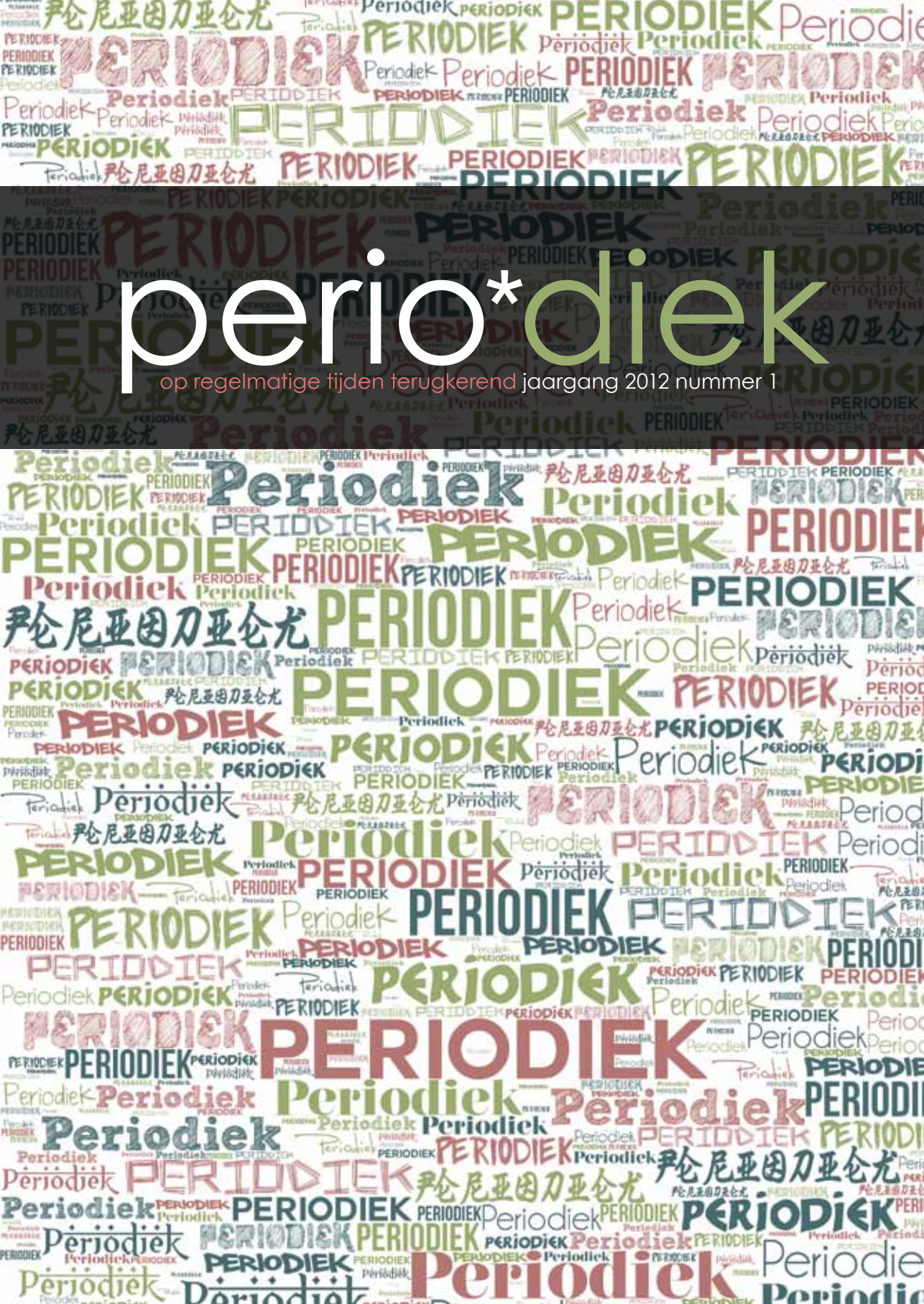
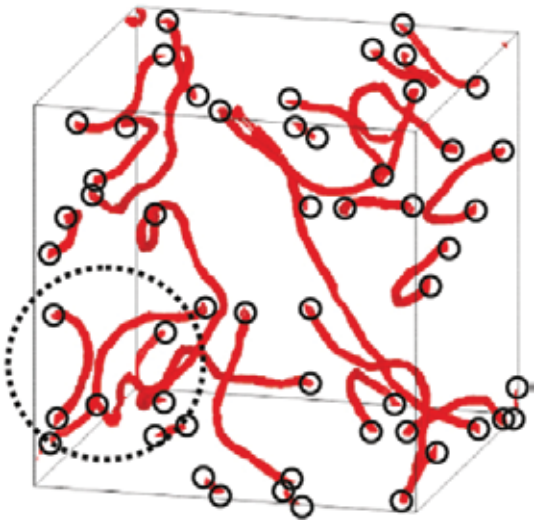
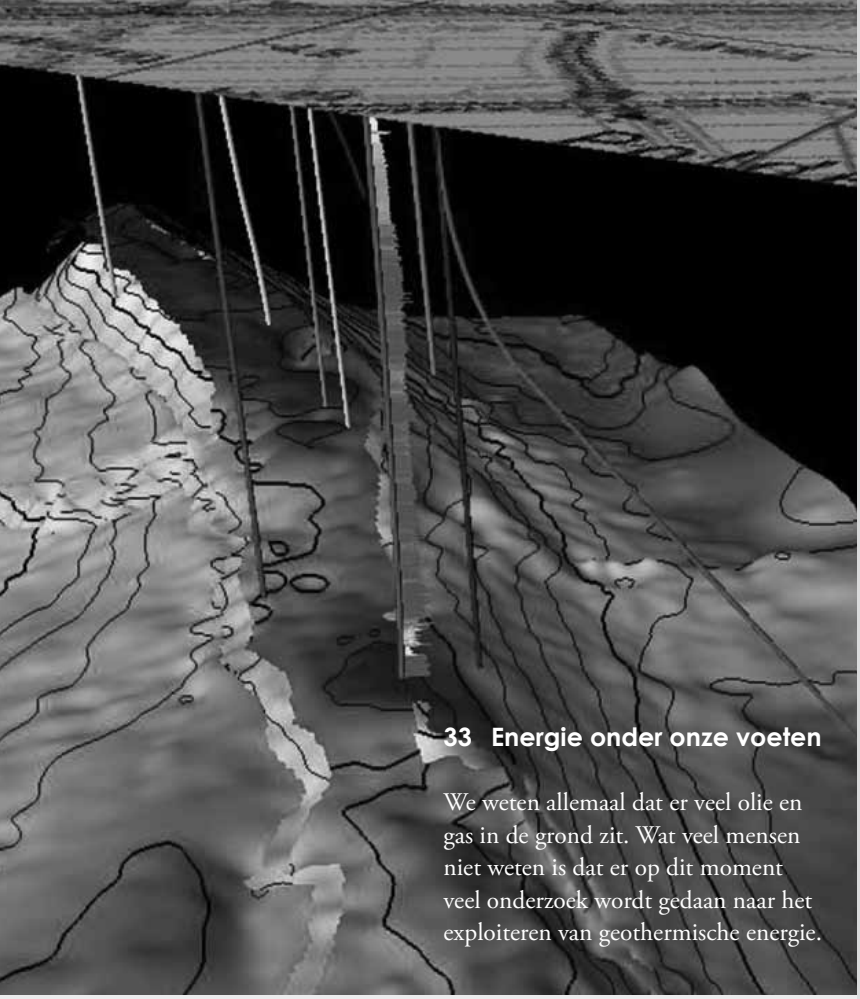

