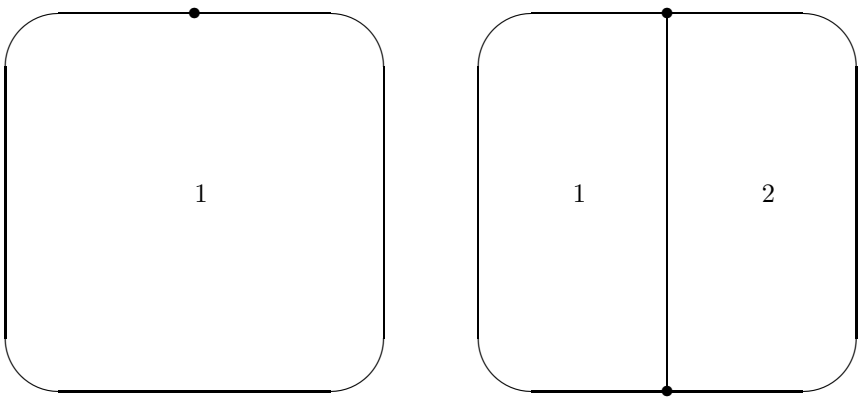
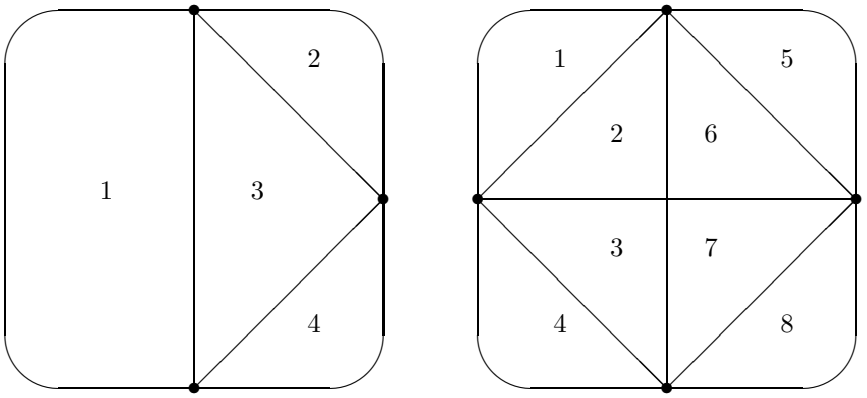
Hoofdstuk 1

Waarom iets bewijzen?

Teken eens een cirkel of aardappel of iets wat daar op lijkt met een punt op de rand. De cirkel bestaat nu uit een stuk. Teken nu een tweede punt op de rand, en verbind die met het eerste punt. Nu bestaat de cirkel uit twee stukken, zie onderstaand plaatje.



Teken nu een derde punt op de rand van de cirkel, en verbind die met de eerder gekozen punten. Nu bestaat de cirkel uit vier stukken. Teken nu een vierde punt op de cirkel, en verbind die met de eerder gekozen punten. Nu is de cirkel opgedeeld in acht stukken. Zie de plaatjes hieronder.



We doen het nog een keer: we kiezen een vijfde punt en verbinden dat met de eerdere vier punten. Als we goed tellen zien we dat nu de cirkel in zestien stukken is opgedeeld. Het zal duidelijk zijn wat het patroon hierin is: we beginnen met een stuk, en elke keer als er een punt bij komt krijgen we twee keer zo veel stukken. Bij een punt hebben we zo $1 = 2^0$ stukken, bij twee punten $2 = 2^1$, bij drie $4 = 2^2$, bij vier $8 = 2^3$ en bij vijf $16 = 2^4$. We concluderen:

> Als je n punten op een cirkel met elkaar verbindt, verdeel je daarmee de cirkel in 2^{n-1} stukken.

Dit lijkt allemaal best aannemelijk, en je bent niet zo gauw geneigd om dit nog uit te proberen voor zes of meer punten, want daarvoor moet je toch wel heel veel tekenen en tellen. Toch is het de moeite waard om dat wel eens te doen: bij zes punten lukt het je namelijk helemaal niet om 32 stukken te krijgen, en blijf je bij 31 steken, ook als je er voor zorgt dat er nergens drie verbindingslijnen door een punt gaan. We zijn er dus met zijn allen ingeluisd, en de hele bewering is niet waar, althans niet voor zes of meer punten.

