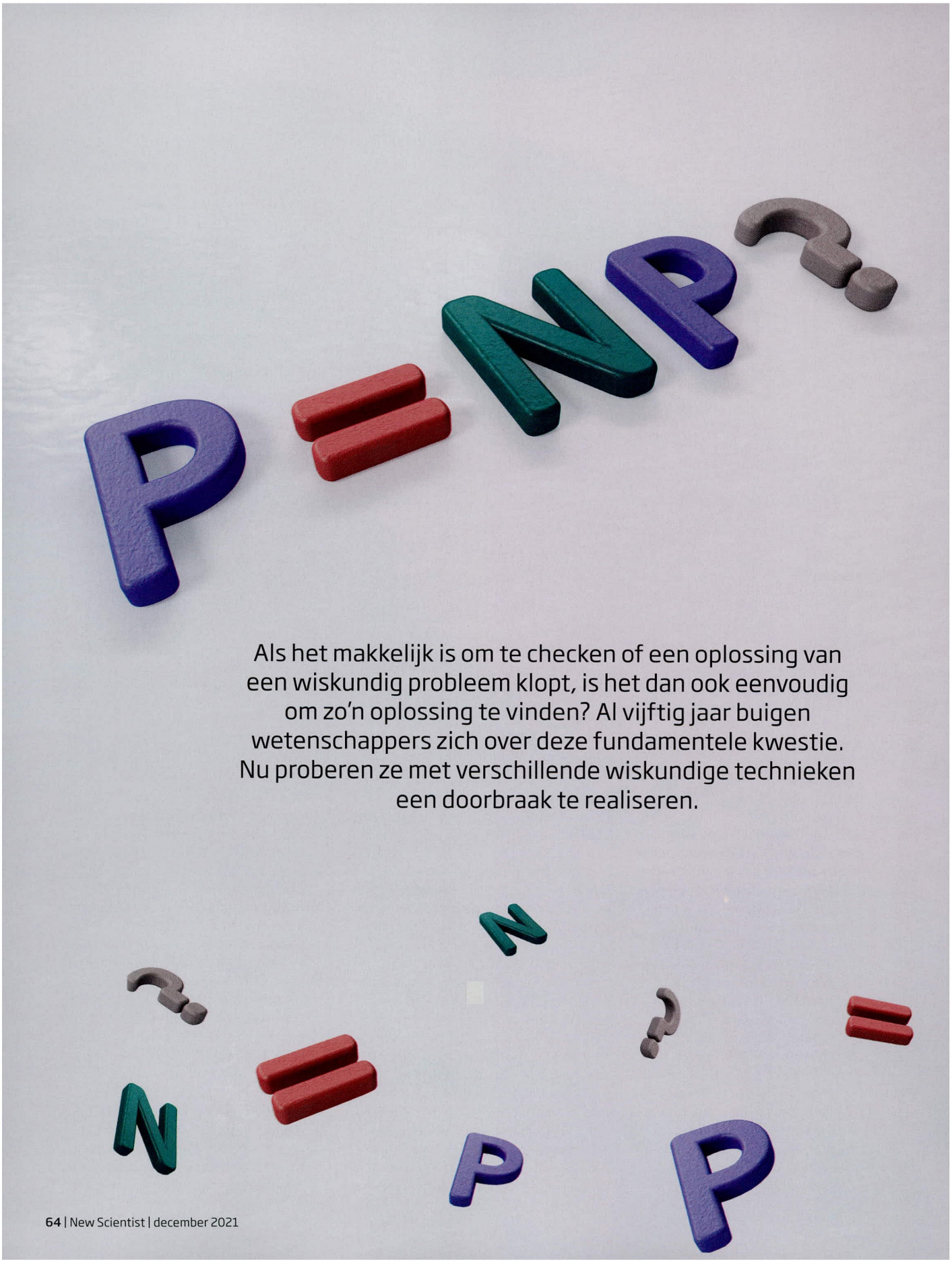
Publicatie : New Scientist
Datum : 31 dec 2021
cm2 : 2568
Pagina : 64
AVE : € 13338,00
Regio : Nederland
Frequentie : 11x per jaar
Oplage : 15000



Als het makkelijk is om te checken of een oplossing van een wiskundig probleem klopt, is het dan ook eenvoudig om zo'n oplossing te vinden? Al vijftig jaar buigen wetenschappers zich over deze fundamentele kwestie. Nu proberen ze met verschillende wiskundige technieken een doorbraak te realiseren.

