Bewijstechnieken

Marc Denecker en Robbe Van den Eede

October 2023

Samenvatting

Met de bewijstechnieken van Sectie 2 in dit document kun je zien in Sectie 3 hoe je het bewijs van de bewijsopgave kunt aanvatten (en ook veel bewijzen in de cursus overigens). In Sectie 4 wordt het antwoord gegeven op een vraag van de vorm: "wat als de stelling onwaar zou zijn, wat is dan wel waar, en hoe zou je dat bewijzen?". In Sectie 1 staat een vraag die mogelijks wel eens op een examen kan gesteld worden. In sectie 5 staat een uitgewerkt voorbeeld. Feedback is welkom.

1 Bewijstechnieken

Het doel van dit document is om de studenten een aantal bewijstechnieken aan te bieden waarmee bewijzen gecomponeerd kunnen worden, op een natuurlijke en systematische manier.

Het vinden van een bewijs voor een stelling kan diep, origineel inzicht vereisen. Maar vaak genoeg zijn bewijzen, of minstens delen ervan, eenvoudig te bekomen met behulp van bewijstechniek. Bewijstechniek laat toe om een systematische redenering op te bouwen, en om een te bewijzen complexe eigenschap te vereenvoudigen tot een eenvoudige eigenschap die triviaal te bewijzen is.

De wiskundige in spe zoekt een bewijs voor een stelling:

$$(\textbf{Geg. } A; \textbf{ TB.}: B)$$

waarbij A één of meer uitspraken/eigenschappen zijn over bepaalde wiskundige objecten , en B een uitspraak is over diezelfde wiskundige objecten. A bevat 1 of meerdere assumpties over die wiskundige objecten, en B is de te bewijzen uitspraak. Vervolgens worden technieken toegepast om dit paar te herleiden tot één of meer paren

$$(\textbf{Geg. } A'; \textbf{ TB. } B')$$

waarbij B' eenvoudiger is dan B, en/of A' sterker is dan A in de zin dat het meer assumpties bevat. Dit proces gaat door totdat A' voldoende sterk, en B' zo eenvoudig is dat B' triviaal volgt uit A'. Bv. omdat B' een van de assumpties is in A', of omdat A' een inconsistentie bevat.

Deze observatie heeft lang geleden ($\pm$ 80 jaar) geleid tot de ontwikkeling van formele bewijsmethodes zoals *natuurlijke deductie* en *sequent calculus*. Ook de methode van KE-bewijzen uit de cursus Logica is afgeleid hiervan.

Deze tekst is gericht op het maken van bewijzen, niet op de formele studie van bewijsvoering. Ons doel is om informele regels aan te bieden om een bewijs te vinden. We hebben niet geprobeerd een minimaal compleet systeem uit te werken zoals in bewijstheorie wel gebeurt: de voorgestelde bewijsregels zijn verondersteld nuttig te zijn, maar het bevat redundanties en mogelijks ook hiaten.

Op het examen kan gevraagd worden:

> **stel dat we stelling ... moeten bewijzen. Wat zou uw eerste stap zijn?**

Het antwoord is één van de bewijsregels.

2 Reduceren van (**Geg.** A, **TB.** B)

Een paar (**Geg.** A, **TB.** B) noemen we een stelling.

Voorbeeld 1 Een voorbeeld van zo'n paar is:

> **Geg.** Zij S een verzameling en $\sim$ een equivalentierelatie op S.
> **TB.** Voor alle $x, y \in S$ geldt: $x \sim y$ asa $|x| = |y|$.

Een bewijs voor zo'n stelling is een argument waarom uit een gegeven A het te bewijzen B volgt. Men verwacht dat een bewijs een sequentie van uitspraken $A, A_1, \ldots, A_n$ is waarbij elke $A_i, i > 0$ logisch volgt uit de $A, \ldots A_{i-1}$ en B gelijk is aan A_n. Dit is niet het volledige verhaal.