Wat is nu de moraal van dit verhaal? Dat is dit: als je echt zeker wilt weten dat een bewering waar is, kun je niet vertrouwen op een paar voorbeelden en een aannemelijk verhaal dat een patroon in die voorbeelden verklaart, en dat daarom dat patroon altijd wel zal gelden. In de praktijk, zeker in die van de informatica of van die van medische apparatuur, zijn er heel veel situaties waarin je geen genoegen kunt nemen met een paar testgevallen en een aannemelijk verhaal dat het wel goed zit. Durf je te vliegen in een vliegtuig waarvan je zelf de besturingssoftware hebt geschreven, en best wel voor een redelijk aantal gevallen hebt uitgetest? Er zijn mensen om het leven gekomen door een veel te hoge straling, veroorzaakt door een foutje in de software van bestralingsapparatuur. Dit zijn toch dingen die je graag zou willen voorkomen. Nu kun je niet verwachten dat dat voor heel gecompliceerde dingen altijd zal lukken, maar een stap in die richting kan al heel waardevol zijn. En voor veel beweringen van een eenvoudiger type dan dat je correctheid eist van een ingewikkeld stuk software lukt dat prima. Wat wil je dan wel hebben? Een sluitende redenering dat een bepaalde bewering geldig is. Die redenering kun je dan voor je zelf gebruiken, om je zelf ervan te overtuigen dat je bewering klopt. Maar je kunt diezelfde redenering ook gebruiken om iemand anders te overtuigen. Of misschien jezelf weer, over een hele tijd als je de redenering weer vergeten mocht zijn. Daarvoor is het wel nodig

dat je de redenering opschrijft, en wel zodanig dat iemand anders aan de hand van wat je hebt opgeschreven de hele redenering ook kan volgen. En liefst ook omgekeerd: alles wat je hebt opgeschreven speelt een essentiële rol in de redenering. Zo'n redenering noemen we een *bewijs*. De onderdelen van zo'n bewijs hebben een heel preciese betekenis. Een redenering met een heel preciese betekenis kun je alleen maar geven als alles wat je daarin zegt, inclusief de hele bewering waar het om gaat, heel precies *beschreven is*. En daarmee zijn de voornaamste ingrediënten van dit vak *Beschrijven en Bewijzen* genoemd. Vaak maak je hierbij dankbaar gebruik van manieren om je beweringen heel kort in een soort formuletaal op te schrijven, waarbij je een bijbehorend stel spelregels hebt. In dit dictaat zullen uitgebreid dergelijke notaties en begrippen aan de orde komen, over proposities en predicaten en uit de wiskunde. Voordat we dat gaan doen lopen we eerst een aantal bewijsprincipes langs met bijbehorende voorbeelden, om een beetje een gevoel voor wat bewijsprincipes te ontwikkelen voor we ons in ingewikkelde notaties gaan storten.

1.1 Bewijzen uit het ongerijmde

Bewering:

> Een postbode levert 130 poststukken af in een straat met 43 adressen. Dan is er in die straat minstens één adres waarop vier of meer poststukken zijn afgeleverd.

Hoe kun je het makkelijkst inzien dat deze bewering inderdaad klopt? Stel eens dat de geconcludeerde bewering *er is minstens een adres waarop vier of meer stukken zijn afgeleverd* niet waar is. Dan zijn er op elk adres dus hoogstens drie stukken afgeleverd. Met 43 adressen totaal betekent dat dat er in totaal hoogstens $3 \times 43 = 129$ stukken zijn afgeleverd. En dat is in tegenspraak met het gegeven dat er in totaal 130 stukken zijn bezorgd. Dus is de geconcludeerde bewering *er is minstens een adres waarop vier of meer stukken zijn afgeleverd* wel waar, en hebben we de bewering bewezen.

Het patroon in deze redenering komt heel vaak voor. Steeds is er een bewering waarvan je wilt bewijzen dat die waar is. De redenering ziet er dan als volgt uit:

> Stel de bewering is niet waar. Vanuit deze aanname trek je, eventueel samen met aannamen die deel uitmaken van de gegevens in de bewering, allerlei conclusies, tot je op een bewering uitkomt die niet waar is, of in tegenspraak is met gegevens in de bewering. Daaruit concludeer je dat de aanname *de bewering is niet waar*, niet kan kloppen, en is daarmee de bewering zelf wel waar.

Een redenering van deze vorm wordt wel een *bewijs uit het ongerijmde* genoemd, in het Engels: *proof by contradiction*. In dit speciale voorbeeld wordt een telargument gegeven, dat ook wel het *pigeon hole principle* (*duiventilprincipe*) wordt genoemd; we komen daar later nog op terug (Stelling 6.5).