Dit artikel is uitsluitend voor intern gebruik binnen: Centrum Wiskunde & Informatica

Publicatie : New Scientist
Datum : 31 dec 2021
cm2 : 2568
Pagina : 64
AVE : € 13338,00
Regio : Nederland
Frequentie : 11x per jaar
Oplage : 15000

Wiskundigen delen problemen in complexiteitsklassen in, zoals 'sudoku's van alle groottes en indelingen'. ISTOCK

Tekst: Tamara Florijn

ALS P GELIJK IS AAN NP, ZOUDEN COMPUTERS ZO HET WERK VAN WISKUNDIGEN KUNNEN OVERNEMEN

Haperend komt de verbinding tot stand. Op het scherm verschijnen een voor een de namen van verschillende grote wetenschappers. Het is tijd voor de jaarlijkse STOC-conferentie voor theoretische informatica. Op diezelfde conferentie presenteerde de Amerikaans-Canadese informaticus en wiskundige Stephen Cook in 1971 een ongelofelijk lastig wiskundig vraagstuk aan zijn collega's: is P gelijk aan NP? In 2021 helpt zijn kleinzoon de inmiddels 81-jarige Cook om het beeld en geluid aan de praat te krijgen voor de online variant die dit jaar plaatsvindt. Ter ere van het vijftigjarige jubileum komen de hoofdrolspelers van toen nog eenmaal – virtueel – bij elkaar. In een notendop houdt het P versus NP-probleem het volgende in: als het makkelijk is om te controleren of een oplossing van een probleem klopt, is het dan ook makkelijk om dat probleem op te lossen? Als het antwoord 'ja' is, dan is P gelijk aan NP. In dat geval zouden we zonder moeite perfecte tijdschema's voor transport kunnen maken. Computers zouden bewijzen uit hun mouw kunnen schudden en zo het werk van wiskundigen kunnen overnemen. En onze banksystemen zouden niet meer veilig zijn, doordat de beveiliging berust op het oplossen van extreem moeilijke problemen – die ineens veel makkelijker te kraken zouden zijn.

Bijna alle wetenschappers denken echter dat het antwoord 'nee' is: P is niet gelijk aan NP. Maar helemaal zeker zijn ze niet. De Russisch-Amerikaanse informaticus en wiskundige Leonid Levin, die in 1973 onafhankelijk van Cook ook met het idee van P vs. NP kwam, legt de vinger op de zere plek. 'Gezond verstand is een onbetrouwbare bron om de moeilijkheid oftewel de complexiteit van problemen te raden,' zegt hij. 'In plaats daarvan hebben we bewijs nodig om te weten of P gelijk is aan NP.' En dat bewijs is er nog niet.

