TI1300 Redeneren en Logica

College 2: Bewijstechnieken

Tomas Klos

Algoritmiek Groep

TU Delft

Opmerking

Voor alle duidelijkheid:

Het is verre van triviaal om

- definities te leren hanteren,
- beweringen 'op te lossen,'
- bewijzen te vinden,
- tegenvoorbeelden te construeren,

laat staat om uit het niets beweringen te formuleren.

Hier zijn geen pasklare methoden voor!

De mooiste bewijzen bevatten iets slims, creatiefs, elegantie ...

TU Delft

Met voorbeelden kun je niks bewijzen

Vermoeden (Goldbach (1742))

Elk even natuurlijk getal groter dan 2, is de som van twee priemgetallen.

Geverifieerd tot $1,8 \cdot 10^{18}$ (Augustus 2010)

Vermoeden (Riemann Hypothese (1859))

Het reële deel van elk niet-triviaal nulpunt van de Riemann zeta functie is 1/2. (Het is een functie over complexe getallen.)

Geverifieerd voor de eerste $1 \cdot 10^{13}$ nulpunten (2004).

Algemeen

Als er oneindig veel mogelijkheden zijn,
betekenen voorbeelden (wiskundig logisch gezien) niks.

lft

Directe en indirecte bewijzen

Direct bewijs

Begin bij de premissen, en redeneer rechtstreeks naar de conclusie toe.

Indirect bewijs

Begin bij de premissen, en redeneer vanaf de ontkenning van de conclusie naar een tegenspraak.

Andere namen:

- Bewijs uit het ongerijmde
- Reductio ad Absurdum

TU Delft

Bewijs uit het ongerijmde

Bewijs uit het ongerijmde

Om te bewijzen dat een uitspraak **waar** is, maak je de aanname dat de uitspraak **onwaar** is, en leid je daaruit een tegenspraak af.

Definitie (tegenspraak (contradictie, tegenstrijdigheid))

Een tegenspraak is het tegelijkertijd bestaan van een bewering en de ontkenning van diezelfde bewering.

Dan moet de aanname **onwaar** zijn, dus de uitspraak zelf **waar**!

Het beroemdste bewijs (uit het ongerijmde)

Definitie (Priemgetal)

Een natuurlijk getal > 1, slechts deelbaar door 1 en zichzelf.

Voorbeelden: 2, 3, 5, 7, 11, 13, 17, 19, 23, 29, ...

Stelling (Euclides)

Er bestaat geen grootste priemgetal.

Corollary

Er zijn oneindig veel priemgetallen.

Stelling. *Er bestaat geen grootste priemgetal.*

Bewijs (uit het ongerijmde).

Stel dat er wel een grootste priemgetal is, dus dat er n zijn.

$$x = p_1 \times p_2 \times \ldots \times p_n + 1$$

- x is een priemgetal of een samengesteld getal
  - priem: $x > p_n$ en staat dus niet op de lijst
  - samengesteld: dan heeft x een priemdeler, maar die staat niet op de lijst
- In beide gevallen mist er een priemgetal van de lijst.
- Een tegenspraak, want ze zouden er allemaal op staan.

De aanname is dus onjuist: er is geen grootste priemgetal. QED

Stelling. $\sqrt{2}$ *is geen rationaal getal.*

Definitie (Rationaal getal)

Een rationaal getal is een getal dat is te schrijven als $\frac{a}{b}$ $(a, b \in \mathbb{Z})$.

Bewijs (uit het ongerijmde).

Aanname: $\sqrt{2}$ is wel een rationaal getal.

- schrijf dan $\sqrt{2}$ als niet-vereenvoudigbare breuk a/b.
- dus $\sqrt{2} = a/b$, dan is $2 = a^2/b^2$, en is $a^2 = 2b^2$.
- dan is a^2 even, en dus is a even, dus $a = 2m$ en $a^2 = 4m^2$.
- dan is $2b^2 = 4m^2$, dus $b^2 = 2m^2$ en dus even, en ook b even.
- Dus a/b is vereenvoudigbaar—een tegenspraak!

De aanname is onjuist, $\sqrt{2}$ is dus geen rationaal getal. QED

Oefening (5 minuten)

Stelling

Er is geen kleinste rationaal getal groter dan 0.

Bewijs (uit het ongerijmde).

Stel: er is wel een kleinste rationaal getal groter dan 0.

- noem dit getal $r = a/b$.
- beschouw nu het getal $x = r/2 = a/(2b)$.
- x is een rationaal getal, kleiner dan r, en groter dan 0.
- dit is in tegenspraak met de aanname zelf.

