Hans van Ditmarsch
Fil., Logica, Universidad de Sevilla
Calle Camilo Jose Cela s/n
41018 Sevilla Spanje
Computer Science, University of Otago
Dunedin 9015 Nieuw-Zeeland
hans@cs.otago.ac.nz

Jan van Eijck
Centrum voor Wiskunde en Informatica
PO Box 94079
1090 GB Amsterdam
jve@cwi.nl

Rineke Verbrugge
Kunstmatige Intelligentie
Rijksuniversiteit Groningen
Postbus 407
9700 AK Groningen
rineke@ai.rug.nl

Geschiedenis

Publieke werken: Freudenthal's som-en-productraadsel

In 1969 poneerde Hans Freudenthal in Nieuw Archief het som-en-productprobleem [4–5]. Dit probleem heeft daarna de academische gemoederen nogal beroerd. In 2002 kwam het in NAW nogmaals over tafel, in het kader van een ander raadsel, het zeven-kaartenprobleem [14]. In 2005 werd in NAW een lezersoproep geplaatst om de herkomst en de verspreiding van het raadsel te achterhalen. In deze bijdrage berichten de auteurs over de resultaten van deze oproep en plaatsen de analyse van het raadsel in de actualiteit van kennislogica en model checking.

In het laatste NAW-nummer van 1969 [4] poneerde Hans Freudenthal het probleem, zoals afgebeeld in figuur 1. En in het daaropvolgende nummer, in 1970, werden de oplossingen, en de oplossers, besproken.

Dit som-en-productprobleem kan een 'raadsel' genoemd worden, omdat de bekendmakingen ('uitspraken') die door S (voor 'som') en P (voor 'product') gedaan worden op het eerste gezicht niet informatief lijken – ze spreken immers alleen hun onwetendheid uit en zeggen niets over feitelijke getallenparen! De bekendmakingen zijn echter *zo* informatief, dat S en P getallenparen kunnen elimineren.

Bijvoorbeeld, de getallen kunnen niet 2 en 3 zijn, of een ander priemgetallenpaar, omdat in al die gevallen P meteen de getallen uit hun product zou kunnen afleiden. Dan had hij dus niet de eerste bekendmaking 'ik weet het niet' kunnen doen. Iets lastiger is in te zien dat de getallen ook niet, bijvoorbeeld, 14 en 16 kunnen zijn. Als dat zo was, dan was hun som 30. Dit is tevens de som van de priemgetallen 7 en 23. Als het product $7 \cdot 23$ was, dan zou P net als in het voorgaande geval geweten hebben wat de getallen waren. Met andere woorden: gegeven dat de som van de getallen 30 is, zou S het voor mogelijk hebben gehouden dat P wist wat de getallen waren. Maar S zei nu juist 'dat wist ik al', namelijk dat P niet wist wat de getallen zijn. Daarom kunnen de getallen niet 14 en 16 zijn.

Door middel van dit soort eliminatie van getallenparen leren S en P genoeg van hun bekendmakingen om de unieke oplossing van het probleem te bepalen.

Na deze ponering van het probleem kwam het op verschillende andere academische plaatsen eveneens boven water, met name in het vakgebied van de kunstmatige intelligentie, nadat het daar was verspreid door John McCarthy in [9], aan het eind van de jaren 70. Dit werd gevolgd door prettige woekeringen van dit probleem in de populairwetenschappelijke pers (zie de details hierna). Het maakte tevens opgang in de zogenaamde 'kennislogica' voor het expliciet in logische taal beschrijven van kennis en kennisverandering, met name in een publicatie

No. 223. A zegt tot S en P: Ik heb twee gehele getallen x, y gekozen met $1 < x < y$ en $x + y \leqslant 100$. Straks deel ik $s = x + y$ aan S alleen mee, en $p = xy$ aan P alleen. Deze mededelingen blijven geheim. Maar jullie moeten je inspannen om het paar (x, y) uit te rekenen.

Hij doet zoals aangekondigd. Nu volgt dit gesprek:

1. P zegt: Ik weet het niet.
2. S zegt: Dat wist ik al.
3. P zegt: Nu weet ik het.
4. S zegt: Nu weet ik het ook.

Bepaal het paar (x, y).

(*H. Freudenthal*).

Figuur 1 De originele publicatie

van Plaza uit 1989 [12]. Via de kennislogica kwam het recentelijk terecht in het gebied van model checking. Daarin kan het probleem in een programmeertaal geformaliseerd worden en kunnen de eigenschappen van S en P en de uniciteit van de oplossing automatisch worden geverifieerd [15].

In deze bijdrage besteden we eerst uitvoerig aandacht aan de verspreiding van het probleem, mede om de resultaten van een NAW lezersoproep in 2005 te rapporteren. Daarna introduceren we de kennislogica (in een variant waarin we ook kunnen refereren aan de gevolgen van waarheidsgetrouwe uitspraken) en analyseren we het probleem in kennislogica. Tenslotte modelleren we het probleem voor bewerking in de model checker DEMO, ontwikkeld door Jan van Eijck aan het Centrum voor Wiskunde en Informatica.