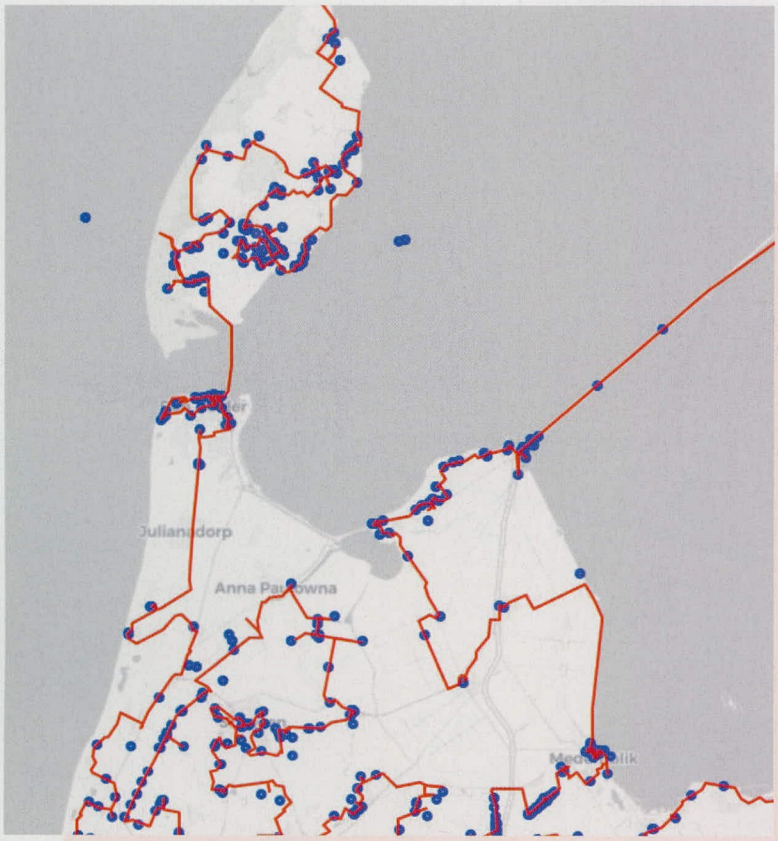
Moeilijke sudoku's

Ook al kunnen computers problemen vaak veel sneller oplossen dan mensen, toch zijn sommige vraagstukken ook met een robotbrein moeilijk te tackelen. De

ANP

Dit artikel is uitsluitend voor intern gebruik binnen: Centrum Wiskunde & Informatica

Publicatie : New Scientist
Datum : 31 dec 2021
cm2 : 2568
Pagina : 64
AVE : € 13338,00
Regio : Nederland
Frequentie : 11x per jaar
Oplage : 15000



ROUTERECORD

Hoe fiets je in een zo kort mogelijke route langs alle 57.912 Rijksmonumenten in Nederland? Een groep Amerikaanse en Deense wiskundigen loste in juli 2021 samen met het Eindhovense adviesbureau CQM dit speciale geval van het handelsreizigersprobleem op. Het optimale rondje van 20.253.062 meter is niet alleen een flinke fietsvakantie, maar ook een nieuw wereldrecord. Nooit eerder is een handelsreizigersprobleem met zo veel locaties op een landkaart opgelost.

OM DE KORTSTE ROUTE TE VINDEN TUSSEN DERTIG STEDEN MOET JE MEER DAN EEN MILJARD STAPPEN NEMEN

hamvraag is dan: welke problemen zijn 'makkelijk' en welke zijn 'moeilijk' met een computer op te lossen? Om dat onderscheid te kunnen maken, delen wiskundigen problemen in verschillende complexiteitsklassen in. Daarbij gaat het niet over specifieke problemen, maar over alle mogelijke problemen van dat type. Bij het oplossen van sudoku's gaat het bijvoorbeeld niet om een mini-sudoku van vier bij vier met een acht in de linkerbovenhoek, maar over sudoku's met alle mogelijke groottes en indelingen.

P is een voorbeeld van zo'n complexiteitsklasse. De problemen uit P zijn makkelijk, want ze zijn binnen een 'redelijke' hoeveelheid tijd op te lossen. Een voorbeeld van een probleem uit klasse P is om het hoogste getal uit een hoop getallen te vissen. Dan zul je de invoergetallen stuk voor stuk moeten bekijken. Dat valt nog onder 'redelijk', omdat het aantal stappen dat je nodig hebt voor de oplossing gelijk is aan het aantal invoergetallen. Dat laatste aantal noemen wiskundigen ook wel de grootte van het probleem.