perio*diek
op regelmatige tijden terugkerend jaargang 2012 nummer 1

Inhoud

En verder





33 Energie onder onze voeten

We weten allemaal dat er veel olie en gas in de grond zit. Wat veel mensen niet weten is dat er op dit moment veel onderzoek wordt gedaan naar het exploiteren van geothermische energie.

Van de redactie

Voor je ligt de nieuwe Periodiek. Dit is tevens de eerste periodiek waarin we stukken hebben gepubliceerd die meedingen naar het winnen van een van drie Kindle's in de Periodiek schrijfwedstrijd. Je kunt deze stukken herkennen aan de speciale deelnemer schrijfwedstrijd banner. Lijkt het je leuk om ook mee te doen, kijk dan eens naar onze advertentie op pagina 32 of kijk op schrijfwedstrijd.fmf.nl. Deze perio staat ook in het teken van een speciale fotozoekplaatjes breinwerk. We hebben deze dan ook speciaal als centerfold geplaatst zodat je hem makkelijk mee kan nemen op je zoektocht naar alle locaties. Verder hebben we natuurlijk geprobeerd jullie een leuk aantal stukken voor te schotelen. Als commissie zijn we altijd op zoek naar versterking, lijkt het je leuk om te leren lay-outen, vind je het leuk om stukken te schrijven, of lijkt het je simpelweg leuk om in de redactie plaats te nemen. Neem dan contact met ons op. Dan rest mij verder nog jullie veel leesplezier te wensen!

— *Bart*

Redactie Bart Visser, Herbert Kruitbosch, Paulus Meessen, Armin Palavra.