Als je van een bewering waarvan je denkt dat die waar is, probeert te bewijzen dat die inderdaad waar is, is het een goed idee om eens op een rijtje te zetten wat er allemaal gebeurt als die bewering niet waar is. Als het lukt om daar iets onzinnigs uit te concluderen, is de hele redenering om te vormen tot een bewijs uit het ongerijmde. Een waarschuwing is hier echter wel op zijn plaats: elke bewering die te bewijzen is, is op deze manier als volgt

te bewijzen met een bewijs uit het ongerijmde. Stel de bewering is niet waar, geef een bewijs van de bewering, dit is in tegenspraak met de aanname dat de bewering niet waar is, en dus is de bewering waar. Wat betreft de geldigheid is hier niets tegenin te brengen, maar deze redenering bevat wel een hoop overbodige ballast: het bewijs van de bewering zelf is natuurlijk een stuk korter dan datzelfde bewijs met nog een hoop geredeneer er om heen. Uit het oogpunt van efficientie is een kort bewijs altijd te prefereren boven een langer bewijs. Tegen de tijd dat je een bewijs uit het ongerijmde hebt gevonden, is het dan ook altijd een goed principe om te kijken of je de redenering uit het ongerijmde wel echt nodig hebt, en niet in feite dezelfde redenering korter rechtstreeks kunt geven.

Nauw verwant aan een bewijs uit het ongerijmde is een bewijs met *contrapositie*. Dat betekent dat je als een bewering van de vorm

> Als P geldt, dan geldt ook Q

wilt bewijzen, in plaats hiervan ook mag bewijzen

> Als Q niet geldt, dan geldt ook niet P.

Merk op dat we twee keer het woord 'niet' hebben toegevoegd, en P en Q hebben omgewisseld. We laten nu zien met een bewijs uit het ongerijmde dat dit nieuwe bewijsprincipe inderdaad klopt. We willen de bewering *Als P geldt, dan geldt ook Q* bewijzen, en stellen dat dit niet waar is. Dat kan alleen maar als er een situatie bestaat waarin P wel waar is, maar Q niet; we komen hier later uitgebreid op terug. We hadden aangenomen dat we konden bewijzen *Als Q niet geldt, dan geldt ook niet P*. Omdat in de betreffende situatie Q niet geldt, kunnen we dus concluderen dat dan ook P niet geldt. Maar dit is in tegenspraak met de eerdere aanname dat in die situatie P juist wel geldt.

Zoals gezegd is het een goed principe om van een bewering die je zou willen bewijzen, te gaan uitpluizen wat er allemaal gebeurt als die bewering niet waar is. Als het lukt om daar een tegenspraak uit af te leiden, is daarmee de bewering bewezen met een bewijs uit het ongerijmde. Als het echter niet lukt een tegenspraak te vinden, kun je juist gaan zoeken naar een voorbeeld waarvoor de bewering niet waar is. Als je zo'n voorbeeld hebt gevonden, heet dat een *tegenvoorbeeld*, (Engels: *counterexample*) waarmee dan juist bewezen is dat de bewering niet waar is.

Opgave 1.1

Geef van elk van de volgende beweringen een bewijs of een tegenvoorbeeld:

- in elke groep van 50 mensen zijn er zes of meer die allemaal in dezelfde maand jarig zijn;
- in elke groep van 50 mensen zijn er vijf of meer die allemaal in dezelfde maand jarig zijn;
- in elke groep van 50 mensen zijn er vier of meer die allemaal in dezelfde maand jarig zijn.

1.2 Bewijzen met gevalsonderscheid

Als je de getallen van 1 tot en met 100 bij elkaar optelt, wat komt er dan uit? Als je gaat rekenen: $1+2=3$, $3+3=6$, $6+4=10$, $10+5=15$, enzovoorts, dan ben je nog al even bezig. Het kan ook handiger:

$$1+100=101,\ 2+99=101,\ 3+98=101,\ldots,\ 50+51=101.$$

Nu hebben we de 100 getallen in 50 groepjes van twee opgesplitst, waarbij voor elk groepje van twee de som 101 is. Het totaal is dus $50\times 101=5050$.

Laten we het algemener bekijken (overigens ook een algemeen principe: probeer eerst een speciaal geval en als je daar iets voor verzonnen hebt, probeer dat dan algemener te maken). Als k en n gehele getallen zijn met $k<n$, en ik tel alle $n-k+1$ getallen van k tot en met n bij elkaar op, wat komt daar dan uit? Met hetzelfde truukje van zonet tellen we de eerste bij de laatste op, de op een na eerste bij de op een na laatste, en zo verder:

$$k+n=k+n,\ (k+1)+(n-1)=k+n,\ (k+2)+(n-2)=k+n,\ldots.$$

Hoe eindigt dit? We zien dat het uitmaakt of het aantal $n-k+1$ even is of niet. Als dit aantal even is, krijgen we precies $\frac{n-k+1}{2}$ groepjes van twee waarvan de som steeds $k+n$ is. De som van de hele rij getallen is dus $(k+n)\times\frac{n-k+1}{2}=\frac{(k+n)(n-k+1)}{2}$.