Om tot de klasse P te behoren, moet het aantal stappen tot de oplossing van een probleem een macht van die probleemgrootte zijn. Bij twee invoergetallen kunnen er bijvoorbeeld 2^3 stappen nodig zijn, of 2^5, of 2^{99}. Bij vier invoergetallen kunnen het er 4^2 zijn, maar ook 4^{200}. De oplostijd die daarbij hoort, noemen we de polynomiale tijd – daar komt de letter P ook vandaan. Een groep getallen sorteren en vermenigvuldigen vergt beide bijvoorbeeld niet meer stappen dan het kwadraat van het aantal getallen. Problemen waarbij je dit moet doen, zijn dus in polynomiale tijd op te lossen en daarmee P-problemen.

De klasse NP (Niet-deterministische Polynomiale tijd) lijkt een tandje lastiger om mee te werken. In NP zitten problemen die in redelijke oftewel polynomiale tijd *geverifieerd* kunnen worden. Als een oplossing al voor je neus ligt, kun je binnen afzienbare tijd checken of die oplossing klopt. Het oplossen van een sudoku is bijvoorbeeld een NP-probleem. Een oplossing van een sudoku controleren is immers zo gedaan. Maar zo'n puzzel oplossen is

Dit artikel is uitsluitend voor intern gebruik binnen: Centrum Wiskunde & Informatica

Publicatie : New Scientist
Datum : 31 dec 2021
cm2 : 2568
Pagina : 64
AVE : € 13338,00
Regio : Nederland
Frequentie : 11x per jaar
Oplage : 15000

ISTOCK

JE KUNT OOK PROBEREN TE BEWIJZEN DAT P NÍET GELIJK IS AAN NP

vaak zo makkelijk nog niet. Of wel? Dat is precies waar het in dit vijftig jaar oude vraagstuk om draait.

Tot hier en niet sneller

Als P gelijk is aan NP, zijn alle makkelijk oplosbare problemen ook makkelijk te controleren, en alle makkelijk controleerbare problemen ook makkelijk op te lossen. Dat eerste is sowieso waar. Als iemand snel een puzzel kan oplossen, dan kun je ook snel controleren of het antwoord klopt. P-problemen zijn dus altijd ook NP-problemen.

Om te bewijzen dat de klassen P en NP daadwerkelijk helemaal gelijk zijn, moet je voor elk NP-probleem weten of er een snelle oplossing voor te vinden is, zoals voor alle P-problemen het geval is. Dat kun je natuurlijk doen door alle denkbare problemen één voor één snel te proberen op te lossen. Maar dat duurt eindeloos. Gelukkig is er een slimmere manier. Wiskundigen kijken naar een bijzondere groep problemen: de zogenoemde NP-volledige problemen. Voor die groep geldt: als je kunt bewijzen dat een van de problemen een snelle oplossing heeft, dan zijn alle andere problemen in NP ook eenvoudig oplosbaar. Laten zien dat één NP-volledig probleem gemakkelijk op te lossen is, is dus genoeg om voor eens en altijd te bewijzen dat P gelijk is aan NP.

Jesper Nederlof, universitair hoofddocent algoritmen en complexiteit aan de Universiteit Utrecht, sleutelt aan verschillende van deze NP-volledige problemen. Een daarvan is het handelsreizigersprobleem. Een handelsreiziger moet pakketjes bezorgen in bijvoorbeeld Amsterdam, Nijmegen en Gent, en moet eindigen in de stad van vertrek. Wat is dan de kortste route? Voor drie steden is dat nog goed te berekenen, maar bij meer raak je al snel de weg kwijt. Zelfs met een slim algoritme vergt die berekening bij tien steden al 2^{10} oftewel 1024 stappen. Bij dertig zijn het er 1.073.741.824. En bij driehonderd steden is het aantal stappen dat je moet nemen om de kortste route te vinden al 2^{300} – meer dan het aantal atomen in het universum.