In realiteit bewijst men een stelling (**Geg.** A; **TB.** B) vaak door de stelling te herleiden tot andere eenvoudiger stellingen die vervolgens bewezen worden. Een sprekend voorbeeld is een bewijs uit het ongerijmde. Daar bewijst men (**Geg.** A, niet B; **TB.** inconsistentie).

In de praktijk is een bewijs eerder een boom van verschillende deelstellingen met bovenaan de te bewijzen stelling en in de bladeren triviaal ware stellingen. Een stelling (**Geg.** A, **TB.** B) in een node van de boom wordt herleid tot deelstellingen in de kinderen van de node. Een bewijs voor deze deelstellingen is ook een bewijs voor (**Geg.** A, **TB.** B). Deze kinderen bekomt men door de stelling te herwerken, ontbinden, of te vereenvoudigen. Zo'n boom kan lineaire takken bevatten overeenkomend met een lineair bewijs $A, A_1, \ldots, B$, maar ook andere soorten herleidingen of opsplitsingen. De bladeren van de boom bevatten triviale stellingen, bv. waar B één van de assumpties in A is. Of, als A een contradictie bevat, want uit een contradictie volgt alles.

De context van de stelling (Geg. A; TB. B) In A en B wordt gesproken over een verzameling van wiskundige objecten die benoemd worden door symbolen. Deze verzameling van symbolen en de objecten die ze benoemen noemen we de context van de stelling. In Voorbeeld 1 benoemt S een willekeurige verzameling en $\sim$ een willekeurige equivalentierelatie op S.

Daarentegen, gekwantificeerde symbolen behoren niet tot de context. In Voorbeeld 1 zijn de symbolen x en y in het te bewijzen expliciet gekwantificieerd door "voor alle $x, y \in S$". Ze behoren dus niet tot de context van de stelling.

Ook de context evolueert in een bewijs; het groeit in sommige stappen en krimpt dan weer in in andere, volgens bepaalde intuïtieve regels. Bv. in een bewijs verschijnt vaak een uitdrukking van de vorm:

Zij x een (willekeurig) element van de verzameling S.

Bij zo'n uitspraak gebeuren twee dingen: de context groeit doordat vanaf nu het symbool x een willekeurig object uit S benoemt, en het huidige **Geg.** A wordt uitgebreid met de assumptie $x \in S$. Nadat de deelstelling (**Geg.** A, $x \in S$; **TB.** B) bewezen is, verdwijnt x weer uit de context. Dan is x weer een ongebonden symbool. In latere delen van het bewijs kan x hergebruikt worden, door het te binden aan een ander wiskundig object door middel van een nieuwe zin van de vorm "Zij x ...". Bv. door de zin "Zij x een getal in het interval $[1, N]$". Dit is zoals variabelen in logische formules.

We noemen de verzameling van objecten $\sigma_1, \ldots, \sigma_n$ en de symbolen die ze benoemen de **context** van de stelling (**Geg.** A, **TB.** B).

De context kan een aantal welbepaalde vaste objecten bevatten, bv. de verzameling van de natuurlijke getallen benoemd door het symbool $\mathbb{N}$, maar ook willekeurig gekozen objecten. In Voorbeeld 1 benoemd het symbool S een willekeurige verzameling, en $\sim$ een willekeurige equivalentierelatie op S.

Wat er wordt bewezen Wat werd bewezen als een bewijs voor (**Geg.** A; **TB.** B) gevonden wordt? Zij $\sigma_1, \ldots, \sigma_n$ de willekeurig gekozen objecten uit de context van deze stelling. Wanneer we erin slagen een bewijs voor (**Geg.** A; **TB.** B) te vinden, dan geldt de volgende eigenschap:

voor alle $\sigma_1, \ldots, \sigma_n$ die voldoen aan A geldt B.

Merk op : in elke stelling (**Geg.** A; **TB.** B) wordt impliciet gekwantificeerd over alle willekeurig gekozen objecten in de context! Dat is belangrijk bv. als we willen bewijzen dat een stelling onwaar is. Zie Sectie 4 hiervoor.

In Voorbeeld 1 bestaat de context van de stelling uit S en $\sim$. Als we een bewijs voor de stelling vinden, dan geldt het te bewijzen voor *elke* verzameling S en elke equivalentierelatie $\sim$ op S.