Scribenten Coen Pijpker, Ivar Postma, Tim van der Beek, Bruno Carpentieri, Wouter Lueks, Arnette Vogelaar, Kasper Duivenvoorden.

Met dank aan Corine Meinema.

Adverteerder ASML (p. 6), Philips (p. 28), Schut (p. 36).

Ook adverteren? Neem contact op met bestuur@fmf.nl.

Oplage 1200 stuks

Druk Scholma

ISSN 1875-4546

De Periodiek is een uitgave van de Fysisch-Mathematische Faculteitsvereniging en verschijnt vijf keer per jaar. Eerder uitgebrachte Periodieken zijn na te lezen op perio.fmf.nl. De redactie is te bereiken via perio@fmf.nl.

In het nieuws

Goedkopere manier om grafeen te maken

Grafeen is erg sterk en kan goed elektriciteit geleiden, vandaar dat het ook geschikt is voor de halfgeleiderindustrie. Een nieuwe productiemethode kan de toepassing ervan in deze industrie bespoedigen. Wetenschappers uit Zuid-Korea en de VS werkten samen aan de nieuwe methode die in staat is om goedkoop grafeen in grote hoeveelheden te maken, daarnaast is de kwaliteit van het materiaal ook nog eens beter. Het proces bestaat uit het in een draaiende trommel stoppen van grafiet met droogijs, de vaste vorm van CO_2. Hierdoor vliegen er splinters van het grafiet die in een bad met chemicaliën komen, waardoor de splinters splitsen in losse grafeenlagen. Door deze lagen vervolgens te verhitten tot 900 graden en te behandelen met andere stoffen, kunnen grote aaneengesloten vellen grafeen gemaakt worden.

pnas.org

Sneller dan licht claim waarschijnlijk meetfout

Volgens het CERN stapelt het bewijs zich op dat neutrino's zich gewoon volgens de geldende natuurwetten gedragen. Wetenschappers hebben een nieuw neutrino-exerperiment gehouden genaamd Icarus, in tegenstelling tot het OPERA expermiment werd er nu geen anomalie gevonden. Mogelijk is de onterechte claim gebaseerd op een meetfout.

cern.ch

Quantum-informatie blijft behouden bij kopiëren

Wetenschappers van de universiteit van Calgary hebben aangetoond dat het mogelijk is om uit imperfecte klonen van een foton het origineel te regenereren. De informatie van quantumsystemen blijft dus behouden bij kopieën hoewel perfect kopiëren niet mogelijk is. Er is nu echter een praktische methode ontworpen op basis van fotonen die in staat is de originele staat uit gebrekkige kopieën te herstellen.

Phys. Rev. Lett.

Kerncentrales waterstof laten produceren

De huidige nucleaire centrales kunnen op milieuvriendelijke wijze waterstof produceren. Toekomstige nucelaire installaties kunnen worden geoptimaliseerd voor het elektrolyseproces. Op dit moment wordt de meeste waterstof geproduceerd in de olie- en gaswinning, als bijproduct wordt CO2 geproduceerd. Kerncentrales zouden op milieuvriendelijke wijze waterstof kunnen produceren door elektrolyse toe te passen op de geproduceerde stoom. Dit zou dan vooral in de daluren moeten gebeuren als de vraag naar elektriciteit fors daalt. Voor de nieuwe nog te bouwen kerncentrales zijn er nog meer mogelijkheden om op een groene en relatief goedkope wijze waterstof te produceren. Politiek gezien is dit een interessante methode aangezien zowel de CO_2 uitstoot als de afhankelijkheid van olie wordt verminderd.

tweakers.net

Breinimplantaat kan vingerbewegingen simuleren

Wetenschappers zijn er in geslaagd om de fijne motoriek van de hand na te bootsen door de benodigde hersensignalen op te vangen met een hersenimplantaat. Daarmee worden dergelijke chips steeds preciezer. Bij het onderzoek werd gebruik gemaakt van apen, die een chip geïmplanteerd kregen in het hersengebied dat voor de aansturing van de spieren zorgt. De apen werden gestimuleerd tot vingerbewegingen, waarna de hersensignalen werden opgevangen door het implantaat. Het signaal werd vervolgens doorgestuurd naar een robothand die vervolgens op dezelfde wijze be-

Leuke nieuwtjes uit de wondere wereld der wetenschap

gon te bewegen als de aap zelf. Op dit moment zijn de gesimuleerde bewegingen nog niet zo precies als die van een echte hand, dit komt doordat de chip slechts de signalen van 200 neuronen opvangt, waar bij de aansturing van een echte hand honderdduizend neuronen betrokken zijn. Nieuwere implantaten moeten in staat zijn meer signalen tegelijkertijd op te kunnen vangen om zo de robotarm nauwkeuriger te laten bewegen.