Het oplossen van dit probleem duurt erg lang: bij elke extra stad die je moet bezoeken, verdubbelt de tijd. Een dergelijke oplostijd met een exponentiële groeifactor duurt veel langer dan polynomiale tijd, wat nodig zou zijn om te bewijzen dat P gelijk is aan NP.

Nederlof probeert het handelsreizigersprobleem in ministapjes sneller op te lossen. Zo wist hij vorig jaar een klein beetje af te snoepen van de oplostijd voor een versimpelde variant van het probleem: in plaats van een verdubbeling van de oplostijd bij een extra stad, kreeg hij het voor elkaar om een algoritme te vinden met een groeifactor van 1,9999. 'Theoretici worden daar enthousiast van, ook al zijn het maar kleine verbeteringen', zegt hij. 'Soms kan een algoritme al jaren niet meer sneller. Dan heb je twee opties. Of je probeert te bewijzen dat de optimale oplostijd al is bereikt, of je kijkt of er toch iets beters bestaat. Ergens moet een barrière zitten: tot hier en niet sneller. Ik ben hard aan het proberen om te laten zien dat die barrière nog niet is bereikt.' Maar P vs. NP is daarmee nog niet opgelost.

Vervulbaar of niet?

In plaats van proberen te bewijzen dat NP hetzelfde is als P, kun je ook proberen om te bewijzen dat ze níét gelijk zijn. Misschien zijn de problemen in NP wel veel moeilijker dan de problemen in P. Iemand die dat probeert aan te tonen, is Harry

EEN MILJOEN VOOR DE OPLOSSING

Op zoek naar eeuwige roem én een grote zak geld? Buig u dan eens over een van de grote onopgeloste hersenkrakers in de wiskunde, de zogenoemde Millenniumproblemen. Rond de eeuwwisseling loofde het Amerikaanse Clay Mathematics Institute 1 miljoen dollar uit aan ieder die een van de zeven mysteries weet te ontrafelen. Een daarvan is het P vs. NP-probleem. Tot nog toe is er nog maar één millenniumprobleem opgelost: het zogenoemde vermoeden van Poincaré, uit 1904.

Dit artikel is uitsluitend voor intern gebruik binnen: Centrum Wiskunde & Informatica

Publicatie : New Scientist
Datum : 31 dec 2021
cm2 : 2568
Pagina : 64
AVE : € 13338,00
Regio : Nederland
Frequentie : 11x per jaar
Oplage : 15000

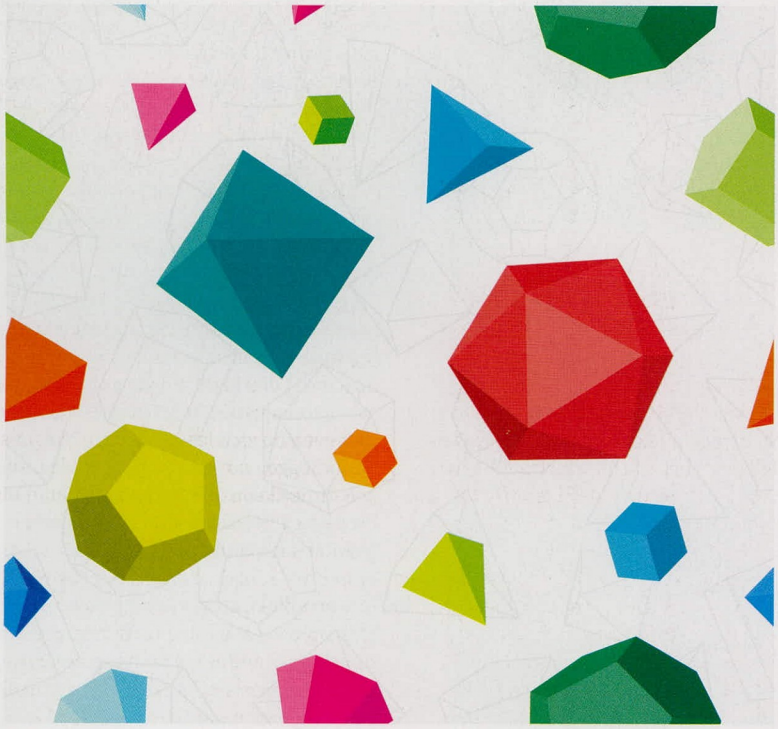
Buhrman, hoogleraar wiskunde en informatica, verbonden aan de Universiteit van Amsterdam en het Centrum Wiskunde & Informatica (CWI) in Amsterdam.