Als het aantal oneven is, krijgen we $\frac{n-k}{2}$ groepjes van twee waarvan de som steeds $k+n$ is, en houden we het middelste van de rij getallen over. Dat middelste getal is het gemiddelde van de eerste en de laatste, dus $\frac{k+n}{2}$. De som van al deze getallen is dus

$$(k+n)\times\frac{n-k}{2}+\frac{k+n}{2}=\frac{(k+n)(n-k)+(k+n)}{2}=\frac{(k+n)(n-k+1)}{2}.$$

We zien dus dat ook in dit geval de som van de hele rij $\frac{(k+n)(n-k+1)}{2}$ is, en concluderen dat het in alle gevallen zo is. We hebben dus bewezen:

> Als k en n gehele getallen zijn met $k<n$, dan is de som van alle getallen van k tot en met n gelijk aan $\frac{(k+n)(n-k+1)}{2}$.

In het bewijs van deze bewering hebben we een *gevalsonderscheid* (Engels: *case analysis*) gemaakt: voor het geval dat het aantal even was hebben we een bewijs gegeven, en voor het geval dat het aantal oneven was hebben we een ander bewijs gegeven. Aangezien elk geheel getal even of oneven is, hebben we hiermee voor alle gevallen een bewijs gegeven.

Net zoals bij bewijzen uit het ongerijmde is het bij bewijzen met gevalsonderscheid een goed principe om te kijken of je het gevalsonderscheid wel echt nodig hebt. Als je het namelijk niet nodig hebt, kun je waarschijnlijk een korter bewijs geven. In dit voorbeeld is dat inderdaad mogelijk als we met het maken van groepjes van twee niet stoppen als we op de helft zijn, maar nog even doorgaan:

$$k+n=k+n,\ (k+1)+(n-1)=k+n,\ (k+2)+(n-2)=k+n,\ldots$$

$$\ldots,(n-1)+(k+1)=k+n,\ n+k=k+n.$$

Nu hebben we evenveel groepjes van twee gemaakt als het aantal getallen wat we bij elkaar op wilden tellen, namelijk $n-k+1$. Elk van deze groepjes heeft $k+n$ als som, al deze

groepjes hebben dus samen $(k+n)(n-k+1)$ als som. In deze groepjes komen elk van de getallen precies twee keer voor: een keer als linkerlid van een groepje en een keer als rechterlid. Daarmee is tweemaal de gevraagde som dus gelijk aan $(k+n)(n-k+1)$, en concluderen we zonder gevalsonderscheid te maken dat de gevraagde som altijd gelijk is aan $\frac{(k+n)(n-k+1)}{2}$.

In het eerste bewijs hebben we een opsplitsing in twee gevallen gemaakt: het aantal is even of het aantal is oneven. Het is ook mogelijk een probleem in meer dan twee gevallen op te splitsen. Van belang is altijd dat alle situaties die aan de voorwaarden van de bewering voldoen, onder tenminste een van de aangegeven gevallen vallen: de opsplitsing moet *uitputtend* zijn, in het Engels: *exhaustive*. Dat sommige situaties onder meer dan een van de gevallen vallen is niet erg. Dit illustreren we met het volgende voorbeeld:

Voor elk reëel getal x geldt dat $x \times x \geq 0$.

We bewijzen dit als volgt: we maken het gevalsonderscheid $x \geq 0$ of $x \leq 0$. Dit onderscheid is inderdaad uitputtend: voor elk reëel getal x geldt een van beide voorwaarden.

Als $x \geq 0$ dan is $x \times x$ het product van twee getallen die elk tenminste 0 zijn; het product is dan ook tenminste 0.

Als $x \leq 0$ dan is $-x \geq 0$, en is $x \times x = (-x) \times (-x)$ het product van twee getallen die elk tenminste 0 zijn; het product is dan ook tenminste 0.

Voor beide gevallen hebben we nu een bewijs gegeven, en daarmee is het bewijs voltooid. Merk op dat het geval dat $x = 0$ onder beide gevallen valt. In feite hebben we de bewering voor dit geval dus twee keer bewezen.

Het is een goed gebruik bij gevalsonderscheid te beginnen bij de makkelijkste gevallen en het moeilijkste voor het laatst te bewaren.