tweakers.net

H_2-auto's

Het zijn misschien wel de auto's van de toekomst, auto's die rijden op basis van waterstof. Er is echter wel een praktisch probleem, hoe sla je deze waterstof op? Amerikaanse en Japanse chemici zouden wel eens een potentiële oplossing bedacht kunnen hebben, ze suggeren dat auto's ook op mierenzuur kunnen rijden. Het probleem van waterstofgas is het feit dat het onder hoge druk opgeslagen moet worden om het ontsnappen ervan tegen te gaan. Een manier om dit probleem tegen te gaan is door het waterstofgas tijdelijk op te slaan in mierenzuur (HCO_2H). Mierenzuur ontstaat uit, en is om te zetten in, CO_2 en H_2. De techniek die de wetenschappers ontdekt hebben is in staat om praktisch mierenzuur te maken en om te zetten.

nrc.nl

Eerste medicijn op microchip succesvol in mens getest

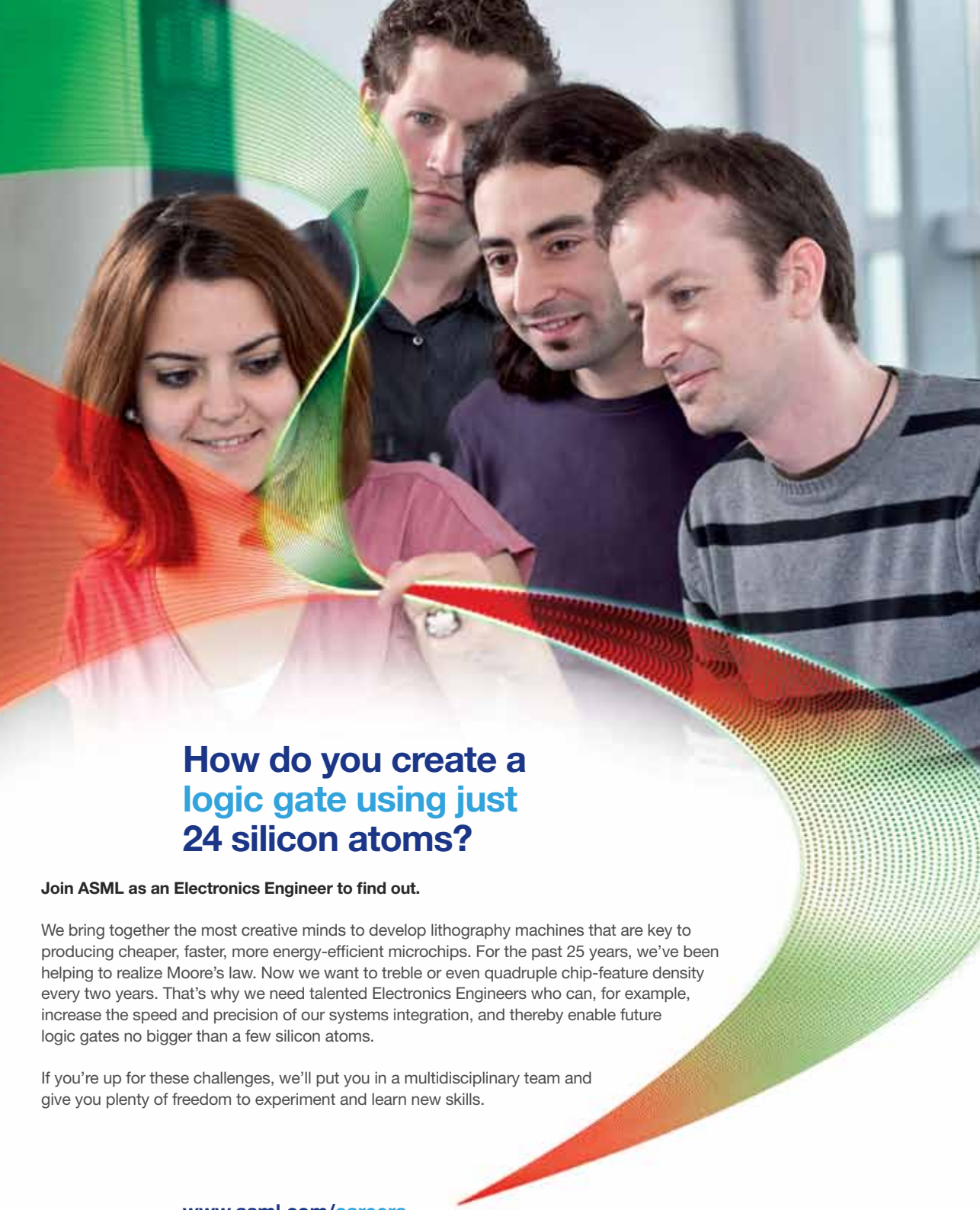
De eerste draadloos bestuurbare microchip die dagelijks een dosis medicijnen tegen botontkalking afgeeft is, is succesvol getest in mensen. In de chip wordt elke dosis van het medicijn apart verpakt in een kleine ruimte ter grootte van een speldenprik en zijn bedekt met een dun laagje platina en titanium. Dit laagje smelt als er een kleine elektrische stroom gaat lopen, waardoor het medicijn vrijkomt. Aangezien de chips programmeerbaar zijn kan van tevoren elke dosis worden bepaald.