De bewijsregels We formuleren een aantal regels om stellingen (**Geg.** A; **TB.** B) te vereenvoudigen. Verwacht niet om in een bewijs in een wiskundige tekst expliciet zo'n serie van paren te zien. Maar we kunnen garanderen dat bij

vele overgangen in zo'n bewijs één van deze regels wordt toegepast. Voor een voorbeeld hoe dit in zijn werk gaat vewijzen we naar Voorbeeld 2.

De eerste groep regels dient om een bewijs af te sluiten. Het zijn de triviale stellingen.

1. (Geg inconsistentie) Bewijs door inconsistent gegeven:

   (**Geg.** A; B; niet B ; **TB.** C)
   $\rightarrow$
   QED

   QED staat voor "quod erat demonstrandum", of "wat bewezen moest worden".

   Uit een inconsistentie kan alles bewezen worden. Als het gegeven een inconsistentie bevat, dus een uitspraak B en zijn negatie niet B, dan is het bewijs geleverd, voor gelijk welk te bewijzen C, zelfs als C gelijk is aan "inconsistentie", zoals in een bewijs uit het ongerijmde.

2. (TB subsumptie) Het te bewijzen zit bevat in het gegeven:

   (**Geg.** A; B; **TB.** B)
   $\rightarrow$
   QED

   Als het gegeven het te bewijzen bevat, dan is het bewijs triviaal geleverd.

De volgende groep regels dient om het te bewijzen te vereenvoudigen.

3. (TB conjunctie) Conjunctie elimineren uit **TB.**:

   (**Geg.** A; **TB.** B en C)
   $\rightarrow$
   (1) (**Geg.** A; **TB.** B)
   (2) (**Geg.** A; **TB.** C)

   Als (1) en (2) bewezen zijn, dan is de oorspronkelijke stelling bewezen.

   Het te bewijzen werd vereenvoudigd.

4. (TB disjunctie) Disjunctie elimineren uit **TB.**:

   (**Geg.** A; **TB.** B of C)

   $\rightarrow$

   (**Geg.** A; veronderstel niet B **TB.** C)

   Het gegeven werd versterkt, het te bewijzen vereenvoudigd. (En natuurlijk mag je B en C verwisselen.)

5. (TB $\forall$) Universele kwantor elimineren uit **TB.**:

   (**Geg.** A; **TB.** voor alle $x \in S$ geldt $B[x]$)

   $\rightarrow$

   (**Geg.** A; zij u een willekeurig element van S; **TB.** $B[u]$)

   Men kiest het symbool u zodat u niet in de context van de stelling voorkomt. Eventueel kan men x zelf kiezen.

   Deze belangrijke regel laat toe om een universele kwantor uit het TB te elimineren. Het te bewijzen wordt eenvoudiger en het gegeven wordt versterkt. De context wordt uitgebreid.

6. (TB $\exists$) Existentiële kwantor elimineren uit **TB.**:

   (**Geg.** A; **TB.** er bestaat $x \in S$ zodat $B[x]$)

   $\rightarrow$

   (**Geg.** A; **TB.**: $a \in S$ en $B[a]$)

   Dit vereist dat je object a uit de context vindt waarvoor je kunt bewijzen dat $a \in S$ en $B[a]$.

7. (TB Implicatie) Implicatie verwijderen uit **TB.**:

   (**Geg.** A; **TB.**: als B dan C.)

   $\rightarrow$

   (**Geg.** A; B; **TB.**: C.)

8. (TB equivalentie)

   (**Geg.** A; **TB.**: B asa C)

$\rightarrow$

($\Rightarrow$) (**Geg.** A; veronderstel B; **TB.** C)

($\Leftarrow$)) (**Geg.** A; veronderstel C; **TB.** B)

Als beide delen kunnen bewezen worden, is de equivalentie bewezen.

9. (TB deelverzameling)

   (**Geg.** A; **TB.** $S \subseteq T$)

   $\rightarrow$

   (**Geg.** A; zij x een willekeurig element van S; **TB.** $x \in T$.