De aanname is onjuist, er is dus geen kleinste rationaal getal groter dan 0. QED

TU Delft

Bewijzen van een implicatie

Heel veel stellingen hebben de vorm "als p, dan q"

- als n een even geheel getal groter dan 2 is, dan is n de som van 2 priemgetallen (vermoeden van Goldbach).
- als $ax^2 + bx + c = 0$ en $a \neq 0$, dan is $x = \frac{-b \pm \sqrt{b^2-4ac}}{2a}$.
- als a^2 is even, dan is a even.
- als de som van de cijfers in een getal deelbaar is door 3, dan is het getal ook deelbaar door 3.
- als $a \mid b$ en $a \mid c$, dan geldt $a \mid (b + c)$.

Hoe bewijzen we zo'n implicatie?

Bewijsvorm voor een implicatie "als p, dan q"

1. Schrijf op: "Stel p," dus neem aan dat p waar is,
2. laat zien dat q logisch volgt.

Vaak zit de aanname al in de premissen. Vergelijk:

Stelling

(. . . premissen . . .) Stel p. Dan geldt q.

Bewijs.

Te bewijzen: q. ⟨ bewijs van q hier. ⟩ QED

met

Stelling

(. . . premissen . . .) Dan geldt: als p dan q.

Bewijs.

Stel dat p waar is. Te bewijzen: q. ⟨ bewijs van q hier. ⟩ QED

Bovendien. . .

Stelling

Stel p. Stel q. Dan geldt r.

is hetzelfde als

Stelling

Stel p. Dan geldt: als q dan r.

is hetzelfde als

Stelling

Stel q. Dan geldt: als p dan r.

TU Delft

Direct bewijs van een implicatie

Stelling

Als x^2 is even, dan is x even.

Bewijs.

- Stel: x^2 is even, te bewijzen: x is even
  - Stel: x is *niet* even (dus oneven)
  - Dus $x = 2k + 1$ (voor $k \in \{\ldots, -2, -1, 0, 1, 2, \ldots\}$)

$$\begin{aligned} x^2 &= (2k+1)^2 \\ &= \underbrace{\underbrace{4k^2 + 4k}_{\text{even}} + 1}_{\text{oneven}} \end{aligned}$$

  - dit is een tegenspraak!
  - de aanname is dus onjuist; x is even

QED

Oefenen

Stelling

Als de som van de cijfers in een getal deelbaar is door 3, dan is het getal ook deelbaar door 3.

Bewering

Als a^2 even is, dan geldt $4 \mid a^2$.

Analyze this:

- vul natuurlijke getallen $(0, 1, 2, \ldots)$ in voor x
- beschouw voor elke waarde van x de waarde van $y = 2^x - 1$
- is x een priemgetal, is y een priemgetal? wat valt je op?
- formuleer in 'als ..., dan ...' vorm. Kun je een bewijs vinden?

TurningPoint opdracht van gisteren

Een geldige redenering

premisse	Als het regent, dan wordt de straat nat.
premisse	De straat wordt niet nat.
conclusie	Het regent niet.

Stelling

Stel p. Stel q. Dan geldt r.

is hetzelfde als

Stelling

Stel p. Dan geldt: als q dan r.

Implicatie en Contrapositie

Ook geldig zijn dus:

premisse	Als het regent, dan wordt de straat nat.
conclusie	Als de straat niet nat wordt, regent het niet.

en

premisse	Als de straat niet nat wordt, regent het niet.
conclusie	Als het regent, dan wordt de straat nat.

Equivalenties

Equivalent zijn:

implicatie: Als p, dan q

contrapositie: Als niet q, dan niet p

Niet equivalent zijn:

implicatie: Als p, dan q

converse: Als q, dan p

TU Delft

Bewijzen van een implicatie

Contrapositie

Als je wil bewijzen "als p, dan q,"
mag je ook bewijzen "als niet q, dan niet p."

Afhankelijk van de stelling kan dat handiger zijn.

Bewijsvorm voor een implicatie "als p, dan q"

1. Zeg: "We bewijzen de contrapositie: als niet q, dan niet p. Stel dus 'niet q.'"
2. Laat zien dat 'niet p' logisch volgt.

TU Delft

Voorbeeldbewijs met contrapositie

Stelling

Als r irrationaal is, dan is $\sqrt{r}$ ook irrationaal.

Met andere woorden: als je r *niet* kunt schrijven als de ratio van twee gehele getallen, dan kan dat voor $\sqrt{r}$ ook niet ...

