (\forall k \in \mathbb{Z}_{\geq n_0} \,.\, P(k) \Rightarrow P(k+1))$$

   In de cursus en examens wordt volgend formaat aangeraden:

   (a) **(Inductiebasis)** Bewijs voor $P(n_0)$

   (b) **(Inductiestap)** Zij k een willekeurig getal. Stel dat $P(k)$ geldt. Bewijs voor $P(k+1)$

2. *sterke inductie*: deze vorm van inductie gaat terug op volgende stelling:

$$\forall n \in \mathbb{N} \,.\, P(n) \equiv \forall m \in \mathbb{N} \,.\, (\forall j \in \mathbb{N}_{<m} \,.\, P(j)) \Rightarrow P(m)$$

   Het is dus niet nodig om een basisgeval te bewijzen.

Hoofdstuk 5

Een Hoare triplet bestaat uit:

$$\{p\}S\{q\}$$

1. p : de preconditie
2. S : het programmasegment
3. q : de postconditie

Om bewijzen te vormen wordt veel gebruik gemaakt van **substitutie**. Als we de veranderlijke w substitueren door een uitdrukking in E in een uitdrukking g wil dit zeggen dat we alle vrije voorkomens van w in G vervangen door E. We noteren de uitdrukking dan als $G[w := E]$. Bv:

$$(a \cdot x + y)[x := z \cdot b] = a \cdot (z \cdot b) + y$$

Substitutie is linksassociatief, d.w.z. dat $G[w_1 := E_1][w_2 := E_2]$ gedefinieerd is als $(G[w_1 := E_1])[w_2 := E_2]$. Substitutie heeft ook steeds de hoogste prioritiet. Zo is bv.

$$z + y[z := a] = z + y$$

terwijl

$$(z + y)[z := a] = a + y$$

We kunnen omgekeerde substitutie gebruiken om gegeven een postconditie q en een toekenningsopdracht $x := E$ de zwakste preconditie te berekenen:

$$\{q[x := E]\}x := E\{q\}$$

Conditionele opdrachten hebben vaak volgende vorm:

$$\text{if } b \text{ then } S_1 \text{ else } S_2$$

met b een predikaat en S_1, S_2 programmasegmenten. Er zijn twee soorten

- Om aan te tonen dat $\{p\}$ if b then S_1 else S_2 $\{q\}$ een geldig Hoare-triplet is volstaat het aan te tonen dat $\{p \wedge b\}S_1\{q\}$ en $\{p \wedge \neg b\}S_1\{q\}$ geldige Hoare-tripletten zijn.
- Om aan te tonen dat $\{p\}$ if b then S_1 $\{q\}$ een geldig Hoare-triplet is volstaat het aan te tonen dat $\{p \wedge b\}S_1\{q\}$ een geldig Hoare-triplet is en dat $(p \wedge \neg b) \Rightarrow q$.

Lussen hebben vaak de volgende vorm:

$$\text{while } b \text{ do } S$$

met b een predikaat en S een programmasegment. Elke uitvoering van S wordt een *iteratie* genoemd en als b vals is zullen er dus 0 iteraties zijn.

De **lusinvariant** is een predikaat dat waar blijft na elke iteratie van de lus. M.a.w. p is een lusinvariant voor de lus "while b do Säls en slechts als $\{p \wedge b\}S\{p\}$ een geldig Hoare-triplet is.

Als p een lusinvariant is en indien de lus eindigt moet $\{p\}$ while b do $S\{p \wedge \neg b\}$ een geldig Hoare-triplet zijn.

Om nu daadwerkelijk te bewijzen dat de lus eindigt wordt van een *begrenzingsfunctie* gebruik gemaakt. Dit is een uitdrukking waarvan de waarde een geheel getal is dat een bovengrens is voor het aantal iteraties van de lus dat nog moet uitgevoerd worden. We bewijzen dus dat:

1. elke iteratie van de lus moet de begrenzingsfunctie met minstens 1 verkleinen
2. de begrenzingsfunctie mag niet kleiner worden dan 0

deze twee eigenschappen samen bewijzen dat de lus na een eindig aantal iteraties *moet* eindigen. Om te bewijzen dat een lus eindigd bewijzen we dus concreet:

1. $p \Rightarrow t \geq 0$, m.a.w. de begrenzingsfunctie kan niet kleiner worden dan 0.
2. $\{p \wedge b \wedge t = K\}S\{t < K\}$ is een geldig Hoare-triplet, m.a.w. elke iteratie verminderd de begrenzingsfunctie

Volgend is een overzicht van de verschillende bewijstechnieken:

Correctheid van een toekenningsopdracht $x := E$ m.b.t. preconditie p en postconditie$q$:

$$\frac{p \Rightarrow q[x := E]}{\{p\}x := E\{q\}}$$

Correctheid van een samengesteld programma $S_1; S_2$ m.b.t. preconditie p en postconditie r

$$\frac{\begin{array}{c}\{p\}S_1\{q\} \\ \{q\}S_1\{r\}\end{array}}{\{p\}S_1; S_2\{r\}}$$

Correctheid van een conditionele opdracht "if b then S_1 else S_2" m.b.t. preconditie p en postconditie q

$$\frac{\begin{array}{c}\{p \wedge b\}S_1\{q\} \\ \{p \wedge \neg b\}S_2\{q\}\end{array}}{\{p\} \text{ if } b \text{ then } S_1 \text{ else } S_2 \ \{q\}}$$

Coorectheid van een conditionele opdracht "if b then S_1" m.b.t. preconditie p en postconditie q:

$$\frac{\begin{array}{c}\{p \wedge b\}S_1\{q\} \\ (p \wedge \neg b) \Rightarrow q\end{array}}{\{p\} \text{ if } b \text{ then } S_1 \ \{q\}}$$

Correctheid van een lus "while b do S" m.b.t. preconditie q en postconditie r:

$$\frac{\begin{array}{c}q \Rightarrow p[\text{na substitutie van init omgekeerd}] \\ \{p \wedge b\}S\{p\} \\ p \Rightarrow t \geq 0 \\ \{p \wedge b \wedge t = K\}S\{t \leq K\} \\ p \wedge \neg b \Rightarrow r\end{array}}{\{q\} \text{ while } b \text{ do } S \ \{r\}}$$

p is een lusinvariant en t is een begrenzingsfunctie.

Andere

$$x^{\frac{a}{b}} = \sqrt[b]{x^a}$$