Opgave 1.2

Wat komt er uit als je alle even getallen van 2 tot en met 100 bij elkaar optelt? En wat komt er uit als je alle oneven getallen van 17 tot en met 47 bij elkaar optelt? Geef een formule die voor elke n aangeeft wat de som is van alle even getallen van 2 tot en met $2n$.

Opgave 1.3

Bewijs dat het kwadraat van een oneven getal altijd te schrijven is als $8n + 1$ voor een geheel getal n.

1.3 Bewijzen met inductie

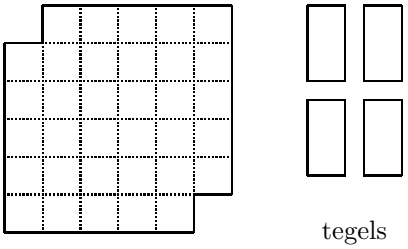
Voor beweringen die afhangen van een natuurlijk getal n is het vaak handig in het bewijs gebruik te maken van het gegeven dat de bewering voor kleinere waarden dan n al waar is. Dat je daarmee toch een correct bewijs mee kunt leveren zegt het *principe van volledige inductie*. In hoofdstuk 7 zal dit uitgebreid aan de orde komen.

1.4 Bewijzen met invarianten

Alvorens het principe uit te leggen beginnen we met een aantal puzzels.

De keukenvloer

We hebben een vierkante keukenvloer met een zijde van n decimeter. In de rechter onderhoek en in de linker bovenhoek mist een vierkante decimeter (voor een verwarmingsbuis). Voor welke n kan de keukenvloer met tegels van 2×1 decimeter betegeld worden? Bijvoorbeeld voor $n = 6$ is de situatie als volgt:



vloer tegels

De koffiekan

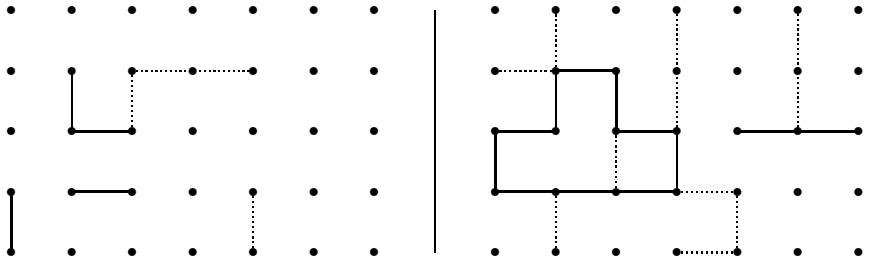
In een koffiekan zitten 25 zwarte en 25 witte bonen. De volgende handeling wordt uitgevoerd zolang dat mogelijk is: *haal twee bonen uit de kan; als ze dezelfde kleur hebben, stop dan een zwarte boon in de kan; als ze verschillend van kleur zijn, stop dan de witte terug in de kan.* Er is een voldoende voorraad extra zwarte bonen. Vraag: wat is de kleur van de laatste boon in de kan?

Het lijnen-spel

Het speelbord bestaat uit een rechthoek met punten. Twee spelers, A en B, doen om beurten een zet; A begint. Speler A doet een zet door twee aangrenzende punten met een horizontale of een verticale lijn te verbinden, speler B doet hetzelfde, maar dan met stippellijnen. Spelers mogen reeds verbonden punten niet nog eens verbinden. Na vier zetten van beide spelers kan het bord er bijvoorbeeld uitzien als links in onderstaand plaatje.

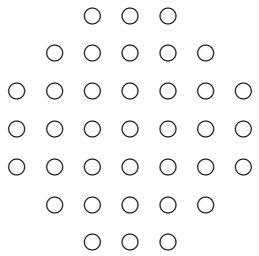
Speler A wint als hij een gesloten figuur kan maken, zoals in het rechter plaatje; speler B heeft een andere opdracht: B wint als ze A kan verhinderen een gesloten figuur te maken.

Vraag: is er voor één van beide spelers een winnende strategie? Zo ja, welke?