Science Translational Medicine

Geneticus Clevers nieuwe president KNAW

Arts en geneticus Hans Clevers is officieel gekozen als nieuwe president van de Koninklijke Nederlandse Akademie van Wetenschappen (KNAW). Hij volgt per 1 juni Robbert Dijkgraaf op. Clevers zal voor vier jaar het presidentschap op zich nemen. Vanuit zijn nieuwe functie zal Clevers proberen, gezien zijn status als gelauwerd wetenschapper, een stempel te drukken op de relatie tussen de wetenschap en de maatschappij. Naast zijn nieuwe functie blijft Clevers onderzoek doen aan het Universitair Medisch Centrum in Utrecht.

knaw.nl



How do you create a logic gate using just 24 silicon atoms?

Join ASML as an Electronics Engineer to find out.

We bring together the most creative minds to develop lithography machines that are key to producing cheaper, faster, more energy-efficient microchips. For the past 25 years, we've been helping to realize Moore's law. Now we want to treble or even quadruple chip-feature density every two years. That's why we need talented Electronics Engineers who can, for example, increase the speed and precision of our systems integration, and thereby enable future logic gates no bigger than a few silicon atoms.

If you're up for these challenges, we'll put you in a multidisciplinary team and give you plenty of freedom to experiment and learn new skills.

www.asml.com/careers

ASML

For students who think ahead

Van de extern

DOOR **COEN PIJPKER**

Nadat twee van mijn collega's al de kans hebben gekregen om een stukje voor de Periodiek te schrijven, is mij nu deze eer toebedeeld. Hieronder zal ik een kort verhaal vertellen over wie ik ben en wat ik zoal doe als extern zijnde.

Mijn naam is Coen Pijpker. In 2007 ben ik begonnen aan mijn bachelor natuurkunde, welke ik in 2010 met goed gevolg afrondde, om daarna aan een master in de richting experimentele natuurkunde te beginnen. Na een jaar van deze master en twee serieuze commissies leek het mij leuk om een jaar bestuur te doen. Inmiddels vervul ik de functies van commissaris-extern en vicevoorzitter.

Wat doet een commissaris-extern nou zoal de hele dag? De extern kun je ook wel de bedrijvencommissaris van het bestuur noemen: al het contact met bedrijven van de vereniging loopt via hem. De grootste taak is dan ook het verlengen van contracten met bestaande sponsoren en het binnenhalen van nieuwe sponsoren. Daarnaast zorgt de extern, als voorzitter van de Huygenscommissie, er ook voor dat alle excursies en lezingen plaatsvinden. Naast commissaris-extern, mag ik als vicevoorzitter ook nog een klein beetje toezicht houden op de voorzitter, en hem vervangen indien nodig.

Er is inmiddels al weer een boel gebeurd sinds de bijdrage van Ricardo in de vorige Periodiek. Onze dappere archivarissen hebben zich door een enorme berg materiaal gewerkt en het archief is nu volledig opgeruimd! Deze leeuwentaak gaf de ruimte aan ons als bestuur om de vectorruimte eens goed onder handen te nemen. De vectorruimte is inmiddels door de comcie ingericht als werkkamer en huisvest nu ook de server. Dit gaf groen licht aan een opruimsessie van de NSFW, die ook heringericht is. Daarnaast zal de KNOB een facelift krijgen, zodat commissies hier weer prettig kunnen werken.