10. (TB gelijkheid van verzamelingen)

    (**Geg.** A; **TB.** $S = T$)

    $\rightarrow$

    ($\subseteq$) (**Geg.** A; **TB.** $S \subseteq T$)

    ($\supseteq$) (**Geg.** A; **TB.** $S \supseteq T$)

    Het bewijs wordt dus opgesplitst in twee deelstellingen. Als beide slagen, is de oorspronkelijke stelling bewezen.

De volgende regels dienen om het gegeven te versterken. Hieronder wordt het onderlijnde toegevoegd aan het gegeven ter versterking.

11. (Case analyse)

    (**Geg.** A; **TB.** B)

    $\rightarrow$

    (1) (**Geg.** A; $\underline{C}$ **TB.** B)

    (2) (**Geg.** A; $\underline{\text{niet } C}$ **TB.** B)

    Het gegeven werd 2x versterkt.

12. (Ongerijmde) Bewijs uit het ongerijmde:

    (**Geg.** A; **TB.** B)

    $\rightarrow$

    (**Geg.** A; $\underline{\text{niet } B}$; **TB.** inconsistentie)

Te allen tijde kan men een stelling of een onderdeel van een stelling met deze regel omzetten in een bewijs uit het ongerijmde.

13. (Geg disjunctie) Disjunctie in **Geg.**:

    (**Geg.** A; B_1 of B_2; **TB.** C)
    $\rightarrow$
    (1) (**Geg.** A, $\underline{B_1}$; **TB.** C)
    (2) (**Geg.** A, $\underline{B_2}$; **TB.** C)

    Het gegeven werd 2x versterkt. Dit werkt ook met een langere disjunctie B_1 of $\ldots$ of B_n.

14. (Geg $\exists$) Existentiële kwantor in **Geg.** instantiëren:

    (**Geg.** A; er bestaat $x \in S$ zodat $B[x]$; **TB.** C)
    $\rightarrow$
    (**Geg.** A; er bestaat $x \in S$ zodat $B[x]$; $\underline{u \in S;\ B[u];}$ **TB.** C)

    Een bestaand object wordt benoemd door het symbool u. Het symbool u mag niet in de context zitten. Het object en u worden toegevoegd behoren tot de context totdat dit onderdeel van het bewijs af is.

15. (Geg implicatie):

    (**Geg.** als A dan C; A ; **TB.** B)
    $\rightarrow$
    (**Geg.** als A dan C; A ; $\underline{C}$ **TB.** B)

    Dezelfde regel kan ook toegepast worden als een equivalentie gegeven is.
    (**Geg.** A asa C; A ; **TB.** B)
    $\rightarrow$
    (**Geg.** A asa C; A ; $\underline{C}$ **TB.** B)

16. (Geg intro $\exists$)
    Omgekeerd redeneren is ook mogelijk:

    (**Geg.** A; $c \in S$; $B[c]$; **TB.** C)
    $\rightarrow$

(**Geg.** A; $c \in S$; $B[c]$; $\underline{\text{er bestaat } x \in S \text{ zodat } B[x]}$; **TB.** C)

17. (Geg $\forall$) Universele kwantor in **Geg.**:

    (**Geg.** A; voor alle $x \in S$ geldt $B[x]$; $a \in S$; **TB.** C)
    $\rightarrow$
    (**Geg.** A; voor alle $x \in S$ geldt $B[x]$; $a \in S$; $\underline{B[a]}$; **TB.** C)

Een belangrijke manier om het gegeven te versterken is het toepassen van een lemma. Een lemma is een onafhankelijke stelling die eerder bewezen werd, of geldig is per assumptie. Veel lemma's zijn rechtstreeks afkomstig uit een definitie. Bv., per definitie geldt $A \cap B = \{x | x \in A \wedge x \in B\}$. Dit geeft aanleiding tot twee geldige stellingen die overal elders gebruikt mogen worden.

- (**Geg.** $x \in A \cap B$; **TB.** $x \in A$ en $x \in B$)
- (**Geg.** $x \in A$; $x \in B$; **TB.** $x \in A \cap B$).

