50 jaar Nederlandse algoritmen

Een kleine greep t.g.v. Algoritmen Alom,
Spoorwegmuseum, Utrecht, zaterdagmiddag 18 april 2009
http://www.algoritmenalom.nl

Nederlandse wiskundigen vieren het feit dat 50 jaar geleden het eerste Nederlandse algoritme het daglicht zag. Een algoritme is een rekenrecept waarmee bepaalde problemen kunnen worden opgelost. Zo bestaan er algoritmen voor veilig elektronisch betalingsverkeer, voor het verbeteren van dienstregelingen en voor het reconstrueren van de evolutie van de mens uit genetische data. Deze drie problemen komen uitgebreid aan bod op Algoritmen Alom, een publieksmiddag over algoritmen in het Spoorwegmuseum te Utrecht (informatie en aanmelden: www.algoritmenalom.nl). Hieronder volgt een kleine greep algoritmen uit de afgelopen vijftig jaar waaraan Nederlanders een grote bijdrage hebben geleverd.

- **1959. Kortste pad. E.W. Dijkstra**
  (A note on two problems in connexion with graphs. Numerische Mathematik, 1 (1959) 269–271)
  Het gaat om: het vinden van een kortste pad van A naar B in een netwerk. Dit algoritme zit in systemen als TomTom.
  zie verder: http://nl.wikipedia.org/wiki/Kortstepadalgoritme

- **1968. AutoMath. N.G. De Bruijn**
  (AUTOMATH, a language for mathematics. T.H. Report 68-WSK-05, TU Eindhoven)
  Het gaat om: de verificatie van formeel opgeschreven wiskundige bewijzen met behulp van een computer. In de jaren zestig was dit een volstrekt nieuwe en vaak onbegrepen gedachte. Tegenwoordig maken pakketten als Isabel en COQ dergelijke verificaties mogelijk. Nederlanders werken aan deze ontwikkelingen actief mee.
  zie verder: http://www.win.tue.nl/automath/

- **1982. LLL. A.K. Lenstra, H.W. Lenstra, L. Lovász**
  (Factoring Polynomials with Rational Coefficients. Math. Ann. 261 (1982) 515–534)
  Het gaat om: het vinden van een stel speciale punten in een hoogdimensionaal rooster. Een rooster is een zeer regelmatig stel punten in bijvoorbeeld de ruimte of het vlak—denk aan de hoekpunten van vierkante tegels die het vlak bedekken. Dit algoritme is heel breed toepasbaar. Het kan bijvoorbeeld worden gebruikt om veeltermen te ontbinden in factoren en om bepaalde optimaliseringsproblemen te lijf te gaan. Het wordt zelfs in GPS systemen toegepast.
  zie verder: http://en.wikipedia.org/wiki/+
  Lenstra-Lenstra-Lovasz_lattice_reduction_algorithm

- **1988. Discrete problemen. M. Grötschel, L. Lovász, A. Schrijver**

  (Geometric algorithms and combinatorial optimization, Springer-Verlag, Berlin, 1988)

  Het gaat om: optimalisatie bij zogenaamde discrete problemen met meetkundige methoden. Deze discrete problemen, zoals het vinden van een kortste route langs verscheidene steden en het samenstellen van een goedlopend treinrooster, zijn onderwerp van actieve studie in Nederland. Schrijver en zijn medeauteurs ontdekten dat de ellipsoïdemethode, een meetkundige techniek die oorspronkelijk bedacht was voor andersoortige problemen, ook kon worden toegepast op discrete problemen. Naast de methoden uit het genoemde boek droegen vele activiteiten in het land op andere wijze bij aan goede strategieën, zoals heuristische algoritmen en speurtochten naar bijna optimale oplossingen.
  zie verder: `http://en.wikipedia.org/wiki/Combinatorial_optimization`

- **1992. Lineaire vergelijkingen. H.A. van der Vorst**

  (BI-CGSTAB: A fast and smoothly converging variant of BI-CG for the solution of nonsymmetric linear systems. SIAM J. Sci. Stat. Comput. 13 (no.2, 1992), 631–644)

  Het gaat om: het numeriek oplossen van grote stelsels lineaire vergelijkingen. Veel problemen uit de natuurwetenschappen zijn in eerste benadering te herleiden tot enorme stelsels lineaire vergelijkingen. Deze stelsels zijn zo groot dat het klassieke algoritme van de Duitse wiskundige Gauß niet snel genoeg tot het gewenste resultaat leidt. Van der Vorsts methode is een van de meest gebruikte algoritmen om zo'n groot stelsel toch numeriek op te kunnen lossen. Numeriek betekent hier dat de getallen in de oplossing met een naar wens vast te stellen aantal cijfers achter de komma worden bepaald. (Het tegenovergestelde, waarbij de getallen precies bepaald worden, heet exact.) Zijn artikel daarover is het meest geciteerde artikel uit de wiskundige literatuur van de jaren negentig. BI-CGSTAB staat voor Stabilized Bi-Conjugate Gradient method.
  zie verder: `http://www.netlib.org/linalg/html_templates/report.html`

- **1993. Getallen ontbinden. A.K. Lenstra, H.W. Lenstra**

  (The development of the number field sieve. Lecture Notes in Math. (1993) 1554. Springer-Verlag)