Versies van het raadsel

Een van de grondleggers van de kunstmatige intelligentie, John McCarthy, schreef van 1978 tot 1981 een artikel over het som-en-productprobleem, dat hij als volgt formuleerde [9]:

Two numbers m and n are chosen such that $2 \leq m \leq n \leq 99$. Mr. S is told their sum and Mr. P is told their product. The following dialogue ensues:

1. Mr. P: I don't know the numbers.
2. Mr. S: I knew you didn't know. I don't know either.
3. Mr. P: Now I know the numbers.
4. Mr. S: Now I know them too.

In view of the above dialogue, what are the numbers?

Er bestaat een aantal verschillen tussen de versies van Freudenthal en McCarthy. In de versie van McCarthy is de bovengrens voor beide getallen 99, terwijl Freudenthal 100 opgeeft als bovengrens voor de *som* van beide getallen. Ook staat McCarthy, anders dan Freudenthal, twee gelijke getallen toe. Daardoor zijn aan het begin veel meer getallenparen toegestaan in de versie van McCarthy. Verder geeft Mr. S. in zijn tweede bekendmaking extra informatie ("I don't know either") die niet voorkomt in de dialoog van Freudenthal. Het blijkt dat geen van deze wijzigingen afzonderlijk, noch in combinatie, invloed heeft op de oplossing (zie [15]).

Vanaf de jaren zeventig zijn er veel verschillende versies van Freudenthal's raadsel in omloop geweest. Deze variaties verschillen van het origineel in een aantal aspecten: andere bekendmakingen in de dialogen, andere toegestane getallen en verschillende keuzen wat betreft de informatie voorafgaand aan de dialoog. Wordt die begininformatie bij voorbeeld impliciet gegeven als 'common knowledge' van S en P, zoals Freudenthal inventief deed in zijn origineel, of is alleen de lezer van die informatie op de hoogte? Voor discussies over de verschillende varianten van dit raadsel verwijzen we graag naar de literatuur over recreatieve wiskunde, bijvoorbeeld [1–3, 6–7, 13], en de website http://www.mathematik.uni-bielefeld.de/~sillke/PUZZLES/logic_sum_product. Voor een bijzonder elegante wiskundige analyse bevelen we graag [7] aan. Interessant is verder Edsger Dijkstra's analyse [19].

Meer op logici gericht zijn de publicaties [10–12]. Plaza maakt een model van het raadsel in een dynamische kennislogica die de voorloper is van de logica van openbare mededelingen die we hier presenteren. We zijn schatplichtig aan Plaza voor de beschrijving van het beginmodel en de formalisering van de effecten van de bekendmakingen in de dialoog.

Op zoek naar de oorsprong

Zowel John McCarthy als Martin Gardner [6, 9] wisten niet van Freudenthal's publicatie en stelden de vraag waar het probleem vandaan kwam, zonder deze bevredigend te kunnen beantwoorden. Zo zegt McCarthy in een voetnoot van zijn artikel [9]:

"I have not been able to trace Mr. S and Mr. P back beyond its alleged appearance on a bulletin board at Xerox PARC."

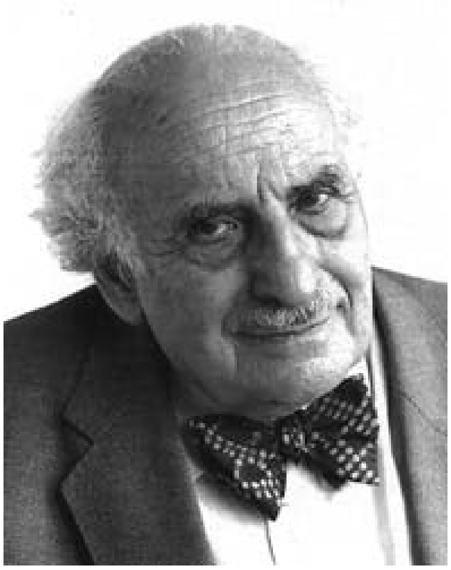
Martin Gardner schrijft in 1979 in zijn column "Mathematical Games" [6]:

"This beautiful problem, which I call "impossible" because it seems to lack sufficient information for a solution, began making the rounds of mathematics meetings a year or so ago. I do not know its origin."

Als reactie op [6] schreef de Nederlandse algebraïcus Robert van der Waall aan Gardner over Freudenthal's publicatie in 1969 in het *Nieuw Archief voor de Wiskunde*, waarna Gardner in een vervolgcolumn de juiste credits gaf.

Wij hebben geprobeerd twee openstaande vragen over de geschiedenis van het som-en-productraadsel te beantwoorden:

1. Als het raadsel inderdaad voor het eerst in druk verscheen in 1969 in [4], hoe is het probleem dan tien jaar later terecht gekomen op "a bulletin board at Xerox PARC" en "the rounds of mathematics meetings" in de Verenigde Staten?



Hans Freudenthal (1905 – 1990)

2. Heeft Freudenthal het raadsel zelf ontworpen? En zo ja, werd hij daarbij wellicht geïnspireerd door mogelijk minder complexe voorgangers?