We zijn bekend met immens veel lemma's van dit soort. Het zou onbegonnen werk zijn deze allemaal op te schrijven in de assumpties van een stelling. Nieuwe, nonevidente lemma's moeten echter wel bewezen worden. Een bewijs voor een stelling kan dus voorafgegaan worden door bewijzen van 1 of meerdere lemma's. In het bewijs van een lemma mag het lemma zelf niet toegepast worden. Anders zou een **circulariteit** ontstaan, zoals in volgend lemma.

> **Lemma 1** Alle natuurlijke getallen zijn priem.
>
> **Bewijs** Door toepassing van Lemma 1 zijn alle natuurlijke getallen priem. **QED**

Vandaar dat het bewijs van een lemma geleverd moet zijn voordat het gebruikt wordt.

Eens een lemma bewezen is, mag het toegepast worden in het bewijs van een stelling om het gegeven te versterken. De volgende regels gaan daarover.

18. (Lemma toepassen) Stel dat lemma (**Geg.** C; **TB.** D) beschikbaar is. Dan kan dit lemma later toegepast worden om het gegeven van een andere stelling te versterken:

    (**Geg.** A; C; **TB.** B)
    $\rightarrow$
    (**Geg.** A; C; $\underline{D}$; **TB.** B)

Let wel, het is niet altijd zo dat letterlijk C gegeven is. Soms is een C' gegeven, waarin bepaalde termen gebonden moeten worden aan symbolen uit de context van het lemma om C te bekomen. Dan kan het lemma gebruikt worden om D' af te leiden bekomen uit D door symbolen uit D te vervangen door de termen in C'. Dit wordt geïllustreerd met een voorbeeld.

We hebben het lemma (**Geg.** $x \in A$; $x \in B$; **TB.** $x \in A \cap B$). Dit lemma wordt hieronder gebruikt.

(**Geg.** $1 \in \{0,1\}$, $1 \in \{1,2\}$; **TB.** $1 \in \{0,1\} \cap \{1,2\}$)
($\rightarrow$ (lemma toepassen met $x = 1, A = \{0,1\}, B = \{1,2\}$)
(**Geg.** $1 \in \{0,1\}$; $1 \in \{1,2\}$; $\underline{1 \in \{0,1\} \cap \{1,2\}}$; **TB.** $1 \in \{0,1\} \cap \{1,2\}$)
$\rightarrow$ (subsumptie)
QED

(Lemma toepassen) heeft vele toepassingen. We sommen er een paar op.

19. (Definitie uitvouwen) en (Definitie opvouwen)

Stel dat de theorie waarin we werken een definitie bevat: $P(x)$ asa $D[x]$. Hiermee zijn twee lemma's verbonden:

- (**Geg.** $P(x)$ **TB.** $D[x]$), en
- (**Geg.** $D(x)$ **TB.** $P[x]$).

Dit geeft aanleiding tot twee speciale vormen van (lemma toepassen) :

(definitie uitvouwen)

(**Geg.** A; $P(a)$; **TB.** B)
$\rightarrow$
(**Geg.** A'; $P(a)$; $D(a)$ **TB.** B)

(definitie opvouwen)

(**Geg.** A; $D[a]$; **TB.** B)
$\rightarrow$
(**Geg.** A'; $D(a)$; $P(a)$ **TB.** B)

20. (**Geg.** vereenvoudigen)

    Het is mogelijk dat men een stelling bekomt van de vorm

    (**Geg.** $A_0; A_1$; **TB.** B)

    waarbij men inziet dat A_0 overbodig is om B te kunnen bewijzen. Dan mag men A_0 schrappen.

    (**Geg.** $A_0; A_1$; **TB.** B)

    $\rightarrow$

    (**Geg.** A_1; **TB.** B)

    Bv. in een lineair bewijs, bewijst men A_1 uit A_0 door middel van een lemma. Dan gebeurt het vaak dat B bewijsbaar is uit A_1. Dan mag A_0 geschrapt worden.