Bewijs.

We bewijzen de contrapositie: als $\sqrt{r}$ rationaal is, is r rationaal.
Stel dat $\sqrt{r}$ rationaal is, dus $\sqrt{r} = a/b$ (voor a, b gehele getallen).
Dan geldt dat $r = a^2/b^2$, dus r is rationaal. QED

TU Delft

Oefening

Bewijs de volgende stelling.

Stelling

Stel dat a, b en c reële getallen zijn, en dat $a > b$. Als $ac \leq bc$ dan is $c \leq 0$.

Bewijs.

We bewijzen de contrapositie: als $c > 0$, dan $ac > bc$.
Stel dus dat $c > 0$. Dan kunnen we beide kanten van de gegeven ongelijkheid $a > b$ met c vermeniguldigen (zonder dat de ongelijkheid omdraait), en krijgen we $ac > bc$. QED

TU Delft

Nog een oefening

Bewering

Stel dat x en y gehele getallen zijn, zodanig dat $x \cdot y$ even is. Dan is tenminste één van beide even.

Bewijs.

We bewijzen de contrapositie: Niet minstens 1 is even dus allebei oneven, dan is $x \cdot y$ niet even, dus oneven. Schrijf y en y als $2m+1$ en $2n+1$. Dan is
$x \cdot y = (2m+1)(2n+1) = 4nm+2m+2n+1 = 2(2nm+m+n)+1$.
De eerste term is even, dus het geheel (eerste term plus 1) is oneven. QED

TU Delft

Alternatieve Oefening: pariteit ("parity")

Definitie (even/oneven)

Een geheel getal x heet even (respectievelijk oneven) als er een ander geheel getal k bestaat zdd $x = 2k$ (respectievelijk $x = 2k+1$).

Definitie (pariteit)

Twee gehele getallen hebben dezelfde pariteit als ze beide even of beide oneven zijn.

Neem aan dat bewezen is dat elk geheel getal ofwel even ofwel oneven is (dit is te bewijzen met inductie).

Stelling

Als x en y gehele getallen zijn zdd $x+y$ even is, dan hebben x en y dezelfde pariteit.

lft

Oplossing

Stelling

Als x en y gehele getallen zijn zdd $x+y$ even is, dan hebben x en y dezelfde pariteit.

Bewijs.

We bewijzen de contrapositie: Als x en y niet dezelfde pariteit hebben, dan is $x+y$ oneven.
Neem dus aan dat x en y verschillende pariteit hebben, dus (wlog) x is even en y is oneven, dus $x = 2k$ en $y = 2m+1$. Te bewijzen is dat $x+y$ oneven is.
Nu is $x+y = 2k+2m+1 = 2(k+m)+1$ en omdat k en m gehele getallen zijn, is dit oneven. QED

TU Delft

De bi-implicatie

Heel veel stellingen hebben de vorm "p desda q"

- a^2 is even, dan en slechts dan als a even is.
- de som van de cijfers in een getal is deelbaar door 3, desda het getal ook deelbaar is door 3.
- een geheel getal a is niet deelbaar door 3, desda a^2-1 deelbaar is door 3
- het product ab van gehele getallen a en b is even, desda tenminste één van a en b even is

p desda q betekent:

p als q Dat is de implicatie "als q dan p"

p slechts dan als q Dus als niet q dan niet p, dus "als p dan q"

TU Delft

Hoe bewijzen we zo'n bi-implicatie?

Bewijsvorm voor een bi-implicatie "p desda q"

Bewijs.

$\Rightarrow$ Schrijf op: "Stel p," en laat zien dat q logisch volgt.

$\Leftarrow$ Schrijf op: "Stel q," en laat zien dat p logisch volgt.

QED

TU Delft

Voor alle x geldt ...

Als je wil bewijzen dat alle elementen in een groep een bepaalde eigenschap hebben, mag je een willekeurig element k kiezen en bewijzen dat k de eigenschap heeft.
Als dat lukt, mag je concluderen dat alle elementen in de groep de eigenschap hebben.

Rationale

k kan elk element in de groep zijn.

Pas Op

Je mag **geen** specifiek element nemen, geen extra aannamen over k maken.

TU Delft

Voorbeelden (hebben we al eerder gezien—vermomd)

Stelling

Voor alle oneven x geldt: x^2 is oneven.

Bewijs.