Net als Nederlof zoekt Buhrman naar het beste algoritme voor specifieke problemen. 'We proberen daarbij een bovengrens en een ondergrens te stellen', zegt Buhrman. De bovengrens voor een probleem krijg je door een algoritme te ontwikkelen dat een bepaalde looptijd heeft. Wanneer het algoritme dan het probleem oplost, is die looptijd meteen een bovengrens: de oplossing zal nooit nóg meer tijd kosten. Wanneer je met een algoritme een ondergrens vindt, zal geen enkel ander algoritme het probleem sneller kunnen oplossen dan de looptijd van dat algoritme. Waar Nederlof probeert de bovengrens van de looptijd te verlagen, probeert Buhrman de ondergrens te verhogen. Want als de ondergrens van de looptijd van een NP-volledig probleem bijvoorbeeld exponentiële tijd is – oftewel: de looptijd is altijd veel langer dan polynomiale tijd – dan weet je dat P niet gelijk is aan NP.

Buhrman kijkt daarbij naar een ander NP-volledig probleem dan het handelsreizigersprobleem, namelijk het vervulbaarheidsprobleem. Dat gaat over wat waar kan zijn binnen de logica. Een voorbeeld is: 'Het regent of de zon schijnt niet.' Die zin is waar als het regent of als de zon niet schijnt. Als zo'n stelling waar kan worden, noemen we die vervulbaar. De zin 'het regent en het regent niet' kan nooit waar zijn, en is dus ook niet vervulbaar.

Het snelste algoritme tot nu toe probeert voor elk element van zo'n zin, elke variabele, de waardes waar en onwaar uit. Vervolgens controleert het of de zin in zijn geheel waar is. Elke extra variabele verdubbelt de looptijd, die dus exponentieel is, legt Buhrman uit. En misschien is een verdubbelend aantal oplosstappen voor het vervulbaarheidsprobleem wel het best haalbare. Buhrman: 'Dat is wat we de sterke exponentiëletijdhypothese of de SETH noemen. Als het vervulbaarheidsprobleem niet sneller kan dan exponentiële tijd, dan is naast de SETH ook gelijk bewezen dat P niet gelijk is aan NP.'

Nederlof probeert tegenwicht te bieden aan de SETH. 'Veel mensen zijn het erover eens dat P niet gelijk is aan NP, maar ook steeds meer mensen hangen de SETH aan. Ik zie mijn onderzoek als een naïeve poging om een gat in de SETH te slaan. Want wat is het argument dat het niet sneller kan? Alleen dat we het al vijftig jaar geprobeerd hebben en het nog steeds niet is gelukt. Maar algoritmen blijven ons verbazen, concludeer ik uit de geschiedenis. Soms staat een algoritme al heel lang, maar blijkt het toch nog iets slimmer te kunnen. Dat probeer ik ook voor elkaar te krijgen.'



ISTOCK

'SPECIFIEKE ALGEBRAÏSCHE PROBLEMEN MET EEN LINK NAAR P VS. NP 'VERTALEN' WE NAAR EEN GEOMETRISCHE VORM'

3D-figuur

Een handjevol onderzoekers zoekt de oplossing in een andere richting: de geometrische complexiteitstheorie. Informaticus Jeroen Zuiddam van de Universiteit van Amsterdam is er daar een van. 'In de geometrische complexiteitstheorie kijken we vanuit een nieuw kader naar hetzelfde P vs. NP-probleem', zegt hij.