Over vraag 1 hebben we oproepen gedaan op internationale maillijsten zoals "Foundations of Mathematics" en een groot aantal Nederlandse en Amerikaanse wiskundigen aangeschreven die in de jaren 60 en 70 een goed internationaal netwerk hadden. Daarbij hebben we een aantal mooie anekdotes gehoord. Zo leerde de psycholoog en internationaal schaakmeester J.T. Barendregt, vader van logicus Henk Barendregt, in de vroege jaren 60 van zijn Russische schaakcollega's een raadsel kennen dat nu een van de voorgangers van het som-en-productprobleem uit [17] blijkt te zijn. De beroemde wiskundige John Conway had zelf in de jaren 70 onafhankelijk een andere puzzel bedacht waarbij kennis en gebrek aan kennis een sleutelrol vervullen. Hij raakte begin jaren 70, met de trein op reis in Nederland, een keer aan de praat met de reiziger tegenover hem, die Hans Freudenthal bleek te heten. Conway heeft Freudenthal toen uitgebreid gecomplimenteerd over LINCOS (Lingua Cosmica), Freudenthal's taal om met eventueel buitenaards leven in contact te komen, maar beide heren kwamen er niet achter dat zij zulke gelijksoortige raadsels hadden ontworpen. Toch kunnen we nog steeds geen precies antwoord geven op de eerste vraag.

Wat de tweede vraag betreft vonden we geen bevestiging in Freudenthal's gepubliceerde geschriften, noch in onze contacten met het Freudenthal-instituut. Professor N.G. de Bruin schreef ons wel het bemoedigende bericht dat, als geen bron werd vermeld

BREINBROUWSELS - 492

OP HET VOETBALVELD

Samen zaten ze op de tribune. Tevoren kenden zij elkaar niet, maar sport verbroedert. ,,Kijk," zei de heer Brouwers tot zijn buurman, ,,die met rugnummer 2 is mijn wettige nazaat! Toevallig ook nummer twee van de serie!"

De heer Raadmans moest even wennen aan de zonderlinge zinswendingen van zijn medetribunist. ,,Heeft die serie van u een grote lengte?" vroeg hij dan, geheel in stijl.

,,Het zijn er vijf, met de nodige tussenpozen," sprak de heer Brouwers met gepaste trots, ,,twee durskes en drie jongs!"

,,En hoe oud is dat vijftal dan wel?" wilde de heer Raadmans weten, daar hij steeds meer schik in zijn buur kreeg.

,,Kijk, dat zal ik u eens precies vertellen. Als ik de leeftijden van mijn jongens in hele jaren met elkaar vermenigvuldig, is het produkt precies 900!"

De heer Raadmans keek zijn medevoetbalgeestdrifteling eens aan. Een goede veertiger, schatte hij. ,,U geeft me nu wel dat produkt, maar die jongens van u kunnen allerlei leeftijden hebben. Dat ,,precies vertellen" van u lijkt er niet op."

,,Ziet u daar dat uitslagenbord? Welnu, het getal, dat door de doelpunten wordt aangegeven, is juist gelijk aan de som van de jaren van de drie jongs!"

De heer Raadmans, die het spel met aandacht had gevolgd, behoefde niet eens naar het bord te kijken, want hij wist best hoe de stand was. ,,Maar nu weet ik nog niet hoe oud uw jongens zijn. Om van de meisjes nog maar niet te spreken!" Hij werd een weinig kriegel, maar vond toch dat het gesprek enige spanning vertoonde. ,,U moet me toch nog iets meer vertellen," drong hij aan.

,,Nu, goed dan. Als ik de lieftallige leeftijden van mijn durskes met elkaar vermenigvuldig, krijg ik 144!"

Even dacht de heer Raadmans na. En toen wist hij hoe oud de vijf kinderen waren. . .

Deze episode is mij verhaald door de heer C. G. Möhlmann te Hamersveld. Ik ben zeer benieuwd of u even scherpzinnig bent als de heer Raadmans. Indien dit inderdaad zo is en u deelt mij het resultaat van uw bevindingen mee, dan krijgt u een aantal punten, dat gelijk is aan de leeftijd van een der kinderen, wederom in gehele jaren! *Ir. G. van Tilburg*

VOORWAARDEN

Dit Breinbrouwsel maakt deel uit van onze ladderwedstrijd, waaraan iedereen op elk gewenst ogenblik kan deelnemen. De punten, die men voor zijn ingezonden oplossing krijgt, blijven geldig, tenzij men zonder opgave van redenen gedurende drie maanden niet inzendt. Indien u echter blijft inzenden, wordt uw puntentotaal steeds hoger. Elke week krijgen de drie oplossers, wier puntentotaal dan het hoogste is, een prijs van 25 gulden. De punten, die de hoogste en de op één na hoogste méér hebben dan de derde, worden voor beide eerstgenoemden op hun volgende ladder als beginpunten genoteerd! U ziet, dat hier geen geluk in het spel is, maar dat de noeste volhouder er zeker van is op de duur een prijs te zullen winnen!