Neem een willekeurig oneven getal, zeg k.
k is oneven, dus $k = 2m + 1$ voor $m \in \mathbb{Z}$.

$$\begin{aligned} k^2 &= (2m+1)^2 \\ &= \underbrace{\underbrace{4m^2 + 4m}_{\text{even}} + 1}_{\text{oneven}} \end{aligned}$$

Omdat k willekeurig was gekozen, geldt dit voor *alle* oneven getallen. QED

lft

Bewijzen met gevalsonderscheid

Idee

Als in alle mogelijke gevallen van een uitputtende opsomming p kan worden afgeleid, dan is p bewezen.

Bijvoorbeeld:

- x is even of x is oneven
- $c < 0$ of $c > 0$ of $c = 0$
- y is een priemgetal of y is een samengesteld getal.
- `if (`$a < b$`) {<dingen> ...} else {<dingen> ...}`

De opsomming moet (impliciet) als premisse gegeven zijn, of afgeleid worden.

TU Delft

Euclides' bewijs
Er zijn oneindig veel priemgetallen (Elements, book IX, propositie 20)

$\vdots$

$x = p_1 \times p_2 \times \ldots \times p_n + 1$

er zijn 2 (uitputtende) mogelijkheden:

1. x is een priemgetal ... er mist een priemgetal (q)
2. x is samengesteld ... er mist een priemgetal (d)

dus: er mist een priemgetal

$\vdots$

(rest van het bewijs)

Samenvattend

De opsomming is uitputtend, in beide gevallen geldt de uitspraak "er mist een priemgetal," dus die uitspraak mag in het algemeen geconcludeerd worden.
Er bestaat geen 'geval' waar de uitspraak onwaar is, dus is hij waar.

Wat getallen ...

n	n^2	n^2 mod 4
-2	4	0
-1	1	1
0	0	0
1	1	1
2	4	0
3	9	1
4	16	0

Oefenen

Stelling

Voor alle getallen $n \in \mathbb{Z}$ geldt

$$n^2 \mod 4 = 0 \text{ of } 1.$$

Bewijs.

We onderscheiden de volgende 2 gevallen:

n is even: dan schrijven we n als $2m$ voor $m \in \mathbb{Z}$. Nu geldt $n^2 = (2m)^2 = 4m^2$, en $4m^2/4 = m^2$ met rest 0.

n is oneven: dan schrijven we n als $2m+1$ voor $m \in \mathbb{Z}$. Nu geldt $n^2 = (2m+1)^2 = 4m^2 + 4m + 1 = 4(m^2+m)+1$ en $(4(m^2+m)+1)/4$ geeft rest 1.

In beide gevallen hebben we rest 0 of 1. QED

Nog wat getallen ...

n	$n^3 - n$	$(n^3 - n)$ mod 3
-2	-6	0
-1	0	0
0	0	0
1	0	0
2	6	0
3	24	0
4	60	0

Oefenen

Stelling

Voor alle getallen $n \in \mathbb{Z}$ geldt $3 \mid (n^3 - n)$.

Bewijs.

We schrijven $n^3 - n$ als $n(n^2 - 1)$.
We onderscheiden de volgende 3 gevallen ($k \in \mathbb{Z}$):

$n = 3k$: Nu is $n(n^2 - 1) = 3k((3k)^2 - 1)$, deelbaar door 3.

$n = 3k + 1$: Nu is $n(n^2-1) = (3k+1)((3k+1)^2-1) = 3(9k^3+9k^2+2k)$, deelbaar door 3.

$n = 3k + 2$: Nu is $n(n^2 - 1) = (3k + 2)((3k + 2)^2 - 1) = 3(9k^3 + 18k^2 + 11k + 6)$, deelbaar door 3.

In alle gevallen geldt $3 \mid (n^3 - n)$. QED

N.B.: gevalsonderscheid even/oneven werkt hier niet!

Interessant voorbeeld

Stelling

Er bestaan irrationale getallen p en q, zodanig dat p^q rationaal is.

Bewijs.

We nemen $q = \sqrt{2}$. Zij $v = \sqrt{2}^{\sqrt{2}}$. Er zijn nu 2 mogelijkheden:

1. v is rationaal. Zij $p = \sqrt{2}$, zodat $v = p^q$ rationaal is.
2. v is irrationaal. Zij $p = v$,
   zodat $p^q = \left(\sqrt{2}^{\sqrt{2}}\right)^{\sqrt{2}} = \sqrt{2}^2 = 2$.

In beide gevallen zijn er irrationale p en q, en rationale p^q. QED

Samenvattend

De opsomming is uitputtend, en in beide gevallen worden p en q geïdentificeerd die aan de voorwaarden voldoen.