    Het schrappen van een uitspraak A_0 verwijdert potentieel ook een aantal objecten uit de context, namelijk al die objecten waarvan enkel gesproken wordt in A_0.

Herhaalde toepassing van regels die te bewijzen bewaren maar het gegeven versterken, geven aanleiding tot lineaire bewijzen.

Bewijsvoering, concreet en realistisch Een bewijs in een wiskundige tekst zal nooit bestaan uit een letterlijke en expliciete toepassing van al deze regels. Er is immers veel te veel redundantie in opeenvolgende deelstellingen aangezien een groot deel van het gegeven en te bewijzen gecopieerd wordt. Dat maakt het enorm onleesbaar. In een vlot bewijs wordt redunantie zoveel mogelijk vermeden. In elk punt in het bewijs wordt zoveel mogelijk enkel het nieuwe vermeld. Bv. in een lineaire afleiding $A_0, A_1, \ldots$ om het gegeven te versterken wordt telkens uitgelegd hoe A_i wordt afgeleid uit de premissen $A_0, \ldots, A_{i-1}$ en een lemma. Niettemin wordt in elke stap een van de bewijsregels toegepast.

3 Toepassing in Voorbeeld 1

In Voorbeeld 1 is de stelling:

> **Geg.** Zij S een verzameling en $\sim$ een equivalentierelatie op S.
> **TB.** Voor alle $x, y \in S$ geldt: $x \sim y$ asa $|x| = |y|$.

Men kan onmiddelijk zien aan de vorm van het te bewijzen dat we de volgende bewijsregels zullen moeten toepassen, om het te bewijzen te vereenvoudigen:

- (TB $\forall$) om de universele kwantificatie "voor alle $x, y \in S$" weg te werken. In het gegeven verschijnt dan "Zij x, y willekeurige elementen in S", en te bewijzen is "$x \sim y$ asa $|x| = |y|$".

- (TB equivalentie) om deze equivalentie weg te werken. Dit wordt omgezet in twee deelstellingen ($\Rightarrow$) en ($\Leftarrow$).

Het bewijs voor de stelling van Voorbeeld 1 zou dus als volgt kunnen beginnen:

> Zij $x, y \in S$.
> ($\Rightarrow$) Veronderstel dat $x \sim y$. **TB.** $|x| = |y|$.
> ...
> ($\Leftarrow$) Veronderstel dat $|x| = |y|$. **TB.** $x \sim y$.
> ...

On het bewijs te vervolledigen zul je ook andere bewijsregels moeten toepassen, bv. (TB gelijkheid van verzameling) om te bewijzen dat $|x| = |y|$, of (Geg definitie) of (Geg implicatie) om het gegeven $|x| = |y|$ uit te schrijven, enz.

4 Wat is geldig als de stelling (Geg. A; TB. B) onwaar is? Hoe bewijzen dat de stelling onwaar is?

Ter herinnering, zo'n stelling drukt uit dat alle objecten $\sigma_1, \ldots, \sigma_n$ uit de context die voldoen aan A, ook voldoen aan B.

Wat is dan waar als de stelling onwaar is? Dat er objecten $\sigma_1, \ldots, \sigma_n$ bestaan die voldoen aan A, maar niet voldoen aan B.

Hoe bewijst men zoiets? De te bewijzen stelling is nu van de vorm

(**Geg.** niets; **TB.** er bestaan $\sigma_1, \ldots, \sigma_n$ waarvoor A geldt, zodat B onwaar is)

Om dit te bewijzen is de bewijsregel (TB $\exists$) van toepassing. Je zoekt dus een objecten $\sigma_1, \ldots, \sigma_n$ die voldoen aan A maar niet aan B. Deze objecten vormen een **tegenvoorbeeld**. Kortom, zoek een tegenvoorbeeld!

5 Voorbeeld 2

Laat ons de bovenstaande bewijsregels gebruiken om de volgende stelling te bewijzen:

> **Geg.** Zij $f : X \to Y$ een injectie, en $A, B \subseteq X$.
> **TB.** $f(A \cap B) = f(A) \cap f(B)$.