Men mag twee opeenvolgende oplossingen tegelijk inzenden; ook mogen de oplossingen van meer deelnemers tegelijk worden ingestuurd. Ik vertrouw er echter op, dat elke oplossing onafhankelijk wordt gevonden. Lossen sommige deelnemers samen op, dan krijgen zij samen punten, bijvoorbeeld als ,,de familie X" of ,,J. Karelsen en P. van Peuteren samen".

Indien u vragen heeft, worden deze beantwoord, mits u een postzegel van 12 cent insluit.

De oplossingen van deze puzzel moeten uiterlijk 15 juni 1963 binnen zijn bij de redactie van de Katholieke Illustratie, Nassaulaan 51, Haarlem. In de linkerbovenhoek van briefkaart of envelop moet ,,Breinbrouwsel 492" vermeld staan, terwijl in het schrijven naam en adres van de inzender *duidelijk* dienen te worden geschreven en wijzigingen daarin bij een volgende inzending uitdrukkelijk moeten worden opgegeven!

Figuur 2 Breinbrouwsel 492, uit: *de Katholieke Illustratie*, 1932

in de rubriek met wiskundige problemen in het *Nieuw Archief* in de jaren zestig, degene die het probleem had aangeleverd altijd ook de bedenker ervan was.

Het interessantst was een reactie op onze oproep in het *Nieuw Archief*. Een abonnee antwoordde dat hij zich herinnerde het som-en-productprobleem voor het eerst te hebben gelezen in de jaren 50, in de puzzelcolumn *Breinbrouwsels* van het weekblad *De Katholieke Illustratie*. Twee van de auteurs van dit artikel hebben tijdens enkele ochtenden in de Groningse Universiteitsbibliotheek en de Provinciale Bibliotheek Friesland te Leeuwarden alle relevante jaargangen van *De Katholieke Illustratie* doorgezocht. Wij vonden daarbij bijna alle 626 afleveringen van "Breinbrouwsels" van de hand van ir. G. van Tilburg, iedere week verschenen van 1954 tot het door Van Tilburg zeer betreurde besluit van de redactie in 1965 om de puzzelrubriek te stoppen. Hierbij stuitten we niet op het som-en-productprobleem, maar wel op vier interessante voorgangers ervan, waarin de puzzelaar ook geholpen wordt in de berekening van bepaalde getallen door de kennis dat deelnemers aan een conversatie bepaalde feiten *niet* weten. Voor degenen onder de lezers die toegang hebben tot *De Katholieke Illustratie*: het gaat om *Breinbrouwsels* nummers 12 (1954), 56 (1955), 166 (1957) en 492 (1963).

Als voorbeeld geven we in figuur 2 *Breinbrouwsel* 492 uit *De Katholieke Illustratie* vol. 97 (22), 1963, p. 47. Dit is een ware voorganger van het som-en-productprobleem vanwege een uitspraak van de heer Raadmans over zijn onwetendheid, die cruciaal is voor het vinden van de oplossing: "Maar nu weet ik nog niet hoe oud uw jongens zijn. Om van de meisjes nog maar niet te spreken!"

We zullen het antwoord niet weergeven: dat laten we aan de lezer over. Interessant is dat Van Tilburg in het raadsel het volgende niet expliciet vermeldde: "Rugnummers worden door voetballers gedragen, dus is het tweede kind van de heer Brouwers een zoon", zoals hij in de oplossing als bekend veronderstelt – en dat was het in 1963 waarschijnlijk ook nog.

Van Tilburg was overigens niet de allereerste die een analoog probleem publiceerde. De eerste twee publicaties die we hebben gevonden met behulp van David Singmaster's bibliografie van de recreatieve wiskunde (zie http://www.g4g4.com/MyCD5/SOURCES/singmaterial.htm) zijn van de Britse puzzelpublicisten Williams en Savage [17–18] uit de jaren 40, waarover we hebben geschreven in [15].

Het antwoord op onze tweede vraag is dus waarschijnlijk: "Ja, Freudenthal heeft het probleem inderdaad zelf ontworpen, maar kende wellicht enkele analoge problemen."

Na dit gedetailleerde verslag van de ontstaansgeschiedenis en verspreiding van het raadsel, gaan we verder met het meer technisch-logische gedeelte: een algemeen logisch model van het effect van bekendmakingen in dialogen zoals die tussen S en P op de kennis van de deelnemers. Voor we dit vergeten: de oplossing van het raadsel is dat Som het getal 4 en Product het getal 13 heeft.

Kennislogica

Kennislogica (ook wel: 'epistemische logica') kan gezien worden als een uitbreiding van de propositielogica met operatoren voor kennis en voor kennisverandering. De historische bron voor deze logica is Jan Plaza [12].

Gegeven een verzameling actoren A en een verzameling propositievariabelen P, is de taal van de kennislogica inductief te definiëren als volgt.

(i) Ieder atoom $p \in P$ is een formule, en
(ii) als ϕ en ψ formules zijn, dan zijn ook $\neg\phi$, $(\phi \wedge \psi)$, $K_a\phi$ en $[\phi]\psi$ formules, voor iedere $a \in A$.