Naast administratieve en binnenhuisarchitectonische veranderingen zijn er ook nog een boel leuke activiteiten geweest. Zo heeft inmiddels het eerste kerstdiner van de FMF plaatsgevonden in de kantine van het NCC. De kantine werd mooi versierd door de meiscie, waarna er een driegangenmenu geserveerd werd. Daarna vond er een kerstborrel plaats om het kalenderjaar goed uit te luiden. Het nieuwe jaar werd ook goed ingeluid met de nieuwjaarsborrel, waar voor het luttele bedrag van één euro cocktails genuttigd konden worden. Deze borrel werd opgevolgd met activiteiten zoals onze derde ALV; een valentijnsactie van de meiscie; het gaming event; en het actieve-ledendiner. Daarnaast hebben ook de Bèta Bedrijvendagen plaatsgevonden, waar veel leden van de FMF hun toekomstige werkgever kon ontmoeten. Ten slotte was er een sportieve activiteit met Commotie – de studievereniging voor communicatie- en informatiewetenschappen. Daar konden deelnemers onder andere slagbal, trefbal en apenkooi spelen.

Ook de komende tijd zullen er nog veel activiteiten plaats gaan vinden. Zo heeft Huygens een heleboel lezingen en excursies gepland staan tot de zomervakantie. Tevens zullen wij in april afreizen naar Milaan en München met de KBE. Tijdens deze reis zullen er een boel interessante bedrijven en universiteiten bezocht worden, maar ondertussen toch ook genieten van het schoons dat deze steden te bieden hebben. Ik hoop jullie dan ook allemaal terug te zien op een van deze activiteiten. Mocht je nog wat van mij willen weten? Schroom dan niet en spreek me aan in de NSFW!

Kunstig woordgebruik

DOOR **IVAR POSTMA**

Soms zegt een plaatje meer dan duizend woorden. Fotografen, schilders en andere visuele kunstenaars zullen dit beamen. Maar met duizend woorden kun je juist hele leuke plaatjes maken. Vooral als je een computer het werk laat doen.

Het Chinese schrift bestaat uit andere karakters dan het Latijnse schrift. In het Latijnse schrift gebruiken we lettercombinaties om woorden te coderen. Het Chinees heeft geen letters, in plaats daarvan heeft ieder woord een eigen karakter. Deze karakters zijn ontstaan uit simpele tekeningen. De tekeningen zijn door de eeuwen heen erg veranderd en inmiddels is bij de meeste tekens de originele vorm ver te zoeken. Figuur 1 laat zien hoe het karakter voor het woord 'paard' zich heeft ontwikkeld. Van eenherkenbare tekening blijft slechts een abstracte vorm over.

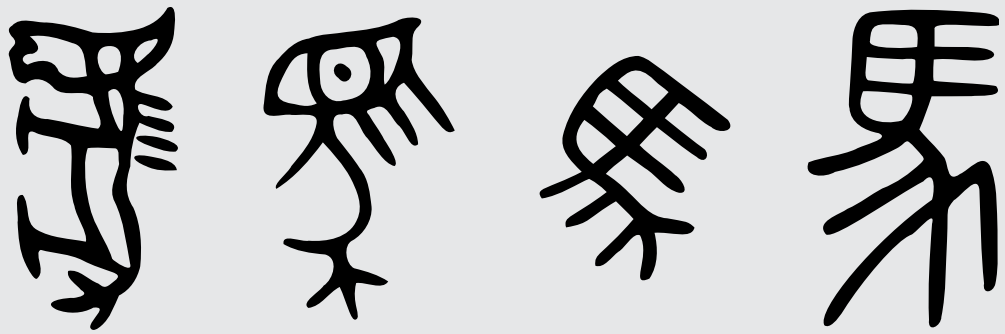
De ontwikkeling van Chinese karakters houdt verband met de kunst van het schoonschrijven, wat ook wel kalligrafie wordt genoemd. Kalligrafie is een eeuwenoude traditie in China. Het is een kunstvorm waarbij kunstenaars proberen om karakters harmonieus of expressief weer te geven. Hierdoor worden karakters visueel aantrekkelijk en drukken ze opeens veel meer uit dan alleen hun originele betekenis.

Het gebruik van tekst in visuele kunst beperkt zich niet tot China en het Chinese schrift. Christelijke monniken in Europa investeerden vaak veel tijd in het mooi opmaken van een tekst. En in de islamitische cultuur zie je ook veel tekst in kunst terug omdat het afbeelden van heiligen daar vaak taboe is. Tekst is dan een goed alternatief om aantrekkelijke plaatjes te maken.

Tegenwoordig wordt tekst vaak in grafische ontwerpen gebruikt. Hierbij gaat het niet alleen meer om het mooi opmaken van karakters, ze kunnen ook gebruikt worden om vormen uit te drukken. Dit is de representationele kalligrafie. Hierin draait het om een samenspel tussen het geheel en de onderdelen, zoals je dat ook ziet bij een mozaïek. In dit geval zijn die onderdelen karakters of letters en is het geheel een vorm of een contour van een object.