We zullen twee bewijzen leveren hiervoor : eerst, een theoretisch bewijs (a) met de bewijsregels. Het zal duidelijk zijn dat dit veel te veel redundantie bevat. Dan een veel korter realistisch bewijs (b) maar waarbij we het verband met (a) uitleggen.

In ons bewijs zullen we gebruik maken van de volgende definities, die we zullen toepassen door middel van de bewijsregels (Definitie uitvouwen) of (Definitie opvouwen):

- $x \in A \cap B$ asa $x \in A$ en $x \in B$.
- Zij $C \subseteq X$. Dan $u \in f(C)$ asa er bestaat een $c \in C$ waarvoor $u = f(c)$.
- f is een injectie asa voor alle $x_1, x_2 \in X$ geldt dat als $f(x_1) = f(x_2)$, dan $x_1 = x_2$.

Bewijs

1. **Geg.** Zij $f : X \to Y$ een injectie, en $A, B \subseteq X$.[1]
   TB. $f(A \cap B) = f(A) \cap f(B)$.
   2. **Geg.** G
      TB. $f(A \cap B) \subseteq f(A) \cap f(B)$. (TB gelijkheid van verzamelingen)
      3. **Geg.** G; Zij u een willekeurig element van $f(A \cap B)$.
         TB. $u \in f(A) \cap f(B)$. (TB deelverzameling)
      4. **Geg.** G; $u \in f(A \cap B)$. Dan bestaat er een $x \in A \cap B$ zodat $u = f(x)$.
         TB. $u \in f(A) \cap f(B)$. (Definitie $f(X)$ ontvouwen)
         5. **Geg.** G; $u \in f(A \cap B)$. Zij $c \in A \cap B$ zodat $u = f(c)$.
            TB. $u \in f(A) \cap f(B)$. (Geg $\exists$)
         6. **Geg.** G; $u \in f(A \cap B)$; $c \in A \cap B$; $u = f(c)$. Dan $c \in A$ en $c \in B$.
            TB. $u \in f(A) \cap f(B)$. (Def $A \cap B$ ontvouwen)
      7. **Geg.** G; $u \in f(A \cap B)$; $u = f(c)$. Dan $c \in A$ en $c \in B$. Er bestaat een $x_1 \in A$ zodat $u = f(x_1)$, en een $x_2 \in B$ zodat $u = f(x_2)$.
         TB. $u \in f(A) \cap f(B)$. (Geg $\exists$ intro)
      8. **Geg.** G; $u \in f(A \cap B)$; Er bestaat een $x_1 \in A$ zodat $u = f(x_1)$, en een $x_2 \in B$ zodat $u = f(x_2)$. Dan $u \in f(A)$ en $u \in f(B)$.
         TB. $u \in f(A) \cap f(B)$. (Def f(X) opvouwen voor f(A) en f(B))
      9. **Geg.** G; $u \in f(A \cap B)$; $u \in f(A)$; $u \in f(B)$. Dan $u \in f(A) \cap f(B)$.
         TB. $u \in f(A) \cap f(B)$. (Def $\cap$ opvouwen voor $f(A) \cap f(B)$)
   10. QED. (TB subsumptie)
11. **Geg.** G
    TB. $f(A \cap B) \supseteq f(A) \cap f(B)$. (TB gelijkheid van verzamelingen)
    12. **Geg.** G; Zij u een willekeurig element van $f(A) \cap f(B)$.
        TB. $u \in f(A \cap B)$. (TB deelverzameling)
    13. **Geg.** G; $u \in f(A) \cap f(B)$. Dan bestaan er $x_1 \in A$ en $x_2 \in B$ zodat $u = f(x_1) = f(x_2)$.
        TB. $u \in f(A \cap B)$. (Def $\cap$ uitvouwen)
        14. **Geg.** G; $u \in f(A) \cap f(B)$; er bestaan $x_1 \in A$ en $x_2 \in B$ zodat $u = f(x_1) = f(x_2)$. Zij $a \in A$ en $b \in B$ zodat $u = f(a) = f(b)$.
            TB. $u \in f(A \cap B)$. 2x(Geg $\exists$)
        15. **Geg.** G; $u \in f(A) \cap f(B)$; $a \in A$; $b \in B$; $u = f(a) = f(b)$. Voor alle $x_1, x_2 \in X$ geldt dat als $f(x_1) = f(x_2)$, dan $x_1 = x_2$.
            TB. $u \in f(A \cap B)$. (Definitie f is injectie uitvouwen)
        16. **Geg.** G; $u \in f(A) \cap f(B)$; $a \in A$; $b \in B$; $u = f(a) = f(b)$; Voor alle $x_1, x_2 \ldots$. Dan $a = b$.
            TB. $u \in f(A \cap B)$. (lemma toepassen)