Een formule van de vorm $K_a\phi$ lezen we als 'agent a weet formule ϕ'. De operator K staat voor 'knows'. Een formule van de vorm $[\phi]\psi$ lezen we als 'na *openbare bekendmaking* van ϕ, (is) ψ (waar)'. Met 'openbaar' (of 'publiek') bedoelen we dat alle actoren kunnen horen wat er gezegd wordt, en dit ook van elkaar weten, enzovoorts. De bekendmaking kan gedaan worden door een van de gemodelleerde actoren, maar ook door een buitenstaander, die als het ware van boven op het systeem neerkijkt. Daarom wordt er ook wel gesproken van een 'openbaring' ('revelation') in plaats van een openbare bekendmaking. Behalve openbaar nemen we ook aan dat de bekendmaking waarheidsgetrouw is, en dat ook dat gemeenschappelijk bekend is bij de actoren.

Deze logische taal interpreteren we op relationele structuren. Een *kennismodel* is een drietal $M = \langle S, \sim, V \rangle$ dat bestaat uit een *domein* S van *toestanden* (traditioneel ook wel 'werelden' genaamd), een *toegankelijkheidsrelatie*, of eerder gezegd *-functie* $\sim : A \to \mathcal{P}(S \times S)$, zodat iedere $\sim_a$ een equivalentierelatie is, en een *waardering* $V : P \to \mathcal{P}(S)$ om te preciseren welke feiten in welke toestanden gelden – de waardering V_p voor atoom p bestaat dus uit de deelverzameling toestanden in het domein waar p waar is. Voor een toestand $s \in S$ noemen we het paar (M, s) een *kennistoestand* of informatietoestand. Gegeven twee toestanden s, s' in het domein, betekent $s \sim_a s'$ dat actor a de toestand s niet van s' kan onderscheiden op basis van de voor die actor beschikbare informatie. Bijvoorbeeld, voordat S en P hun gesprek voeren zijn voor S de paren $(14, 16)$ en $(7, 23)$ niet te onderscheiden maar wel voor P. Gegeven een domein van getalparen hebben we dan dat $(14, 16) \sim_S (7, 23)$ maar $(14, 16) \not\sim_P (7, 23)$.

Hiermee komen we dan uiteindelijk bij de semantiek aan, die ons vertelt hoe we de formele taal op de kennismodellen interpreteren. Gegeven een kennismodel $M = \langle S, \sim, V \rangle$, wordt de interpretatie van een formule op dit model als volgt inductief gedefinieerd. De constructie '$M, s \models \phi$' lezen we als 'formule ϕ is waar in kennistoestand (M, s)', en 'desda' staat voor 'dan en slechts dan als'.

$$
\begin{array}{rll}
M, s \models p & \text{desda} & s \in V_p \\
M, s \models \neg\phi & \text{desda} & M, s \not\models \phi \\
M, s \models \phi \wedge \psi & \text{desda} & M, s \models \phi \ \& \ M, s \models \psi \\
M, s \models K_a\phi & \text{desda} & \text{voor alle } t \in S, \\
& & \quad \text{als } s \sim_a t \text{ dan } M, t \models \phi \\
M, s \models [\phi]\psi & \text{desda} & \\
& \text{als } M, s \models \phi \text{ dan } M|\phi, s \models \psi &
\end{array}
$$

Hierbij is het kennismodel $M|\phi = \langle S', \sim', V' \rangle$ in de clausule voor $[\phi]\psi$ gedefinieerd als

$$
\begin{aligned}
S' &= \{s' \in S \mid M, s' \models \phi\} \\
\sim'_a &= \sim_a \cap (S' \times S') \\
V'_p &= V_p \cap S'
\end{aligned}
$$

De operator $[\phi]$ kan gezien worden als een omvormer van kennistoestanden, namelijk van M naar $M|\phi$. Het Engelse equivalent is 'epistemic state transformer', naar analogie van het bekendere 'state transformer' in de semantiek van programmeertalen. Het model $M|\phi$ is een submodel van M, namelijk de beperking van het domein S van M tot de toestanden waar ϕ waar is, met behoud van toegankelijksrelaties en waardering op deze restrictie. De zogenaamde duale van operator $[\phi]$ is $\langle\phi\rangle$. We bedoelen hiermee dat $\langle\phi\rangle\psi$ gedefinieerd is als $\neg[\phi]\neg\psi$.