Woordenwolk

Omdat veel grafische ontwerpen digitaal gemaakt worden zijn er veel programma's beschikbaar om artistieke effecten na te bootsen. Daarnaast zijn er nieuwe ideeën ontstaan voor grafische ontwerpen die met de hand enorm veel tijd zouden kosten. Een populair



FIGUUR 1 De evolutie van het Chinese karakter voor 'paard'.

FIGUUR 2 Een word cloud gebaseerd op de wikipedia-pagina over de FMF, gemaakt met Wordle [2].

voorbeeld hiervan is de *word cloud* die je vaak op posters ziet. Een word cloud is een manier om grafisch de frequentie van woorden weer te geven. Zo'n plaatje wordt gevormd op basis van een tekst. Ieder uniek woord wordt in de word cloud geplaatst waarbij de grootte van het woord wordt bepaald door het aantal keren dat het in de tekst voor komt. Vaak is een word cloud heel karakteristiek voor een tekst. Zo bevat een word cloud gebaseerd op een tekst over de FMF de grote woorden 'activiteiten', 'vereniging', 'studenten' en 'leden', woorden die de FMF redelijk goed samenvatten (figuur 2).

Op het internet zijn verschillende websites te vinden waar je een eigen word cloud kunt maken, bijvoorbeeld Wordle [2]. Wordle maakt gebruik van een *randomized greedy algoritme* om de woorden te plaatsen. De greedy-eigenschap van het algoritme betekent dat het de grootste woorden als eerste plaatst. En de randomized-eigenschap geeft aan dat het een willekeurige positie kiest om een woord te plaatsen. De woorden worden een vaan een in de cloud geplaatst. Als er bij de plaatsing van een nieuw woord overlap is met een reeds geplaatst woord, dan wordt een nieuwe positie gekozen. Op deze manier veranderen geplaatste woorden nooit meer van positie en kun je een word cloud woord voor-woord opbouwen en breidt de wolk zich steeds verder uit.

Inpakproblematiek

Stel dat je drie weken op vakantie gaat en je kunt slechts één koffer meenemen. Als je al je spulletjes willekeurig in je koffer gooit, dan krijg je hem waarschijnlijk niet dicht. Vaak moet je gestructureerd je kleren opgevouwen stapelen en zelfs dan kan het gebeuren dat het pas bij de vierde poging echt past. Toch is het volume van je spullen in de tussentijd niet afgenomen. Het probleem zit hem dus vooral in de ruimte tussen je spullen. Hoe zorg je ervoor dat er zo weinig mogelijk ruimte tussen je spullen zit? In de wiskunde heet dit een *bin packing* probleem. Gegeven een ruimte en een aantal elementen hoe kan ik de ruimte zo efficiënt mogelijk vullen met de elementen.