[1] Omdat deze condities steeds terugkomen in het gegeven, gebruiken we de letter G om hiernaar te verwijzen in de volgende stappen van het bewijs.

17. **Geg.** G; $u \in f(A) \cap f(B)$; $a \in A$; $b \in B$: $u = f(a) = f(b)$; $a = b$. Bijgevolg $a \in A \cap B$.
    TB. $u \in f(A \cap B)$. (Definitie $\cap$ opvouwen)
18. **Geg.** G; $u \in f(A) \cap f(B)$; Er bestaat een $x \in A \cap B$ zodat $u = f(x)$.
    TB. $u \in f(A \cap B)$. (geg $\exists$ intro)
19. **Geg.** G; $u \in f(A) \cap f(B)$. Er bestaat een $x \in A \cap B$ zodat $u = f(x)$. Dan $u \in f(A \cap B)$.
    TB. $u \in f(A \cap B)$. (Definitie f(X) opvouwen voor $f(A \cap B)$
20. QED. (TB subsumptie)

De indentatie in lijnen 2 en 11 duiden op het feit dat stelling 1 wordt opgedeeld in twee deelstellingen. De andere indentaties duiden op een verandering van de context. In stelling 1 bestaat deze context uit de symbolen f, X, Y, A en B, die respectievelijk gebonden zijn aan een functie en aan verzamelingen. In lijn 3 bijvoorbeeld, wordt de context uitgebreid met het symbool u, dat gebonden wordt aan een willekeurig element uit de verzameling $f(A \cap B)$.

Het bovenstaande bewijs voelt misschien wat kunstmatig en overdreven gedetailleerd aan. Onthoud dat de bovenstaande bewijsregels dan ook bedoeld zijn als leidraad, om op systematische wijze te komen tot wiskundige 'informele' bewijzen. Het formele bewijs van voordien kan bijvoorbeeld herwerkt worden tot volgend informeel bewijs. De nummers achter de verschillende stappen verwijzen naar de overeenkomstige lijnen uit bovenstaand formeel bewijs.

Bewijs.
Zij $f : X \to Y$ een injectie, en $A, B \subseteq X$. (1)
We tonen eerst aan dat $f(A \cap B) \subseteq f(A) \cap f(B)$. (2)
Zij u een willekeurig element van $f(A \cap B)$. (3)
Dan bestaat er een $c \in A \cap B$ zodat $u = f(c)$. (4, 5)
Aangezien $c \in A$ en $c \in B$, volgt dat $u \in f(A) \cap f(B)$. (6, 7, 8, 9)
Dit bewijst dat $f(A \cap B) \subseteq f(A) \cap f(B)$. (10)
Vervolgens tonen we aan dat $f(A \cap B) \supseteq f(A) \cap f(B)$. (11)
Zij u een willekeurig element van $f(A) \cap f(B)$. (12)
Dan bestaan er $a \in A$ en $b \in B$ zodat $u = f(a) = f(b)$. (13, 14)
Aangezien f een injectie is, volgt dat $a = b$. (15, 16)
We leiden af dat $a \in A \cap B$, en bijgevolg dat $u \in f(A \cap B)$. (17, 18, 19)
Dit bewijst dat $f(A \cap B) \supseteq f(A) \cap f(B)$. (20)
De twee inclusies tonen samen aan dat $f(A \cap B) = f(A) \cap f(B)$. $\square$