Bijvoorbeeld, in de begintoestand $(7, 23)$ is de bewering $K_P(x_7 \wedge y_{23})$ – P weet dat de getallen 7 en 23 zijn – waar, omdat er voor P geen ander getallenpaar voorstelbaar is. Zoals al gezegd, heeft het product van twee priemgetallen immers geen andere ontbinding. Aan de andere kant geldt $\neg K_S(x_7 \wedge y_{23})$ – S weet niet dat de getallen 7 en 23 zijn – omdat $(7, 23) \sim_S (14, 16)$, en in de toestand $(14, 16)$ van het model is bewering $(x_7 \wedge y_{23})$ onwaar. En P's bekendmaking 'ik weet het niet' beperkt het domein tot toestanden waarin de bewering waar is. Dit leidt dus tot eliminatie van paar $(7, 23)$ uit het model.

```
module SumProduct
where import DEMO

pairs :: [(Int,Int)]
pairs  = [ (x,y) |  x <- [2..100], y <- [2..100], x < y, x+y <= 100 ]
numpairs = toInteger (length pairs)
indexed_pairs = zip [0..numpairs-1] pairs
msnp :: EM
msnp = (Mo [0..numpairs-1] val [a,b] acc [0..numpairs-1])
  where
  val   = [ (w,[P x, Q y]) | (w,(x,y)) <- indexed_pairs]
  acc   = [ (a,w,v) | (w,(x1,y1)) <- indexed_pairs,
                      (v,(x2,y2)) <- indexed_pairs,
                       x1+y1 == x2+y2              ]
          ++
          [ (b,w,v) | (w,(x1,y1)) <- indexed_pairs,
                      (v,(x2,y2)) <- indexed_pairs,
                       x1*y1 == x2*y2              ]
pform :: Int ->  Int -> Form
pform x y = Conj [Prop (P x), Prop (Q y)]
statement_2 =
  Conj [ pform x y ‘impl‘ Neg (K b (pform x y)) | (x,y) <- pairs ]
announce_2 = public (K a statement_2)
statement_3 =
  Conj [ pform x y ‘impl‘ K b (pform x y) | (x,y) <- pairs ]
announce_3 = public statement_3
statement_4 =
  Conj [ pform x y ‘impl‘ K a (pform x y) | (x,y) <- pairs ]
announce_4 = public statement_4
solution = showM (upds msnp [announce_2,announce_3,announce_4])
```

Figuur 3: De DEMO-module `SumProduct`. Commentaarregels zijn verwijderd.

'Som en product' in kennislogica

Het modelleren van 'som en product' in kennislogica is nu vrij gemakkelijk. Om te beginnen bepalen we de verzameling van atomaire proposities (propositieletters) en actoren. De actoren zijn S en P – de rol van de aangever A is alleen de achtergrondinformatie publiek te krijgen. De gegeven verschillende natuurlijke getallen x, y tussen 1 en 100 leggen we vast in de verzameling $I \equiv \{(x, y) \in \mathbf{N}^2 \mid 1 < x < y \ \& \ x + y \leq 100\}$. De atomaire propositie '$x = 3$' staat voor de informatie 'de waarde van de variabele x is 3.' Iets formeler kunnen we '$x = 3$' representeren als een propositieletter x_3. Op die manier vormen we een eindige verzameling atomen $\{x_i \mid (i, j) \in I\} \cup \{y_j \mid (i, j) \in I\}$.

De propositie 'S weet dat de getallen 4 en 13 zijn' formaliseren we als $K_S(x_4 \wedge y_{13})$. En 'S weet wat de getallen zijn' is dan formeel $K_S(x, y) \equiv \bigvee_{(i,j)\in I} K_S(x_i \wedge y_j)$ (het symbool $\bigvee$ staat voor een disjunctie van meerdere leden). Op dezelfde manier is 'P weet wat de getallen zijn' te beschrijven als $K_P(x, y) \equiv \bigvee_{(i,j)\in I} K_P(x_i \wedge y_j)$. Merk verder op dat 'wist' in bekendmaking 2 van S verwijst naar de waarheid van $K_S\neg K_P(x, y)$ in de *begintoestand* van het probleem, dus niet in de toestand die resulteert na bekendmaking 1 door P. Dit maakt onmiddellijk duidelijk dat bekendmaking 1 door P verder in de analyse over het hoofd gezien kan worden, ook al omdat bekendmaking 2 uit bekendmaking 1 volgt: als je iets weet, is het waar. Op deze wijze modelleren we alle vier de bekendmakingen ter oplossing van het probleem:

1. P zegt: "Ik weet het niet": $\neg K_P(x, y)$
2. S zegt: "Dat wist ik al": $K_S\neg K_P(x, y)$
3. P zegt: "Nu weet ik het": $K_P(x, y)$
4. S zegt: "Nu weet ik het ook": $K_S(x, y)$

Deze bekendmakingen interpreteren we achtereenvolgens, te beginnen met 2, op epistemisch model $\mathcal{SP}_{(x,y)} \equiv \langle I, \sim, V \rangle$ dat bestaat uit een *domein* van paren $(x, y) \in I$ (als hiervoor), *equivalentierelaties* (toegankelijkheidsrelaties) $\sim_S$ en $\sim_P$ zodanig dat voor S: $(x, y) \sim_S (x', y')$ desda $x + y = x' + y'$ en voor P: $(x, y) \sim_P (x', y')$ desda $xy = x'y'$; en *waardering* V zodanig dat $V_{x_i} = \{(x, y) \in I \mid x = i\}$ en $V_{y_j} = \{(x, y) \in I \mid y = j\}$.

Om de oplossing van het probleem weer te geven, kunnen we zeggen dat

$$
\begin{aligned}
&\mathcal{SP}_{(x,y)}, (4, 13) \models \\
&\qquad \langle K_S\neg K_P(x, y)\rangle\langle K_P(x, y)\rangle\langle K_S(x, y)\rangle\top
\end{aligned}
$$

Hierin staat $\top$ ('truth') voor de 'altijd ware' bewering. Met andere woorden, gegeven dat $(4, 13)$ het werkelijke getallenpaar is, kunnen de beweringen 2, 3, en 4 in die volgorde pu-

Publieke werken van Thomas Rosenboom (Querido, 1999)

bliek uitgesproken worden. Eigenlijk geeft deze formule alleen weer dat *ten minste* $(4, 13)$ een oplossing is. Er zijn nog preciezer manieren waarop we ook kunnen uitdrukken dat dit de enige oplossing is (zie [15]).