Solitaire

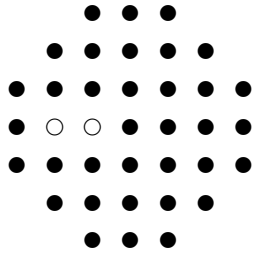
We beschouwen het spelletje *solitaire*, dat — de naam zegt het al — je in je eentje kunt spelen. We kijken hier naar de Franse versie van het spel, dat gespeeld wordt op een bord bestaande uit 37 velden dat er als volgt uitziet:



In de beginsituatie is het middelste veld leeg en staat er op elk ander veld een pionnetje, dus 36 in totaal. Nu mag er geslagen worden: horizontaal en verticaal mag een pionnetje over een een buurpionnetje heenspringen naar het daarachter gelegen lege veld, waarbij het pionnetje waar over heen gesprongen is weggenomen wordt. Laten we pionnetjes met een zwart rondje aangeven en onbezette velden met een open rondje; als dan de volgende situatie op het bord voorkomt

dan kan het linker pionnetje over zijn rechterbuurman heenspringen en is het resultaat:

Na één zet kan het bord er dus als volgt uit zien:



De bedoeling van het spel is nu om net zo lang volgens deze spelregel te spelen totdat er nog maar slechts één pionnetje over is, dat dan liefst ook nog in het midden moet staan. In

het begin is het niet zo moeilijk om te zetten, maar na een tijdje spelen staan er ineens een stuk of wat pionnetjes verspreid over het bord waarvan er geen twee naast elkaar staan, en kan er dus niet meer gezet worden. De vraag is nu: is het mogelijk om te eindigen in een situatie waarbij er nog maar één pionnetje over is?

De oplossingen

Deze vier puzzels zijn allemaal gebaseerd op herhaling: herhaald tegels leggen, herhaald bonen trekken, herhaald regels toepassen en herhaald zetten doen. Ze kunnen opgelost worden door steeds een geschikte *invariant* te beschouwen: een eigenschap die steeds blijft gelden. We geven eerst de definitie.

Definitie 1.1 Een invariant is een eigenschap van een proces of een programma, die voldoet aan het volgende:

- aan het begin geldt de invariant, en
- als de invariant geldt en er wordt vervolgens een stap gedaan, dan geldt na afloop van die stap de invariant weer.

Als we zo'n eigenschap hebben, blijft die dus altijd gelden, hoeveel stappen er ook worden uitgevoerd. Als na eindig veel stappen het proces of programma voltooid is, geldt de invariant na afloop dus nog steeds. Deze observatie is cruciaal voor de oplossingen van elk van de puzzels, en is een belangrijk bewijsprincipe in de informatica.

Hier volgen de oplossingen:

De keukenvloer

We maken een gevalsonderscheid. Als n oneven is dan is n^2 oneven, en $n^2 - 2$ dus ook. Een vloer van een oneven aantal dm^2 is nooit te betegelen met tegels die elk 2 dm^2 groot zijn.

Als n even is dan kleuren we de vloer in gedachten als een schaakbord: om en om wit en zwart, met de rechter onderhoek wit. De twee verwarmingsbuizen staan in een wit veld. Er moeten dus twee zwarte velden méér betegeld worden dan witte velden. Omdat elke tegel één zwart en één wit veld bedekt, zullen we, hoe we ook tegelen, altijd twee zwarte velden overhouden. Een betegeling is dus niet mogelijk.

We hebben gebruik gemaakt van de invariant

$$\textit{aantal onbetegelde zwarte velden} = \textit{aantal onbetegelde witte velden} + 2$$

Deze uitspraak is in het begin waar, en blijft invariant bij het leggen van een tegel. De uitspraak geldt dus voor alle gedeeltelijke betegelingen, en er is geen betegeling waarin geen onbetegelde zwarte velden over zijn.

De koffie-kan

Allereerst merken we op dat bij elke trekking er twee bonen verwijderd worden, en één teruggelegd. Na 49 trekkingen zal er dus nog één boon over zijn.

Het ondoenlijk alle mogelijkheden te proberen, dat zijn er heel erg veel. In plaats daarvan zoeken we naar een geschikte invariant. We kijken naar het netto effect op het aantal witte en zwarte bonen bij elk van de vier mogelijke trekkingen:

trekking	actie	Z	W
$-ZZ$	$+Z$	-1	0
$-WW$	$+Z$	$+1$	-2
$-ZW$	$+W$	-1	0
$-WZ$	$+W$	-1	0

Het aantal witte bonen in de kan blijft gelijk of neemt met twee af. Het oneven-zijn van het aantal witte bonen is dus een invariant in dit spel!

Het aantal witte bonen blijft dus altijd oneven, in het bijzonder aan het eind. De laatste boon is dus altijd wit.

Opgave 1.4

In een doos zitten 100 rode, 100 witte en 100 blauwe ballen. Zolang dat mogelijk is, worden er drie ballen uit de doos gepakt. Als alle drie de ballen dezelfde kleur hebben, wordt er één van die drie teruggelegd. Als alle drie de ballen een verschillende kleur hebben, wordt een rode bal teruggelegd. Als er twee ballen dezelfde kleur hebben, wordt de afwijkende derde teruggelegd en bovendien een blauwe. Is het mogelijk te eindigen met een rode en een blauwe bal?