Bij P vs. NP proberen computers problemen op te lossen. 'De klassieke versie van P vs. NP gaat over een krachtig, abstract

Dit artikel is uitsluitend voor intern gebruik binnen: Centrum Wiskunde & Informatica

Publicatie : New Scientist
Datum : 31 dec 2021
cm2 : 2568
Pagina : 64
AVE : € 13338,00
Regio : Nederland
Frequentie : 11x per jaar
Oplage : 15000

ISTOCK

QUANTUM ALS OPLOSSING

Terwijl klassieke computers al jarenlang P- en NP-problemen proberen te kraken, kijkt Harry Buhrman, hoogleraar informatica verbonden aan de Universiteit van Amsterdam en het Centrum Wiskunde & Informatica in Amsterdam, ook naar de volgende generatie: quantumcomputers. Die horen sommige taken sneller te kunnen verrichten dan klassieke computers. Als een quantumcomputer een NP-volledig probleem snel oplost, zijn P en NP dan gelijk? 'Strikt genomen niet', zegt Buhrman. 'Het P vs. NP-probleem vraagt om een snel algoritme dat werkt op een klassieke computer. Maar alle vragen over P en NP die we tot nu gesteld hebben voor gewone computers, kunnen we ook stellen voor quantumcomputers. In plaats van P hebben we het dan over de quantumversie van P: problemen die quantumcomputers in polynomiale tijd kunnen oplossen.' Kunnen we dan wel binnenkort aantonen dat quantum-P gelijk is aan NP? Waarschijnlijk niet, zegt Buhrman. 'We verwachten niet dat er een NP-volledig probleem gaat zijn dat de quantumcomputer snel oplost.'

model van computers die met bits werken, oftewel nullen en enen. Dat laten wij los,' zegt Zuiddam. Hun techniek gebruikt namelijk een zogenoemd algebraïsch model van berekenen. 'Dat betekent dat je werkt met gehele getallen – in plaats van nullen en enen – die je kunt optellen en vermenigvuldigen. In de algebraïsche wereld kunnen we een soortgelijk probleem als P vs. NP formuleren.'

De nieuwe aanpak maakt daarna ook nog een sprong naar de geometrie, een tak van de wiskunde die zich bezighoudt met vormen en hun eigenschappen. 'De specifieke algebraïsche problemen die een link hebben met P vs. NP 'vertalen' we naar een geometrische vorm; denk aan een 3D-figuur. Daar kun je vervolgens mee gaan spelen. Je kunt er technieken uit de meetkunde op loslaten om eraan te rekenen.' De oplossing die je vervolgens vindt, kun je 'terugvertalen' naar het oorspronkelijke probleem. Zo zou je, via de algebra en de meetkunde, een informaticaprobleem kunnen oplossen.

Helaas is die 'terugvertaling' niet eenvoudig: er bestaat geen een-op-eenrelatie tussen de algebraïsche problemen en P vs. NP. Een oplossing voor P vs. NP zal dus nog wel even op zich laten wachten, volgens de grondlegger van deze methode, de Indiaas-Amerikaanse informaticus Ketan Mulmuley. Die zei tien jaar geleden dat hij gelooft dat het nog wel honderd jaar kan duren voordat de aanpak het P vs. NP-probleem oplost, als dat al ooit gaat gebeuren. Sindsdien is er weinig vooruitgang geboekt.

Ook met andere aanpakken zijn we ondanks onze steeds snellere computers na vijftig jaar niet veel verder met het vinden van het antwoord op de vraag: is P gelijk aan NP? Het is twijfelachtig of de grootheden van de conferentie zelf nog het verlossende bewijs zullen meemaken. Misschien zullen we wel nooit weten of NP-problemen wel of niet snel oplosbaar zijn. Het P vs. NP-probleem zelf is dat in elk geval niet. ■

Dit artikel is uitsluitend voor intern gebruik binnen: Centrum Wiskunde & Informatica