We kunnen nu ook de raadselachtigheid van het raadsel expliciteren. In de begintoestand weet P *niet* wat de getallen zijn, maar na de bekendmaking 2 van S weet P het *wel*. Dit komt overeen met

$$SP_{(x,y)}, (4, 13) \models \langle K_S \neg K_P(x, y) \rangle \neg K_S \neg K_P(x, y)$$

Met andere woorden, iets kan onwaar worden door het bekend te maken. Rara, hoe kan dat? Dat weten we nu.

'Som en product' in DEMO

Sinds enige tijd bestaan er zogenaamde model checkers voor kennislogica, programma's waarmee epistemische eigenschappen van communicatieve acties automatisch kunnen worden geverifieerd. DEMO (de afkorting staat voor *Dynamic Epistemic MOdelling*) is ontwikkeld aan het CWI in Amsterdam door een van de auteurs van dit artikel. Het implementeert kennismodellen, operaties op kennismodellen en toetsing van epistemische formules in kennismodellen. DEMO is geschreven in de functionele programmeertaal Haskell. Openbare bekendmaking is maar een eenvoudig voorbeeld van de communicatieve acties die DEMO aankan, maar het scala aan voorbeelden is heel veel groter.

De implementatie van het som-en-productraadsel in DEMO (van de hand van Ji Ruan) vindt u in Figuur 3. In Haskell is een lijst een standaard datastructuur, maar een verzameling niet. De verzameling $I \equiv \{(x, y) \in \mathbf{N}^2 \mid 1 < x < y \ \& \ x+y \leq 100\}$ is daarom in het programma geïmplementeerd als een lijst

```
pairs = [(x,y) | x<-[2..100],
        y<-[2..100], x<y, x+y<=100]
```

De symbolen { en } zijn dus vervangen door [en], het symbool $\in$ door `<-`, en in plaats van I noemen we dit semantisch object `pairs`. We koppelen nu elk getallenpaar aan een natuurlijk getal, om die natuurlijke getallen vervolgens te kunnen gebruiken als namen voor mogelijke werelden. Het resultaat heet `indexed_pairs`. Het kennismodel voor de begintoestand van het som-en-productraadsel heet in de implementatie `msnp`. Dit model heeft als domein `[0..numpairs-1]`, terwijl de waardering van atomaire proposities is geregeld in `val` en de toegankelijkheidsrelatie voor de actoren in `acc`. Het vierde onderdeel geeft aan dat vooralsnog elk getallenpaar in `[0..numpairs-1]` het werkelijke getallenpaar zou kunnen zijn.

Voor het precieze verband tussen bekendmakingen, de logische formalisering, en de weergave in DEMO, nemen we $K_S \neg \bigvee_{(i,j) \in I} K_P(x_i \wedge y_j)$, voor "$S$ zegt: Dat wist ik al". De logische formule is equivalent met $K_S \bigwedge_{(i,j) \in I} \neg K_P(x_i \wedge y_j)$. Een in het model equivalente maar computationeel zuiniger alternatief is $\bigwedge_{(i,j) \in I}((x_i \wedge y_j) \to \neg K_P(x_i \wedge y_j))$. Dit is de formule `statement_2` in het programma.

Het resultaat van uitvoering van de drie bekendmakingen uit het raadsel in het beginmodel ziet er in DEMO zo uit:

```
SumProduct> solution
==> [0]
[0]
(0,[p4,q13])
(a,[[0]])
(b,[[0]])
```

Dit geeft aan dat op het punt waar alle openbare bekendmakingen verwerkt zijn het kennismodel bestaat uit een enkele wereld 0, een wereld die correspondeert met het getallenpaar $(4, 13)$, terwijl beide actoren op de hoogte zijn van deze unieke oplossing.

Een nieuw raadsel

Met deze uitleg van de implementatie van het som-en-productprobleem besluiten we dit verhaal. Enerzijds doet zo'n programma wellicht wat aan de 'magie' van het oorspronkelijk probleem af, maar anderzijds biedt het ook weer vernieuwende mogelijkheden om soortgelijke raadels te ontwikkelen en te testen. Voor de NAW-lezer presenteren we daarom een nieuw epistemisch raadsel in de traditie van onzekerheid die meerdere actoren over getallen hebben, waarbij die onzekerheid door het uitspreken ervan weggenomen wordt. Het volgende raadsel is een variant op [8].

Drie actoren A, B en C krijgen ieder een positief natuurlijk getal op het voorhoofd geplakt. Ze kunnen alleen het voorhoofd van de anderen zien, maar, uiteraard, niet dat van zichzelf. Een van de getallen is de som van de andere twee getallen. Al het voorgaande is gemeenschappelijke kennis. De volgende conversatie vindt nu plaats:

- *A: "Ik weet mijn getal niet."*
- *B: "Ik weet mijn getal niet."*
- *C: "Ik weet mijn getal niet."*

Agent A weet nu wat haar getal is. Wat zijn de getallen en wie heeft welk getal, als alle getallen priem zijn?