Het lijnen-spel

Op een bord van 2×2 punten kan A niet winnen: er zijn minstens 4 lijnen nodig om een gesloten figuur te maken. Laten we daarom eerst kijken of er een winnende strategie voor B is. Het spel vaak spelen geeft weinig inzicht in een strategie. Daarom kijken we naar de eigenschappen van gesloten figuren. Als B kan verhinderen dat één van deze eigenschappen op het bord komt, kan ze winnen. De invariant luidt dan: het bord bevat geen figuur met de betreffende eigenschap.

Welke eigenschappen heeft een gesloten figuur? Er zitten parallelle lijnen in, maar die kan B niet verhinderen. Er zit een even aantal parallelle lijnen in, maar ook dat kan B niet verhinderen. Er zitten tenminste vier hoeken in, maar B kan niet verhinderen dat A hoeken tekent. Er zit minstens één L-vormige hoek in met de punt links onder, en díe kan B verhinderen! Elke keer als A een horizontale of verticale lijn trekt, kan B deze aanvullen tot een L-vorm (tenzij A op de boven- of rechterrand zet; dan mag B een willekeurige zet doen). A kan dan nooit zelf een L-vorm in zijn figuur maken, en dus geen gesloten figuur. Op grond van de invariant: '*het bord bevat geen* L*-vormen van* A' kunnen we concluderen: B heeft een winnende strategie.

Solitaire

We maken een indeling van de 37 velden in A-velden, B-velden en C-velden, en wel als volgt:

```
      A B C
    A B C A B
  A B C A B C A
  B C A B C A B
  C A B C A B C
    B C A B C
      A B C
```

Verder definiëren we:

- a is het aantal A-velden waarop een pionnetje staat,
- b is het aantal B-velden waarop een pionnetje staat,
- c is het aantal C-velden waarop een pionnetje staat.

Opgave 1.5

Bewijs dat het solitaire spel niet kan eindigen in een situatie waarin er nog slechts één pion op het bord staat.

(Aanwijzing: gebruik de invariant:

a, b en c zijn alle drie even of ze zijn alle drie oneven.)

Bij puzzels zoals deze worden invarianten vaak gebruikt om aan te tonen dat bepaalde oplossingen niet mogelijk zijn. Gelukkig spelen ze in de informatica meestal een wat positievere rol, namelijk om aan te tonen dat na afloop van het uitvoeren van een programma een bepaalde gewenste eigenschap wèl geldt. Een aardig voorbeeld hiervoor is het volgende programma waarmee je handig twee getallen kunt vermenigvuldigen:

z := 0;
a := A;
b := B;
zolang $a \neq 0$ doe dan:
als a oneven is dan: $a := a - 1$;
$z := z + b$
als a even is dan: $a := a/2$;
$b := 2b$

Hierin zijn A en B de getallen die je wilt vermenigvuldigen; aangenomen wordt dat $A \geq 0$. In de variabele z komt het antwoord te staan, en a en b zijn hulpvariabelen. De notatie $x := \cdots$ betekent dat de variabele x de waarde $\cdots$ krijgt. Dat na afloop de waarde van z inderdaad $A \times B$ is, volgt uit het feit dat

$$z + a \times b \;=\; A \times B$$

een invariant is van het "zolang"-stuk van het programma. Voordat aan de uitvoering van dat stuk van het programma begonnen wordt heeft z de waarde 0 en geldt $a = A$ en $b = B$. Dan geldt inderdaad $z + a \times b = 0 + A \times B = A \times B$.

Als de invariant geldt en a is oneven, dan wordt een stap gedaan waarbij a wordt vervangen door $a - 1$ en z wordt vervangen door $z + b$. Vanwege $(z + b) + (a - 1) \times b = z + a \times b = A \times B$ geldt na afloop van die stap dus weer de invariant.

Als de invariant geldt en a is even, dan wordt een stap gedaan waarbij a wordt vervangen door $a/2$ en b wordt vervangen door $2b$. Vanwege $z + (a/2) \times 2b = z + a \times b = A \times B$ geldt na afloop van die stap dus weer de invariant.

We concluderen dat na afloop[1] de invariant nog steeds geldt. In dat geval is $a = 0$, want zolang $a \neq 0$ stop het programma nog niet. Vanwege de invariant hebben we dan

$$z \;=\; z + 0 \times b \;=\; z + a \times b \;=\; A \times B$$

waarmee we bewezen hebben dat z inderdaad de waarde van het gevraagde product heeft.