  Het gaat om: De getallenlichamenzeef (GNFS) is het efficiëntste algemeen bekende algoritme voor het ontbinden in factoren van getallen met meer dan 100 cijfers. Dat wil overigens niet zeggen dat de getallenlichamenzeef echt efficiënt is; zou dat wel zo zijn, dan zouden veel cryptografische systemen onveilig worden.
  zie verder: `http://en.wikipedia.org/wiki/General_number_field_sieve`

- **1995. Punten tellen. R. Schoof**

  (Counting points on elliptic curves over finite fields. Journal de Théorie des Nombres de Bordeaux, 7 (1995) 219–254)

  Het gaat om: het tellen van punten op elliptische krommen. Een elliptische kromme

bestaat uit alle oplossingen van een bepaald soort veeltermvergelijking in twee onbekenden. Na de bekende kegelsneden als de parabool en hyperbool, zijn dit de eenvoudigste krommen die met veeltermen beschreven kunnen worden. Schoof heeft laten zien dat het aantal oplossingen efficiënt te berekenen is. Op elliptische krommen gebaseerde gegevensbeveiliging is geschikt voor gebruik in kleine apparaten met weinig rekenkracht zoals mobiele telefoons, omdat de geheime sleutel die hiervoor gebruikt wordt veel kleiner mag zijn dan in andere systemen. Aan efficiënt rekenen met elliptische krommen wordt in Nederland nog steeds veel aandacht besteed.
zie verder: `http://en.wikipedia.org/wiki/Schoof's_algorithm`

- **1995. Datacompressie. F.M.J. Willems, Yu. M. Shtarkov, T.J. Tjalkens**
(The context-tree weighting method: Basic properties IEEE Trans. Inform. Theory 41 (1995) 653–664)
Het gaat om: het indikken (comprimeren) van gegevens zonder verlies van informatie. Om gegevens op te slaan met zo min mogelijk megabytes worden deze vaak gecomprimeerd. Comprimeren kan bijvoorbeeld door van alle woorden in een tekst de klinkers weg te gooien. Maar dan gaat informatie verloren, want "gooien" ziet er gecomprimeerd hetzelfde uit als "gaan". In het algoritme van Willems, Shtarkov en Tjalkens gaat geen informatie verloren. Het is wereldrecordhouder bij de compressie van natuurlijke tekst.
zie verder: `http://en.wikipedia.org/wiki/Context_tree_weighting`

- **1996. Robots bewegen. L.E. Kavraki, P. Svestka, J.C. Latombe, M.H. Overmars**
(Probabilistic roadmaps for path planning in high-dimensional configuration spaces. IEEE Transactions on Robotics and Automation 12 (1996) 566–580)
Het gaat om: het bewegen van een robot. Gegeven een robot in een bepaalde positie, hoe komt die in een andere, gewenste positie? Deze vraag is opgelost met behulp van een zeer algemene methode die in de praktijk uitstekende strategieën berekent. Veel andere vragen van meetkundige aard zijn ook door de groep van Overmars met succes aangepakt.
zie verder: `http://en.wikipedia.org/wiki/Motion_planning`

- **2003. Differentiaalvergelijkingen. M. van der Put, M. Singer**
(Galois Theory of Linear Differential Equations. Grundlehren der mathematischen Wissenschaften, 328, Springer 2003)
Het gaat om: het automatisch exact oplossen van differentiaalvergelijkingen. Veel continue processen, zoals de beweging van een gewicht aan een veer, worden wiskundig beschreven door differentiaalvergelijkingen. Vaak worden die niet exact opgelost, maar wordt een benadering van de oplossing gevonden. Van der Put en andere Nederlanders hebben substantieel bijgedragen aan algoritmen die vaststellen of bepaalde typen differentiaalvergelijkingen een exacte oplossing hebben binnen een welomschreven verzameling functies.
zie verder: `http://en.wikipedia.org/wiki/Differential_Galois_theory`

- **2007. Symmetrie in het groot. M.A.A. van Leeuwen**

  (Computing Kazhdan-Lusztig-Vogan polynomials for split E_8. Nieuw Archief voor de Wiskunde 9 (2008) 113–116)

  Het gaat om: grote berekeningen aan de grootste exceptionele Lie-groep. Fysici verklaren de wereld graag aan de hand van groepen van symmetrieën. Dat geeft aanleiding tot expliciete vragen over verschijningsvormen van die symmetrieën, waar met algoritmen een antwoord op gevonden kan worden. Nederlandse wiskundigen hebben daar hun steentje aan bijgedragen. Dit werk culmineerde in de completering van een bijna niet haalbaar geachte berekening aan de grootste exceptionele Lie-groep, meestal aangeduid met E_8, die een wereld van 248 dimensies vertegenwoordigt. Andere bijdragen van Nederland zijn algoritmen om met deze groepen van symmetrieën te rekenen in softwarepakketten als LiE, GAP en Magma.

  zie verder: `http://www.liegroups.org/`

Voor iets meer achtergrond van het begrip algoritme en aanmelding voor de middag Algoritmen Alom, zie `http://www.algoritmenalom.nl`