Als u dit een lastig probleem vindt, kunt u natuurlijk ook proberen het antwoord met behulp van DEMO te vinden. Zie hiervoor [16] en http://homepages.cwi.nl/~jve/demo.

Dankwoord

Rineke, Jan en Hans danken het NIAS (Netherlands Institute for Advanced Studies in the Humanities and Social Sciences) voor haar gastvrijheid, in het kader van het NIAS project 'Games, Action, and Social Software'. Verder danken wij het NWO Cognitieprogramma voor de Advanced Studies beurs NWO 051-04-120 waarmee het bezoek van Hans van Ditmarsch aan het NIAS gefinancierd is, en NWO MagW voor de Replacement grant NWO 400-05-710 die het mogelijk maakte dat Rineke Verbrugge haar tijd tijdens het NIAS-project aan onderzoek kon besteden. De titel 'Publieke Werken' van deze bijdrage is naar de bekende roman van Thomas Rosenboom met wie wij met veel genoegen maaltijden op het NIAS gedeeld hebben. Deze titel is een knipoog naar de 'public announcements' – openbare bekendmakingen – en 'public announcement logic' – kennislogica – die centraal staan in onze modellering.

References

1 A. Born, C.A.J. Hurkens, and G.J. Woeringer. The Freudenthal problem and its ramifications: Part (I). *Bulletin of the EATCS*, 90:175–191, 2006.

2 A. Born, C.A.J. Hurkens, and G.J. Woeringer. The Freudenthal problem and its ramifications: Part (II). *Bulletin of the EATCS*, 91:189–204, 2007.

3 A. Born, C.A.J. Hurkens, and G.J. Woeringer. The Freudenthal problem and its ramifications: Part (III). *Bulletin of the EATCS*, 95:201–219, 2008.

4 H. Freudenthal. (formulering van het som-en-productprobleem). *Nieuw Archief voor Wiskunde*, 3(17):152, 1969.

5 H. Freudenthal. (oplossing van het som-en-productprobleem). *Nieuw Archief voor Wiskunde*, 3(18):102–106, 1970.

6 M. Gardner. Mathematical games. *Scientific American*, 241(December):20–24, 1979. Tevens besproken in jaargang 242, nummers March (pagina 24) en May (paginas 20–21), 1980.

7 I.M. Isaacs. The impossible problem revisited again. *The Mathematical Intelligencer*, 17(4):4–6, 1995.

8 A. Liu. Problem section: Problem 182. *Math Horizons*, 11:324, 2004.

9 J. McCarthy. Formalization of two puzzles involving knowledge. In V. Lifschitz, editor, *Formalizing Common Sense : Papers by John McCarthy*, Ablex Series in Artificial Intelligence. Ablex Publishing Corporation, Norwood, N.J., 1990. Origineel manuscript daterend uit 1978–1981.

10 G. Panti. Solution of a number theoretic problem involving knowledge. *International Journal of Foundations of Computer Science*, 2(4):419–424, 1991.

11 R. Parikh. Finite and infinite dialogues. In E. Moschovakis, editor, *Workshop on Logic from Computer Science*, pages 481–498. MSRI Publications / Springer, 1992.

12 J.A. Plaza. Logics of public communications. In M.L. Emrich, M.S. Pfeifer, M. Hadzikadic, and Z.W. Ras, editors, *Proceedings of the 4th International Symposium on Methodologies for Intelligent Systems: Poster Session Program*, pages 201–216. Oak Ridge National Laboratory, 1989. ORNL/DSRD-24.

13 L. Sallows. The impossible problem. *The Mathematical Intelligencer*, 17(1):27–33, 1995.

14 H.P. van Ditmarsch. Het zeven-kaartenprobleem. *Nieuw Archief voor Wiskunde*, 3(4):326–332, 2002.

15 H.P. van Ditmarsch, J. Ruan, and R. Verbrugge. Sum and product in dynamic epistemic logic. *Journal of Logic and Computation*, 18(4):563–588, 2007.

16 J. van Eijck. DEMO — a demo of epistemic modelling. In J.F.A.K. van Benthem, D. Gabbay, and B. Löwe, editors, *Interactive Logic — Proceedings of the 7th Augustus de Morgan Workshop*, number 1 in Texts in Logic and Games, pages 305–363. Amsterdam University Press, 2007.

17 W. T. Williams and G. H. Savage. *The Penguin Problems Book: A Modern Anthology of Perplexities and Tantalizers*. Penguin Books (Allen Lane), Harmondsworth, 1940.

18 W. T. Williams and G. H. Savage. *The Second Penguin Problems Book*. Penguin Books, Harmondsworth, 1944.

19 E.W. Dijkstra, *A problem solved in my head*, E.W. Dijkstra archive, EWD666, see www.cs.utexas.edu/users/EWD/ewd06xx/EWD666.PDF, 1976.