Opgave 1.6

Bereken 13×17 met bovenstaande methode.

Opgave 1.7

Met de volgende regels kun je van rijtjes symbolen andere rijtjes symbolen maken:

1. achter een rijtje met een I aan het eind mag je een U zetten;
2. van het rijtje Mx mag je Mxx maken, voor elk rijtje symbolen x;
3. als er III in een rijtje staat, mag je dat vervangen door U;
4. als er UU in een rijtje staat, mag je dat weglaten.

Als voorbeeld bekijken we een aantal rijtjes die je uit MI kunt produceren:

a.	MI	gegeven
b.	MII	uit a volgens regel 2
c.	MIIII	uit b volgens regel 2
d.	MIIIIU	uit c volgens regel 1
e.	MUIU	uit d volgens regel 3
f.	MUIUUIU	uit e volgens regel 2
g.	MUIIU	uit f volgens regel 4

Vraag: is het mogelijk om beginnend met het rijtje MI uit te komen op het rijtje MU? Zo ja, hoe? Zo nee, waarom niet?

(Aanwijzing: laat zien dat in geen enkel opgebouwd rijtje het aantal I's een drievoud is.)

[1] Het is inderdaad in te zien dat dit programma niet oneindig lang doorgaat, en zelfs vrij snel tot zijn einde komt

1.5 Nog wat terminologie

Een belangrijke bewering waarvoor een bewijs bestaat, wordt vaak een *stelling* genoemd; in het Engels *theorem*. Een iets minder belangrijke bewering waarvoor een bewijs bestaat, wordt wel een *propositie* genoemd; in het Engels *proposition*. Een bewering met een bewijs waarvan het belang niet op zich zelf staat, maar voornamelijk dient als hulpresultaat om een stelling te bewijzen, heet een *lemma*. Een gevolg van een stelling wordt wel *corollarium* genoemd; in het Engels *corollary*. Het precies vastleggen van de betekenis van een nieuw begrip heet een *definitie*. Een fundamentele bewering die je niet bewijst maar als uitgangspunt hanteert heet een *axioma*.

Bij een bewijs is het handig om te zien waar het begin en eindigt. Meestal begint het met het woord *bewijs* (in het Engels *proof*), en eindigt het met een blokje □. In sommige teksten wordt een bewijs wel afgesloten met de afkorting Q. E. D.. Dit staat voor *quod erat demonstrandum*, hetgeen Latijn is voor "hetgeen bewezen moest worden". In dit dictaat zullen we een bewijs vaak afsluiten met de woorden *einde bewijs*.

Een bewering waarvan je verwacht dat die waar is, maar waarvoor geen bewijs gevonden is, heet een *vermoeden*; in het Engels *conjecture*. Het is verbazend dat er veel eenvoudig te formuleren beweringen bestaan waarvan de juistheid wel vermoed wordt, er is dan ook nooit een tegenvoorbeeld voor gevonden, maar waarvoor ook na uitgebreide inspanning van zeer knappe mensen nog nooit een bewijs is gevonden. Enkele voorbeelden van dergelijke vermoedens zijn:

- Elk even getal groter dan 2 is de som van twee priemgetallen.
- Er bestaan oneindig veel priemgetallen p waarvoor $p + 2$ ook een priemgetal is.
- Begin met een willekeurig positief geheel getal. Herhaal steeds het volgende proces: als het even is deel je het door twee, en als het oneven is vermenigvuldig je het met drie en telt er daarna 1 bij op. Vermoeden: dit proces komt altijd terecht in $\cdots \to 1 \to 4 \to 2 \to 1 \to \cdots$.

Het komt ook wel voor dat dergelijke vermoedens toch nog bewezen worden. Een frappant voorbeeld hiervoor is de *laatste stelling van Fermat*, rond 1637 door Fermat geformuleerd: er bestaan geen gehele getallen $n > 2$ en $a, b, c > 0$ waarvoor $a^n + b^n = c^n$. Hoewel Fermat zelf beweerde hiervoor een wonderbaarlijk bewijs te hebben gevonden dat helaas te groot was om in de kantlijn op te nemen, is dat 'bewijs' niet bewaard gebleven en is deze bewering honderden jaren een vermoeden geweest. Tot 1993: toen gaf Andrew Wiles hiervan een bewijs, dat compact opgeschreven enige honderden pagina's besloeg, exclusief de bewijzen van de vele gebruikte veelal zeer diepe al eerder bekende stellingen.