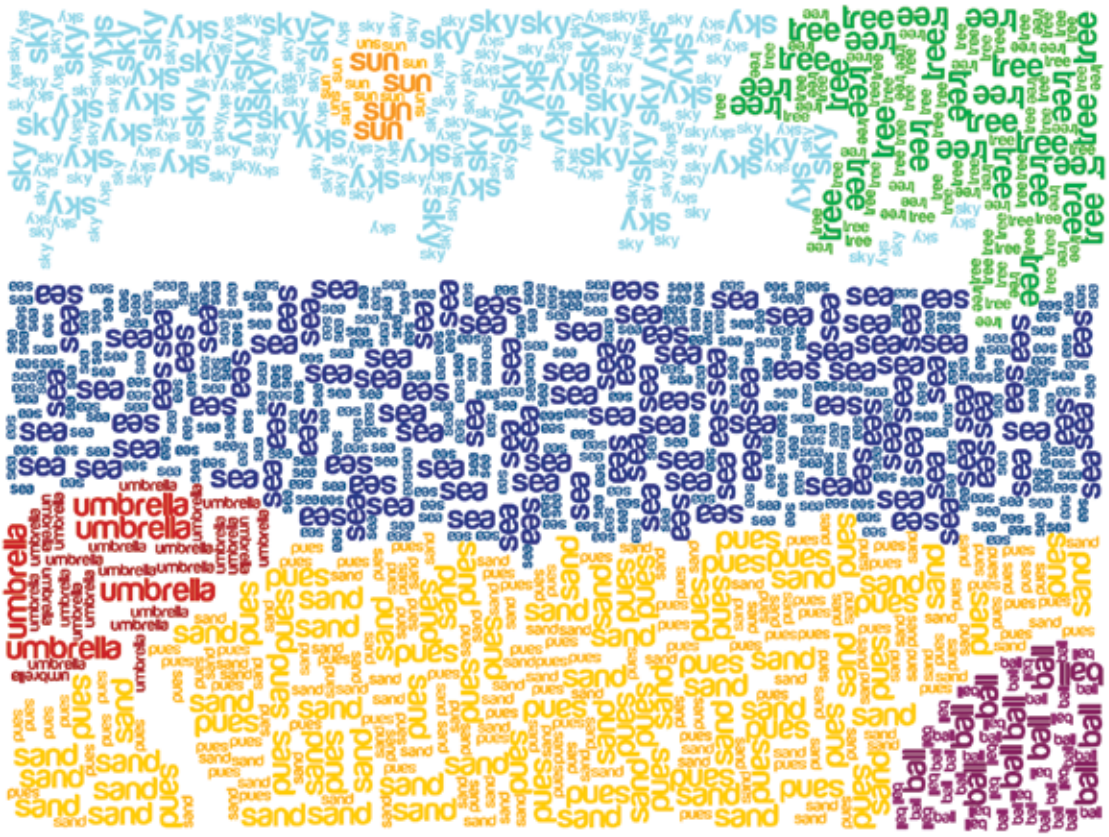
Dit probleem is een np-moeilijk probleem, wat in lekentaal betekent dat het onmogelijk of in ieder geval heel moeilijk is om een perfect efficiënte oplossing voor het probleem te vinden. Dat is waarschijnlijk ook waarom je de spullen in je koffer vier keer moet herstructureren voordat het past. Er is geen aanpak die altijd goed werkt. Wat *packing*-problemen over het algemeen zo lastig maakt is de vaste vorm en grootte van de elementen. Als de grootte van een element variabel is en je een oneindige hoeveelheid elementen hebt, kun je namelijk wel iedere ruimte perfect opvullen. Een mooie illustratie hiervan wordt gegeven door de Sierpinski driehoek (figuur 3). Bij een Sierpin-

FIGUUR 3 Constructie van een Sierpinski driehoek.

ski driehoek wordt een ruimte (de zwarte driehoek) stapsgewijs gevuld met elementen (witte driehoeken). In iedere stap worden zo veel mogelijk elementen geplaatst, als het element nergens meer past wordt het verkleind tot het wel weer past. Bij iedere stap wordt er meer zwart opgevuld totdat er uiteindelijk geen zwart meer over is.

Vormen vullen

Het idee van de Sierpinski driehoek werkt ook voor andere ruimtes en elementen. Ruimtes en elementen hoeven niet eens samenhangend te zijn. Door het randomized greedy algoritme van Wordle een klein beetje aan te passen kunnen we ruimtes gaan vullen met woorden. Het idee van Wordle is dat je ieder woord maar een keer kan plaatsen en dat de grootte vooraf vaststaat. Die twee eisen laten we nu varen. We pakken een willekeurig woord en plaatsen het op een willekeurige plek in de ruimte. Als het woord nergens past verkleinen we het gewoon tot het wel past. Dit herhalen we tot we de vorm van de ruimte die we aan het vullen zijn herkennen. Zoals je kon zien bij de Sierpinski driehoek hoeft niet de hele ruimte gevuld te zijn om een vorm te herkennen. Mensen zijn heel erg goed getraind in het herkennen van vormen. Dat is in dit geval maar goed ook, want als je de gehele ruimte zou vullen verdwijnt ook de witruimte tussen de letters. Je zou de woorden dan helemaal niet meer kunnen lezen.



Grafisch ontwerp

De vormen die opgevuld zijn met woorden kunnen nu gebruikt worden voor het maken van leuke grafische ontwerpen. Zo kun je een herkenbare vorm als een hartje opvullen (zie de inhoudsopgave), maar ook foto's omtoveren in een abstract kunstwerk (zie hierboven). Wie overigens nu denkt dat creatieve kunstenaars binnenkort vervangen zullen worden door computertechnieken zoals deze heeft het mis. Het kiezen van de juiste input en het verwerken van de output zijn de meest belangrijke stappen in het maken van een geslaagd ontwerp. Alleen het tijdrovende en geestdodende werk van het handmatig plaatsen duizenden woorden is nu niet meer nodig. •

NPR

Photorealistic rendering is een tak binnen *computer graphics* waarin wordt geprobeerd beelden te maken die niet van foto's te onderscheiden zijn. Denk bijvoorbeeld aan films die computers voor hun special effects gebruiken. Net als in de schilderkunst zijn er naast deze stroming veel verschillende technieken die proberen andere effecten uit te beelden. In de informatica is dit *non-photorealistic rendering* (NPR). Plaatjes renderen met tekst is hier een voorbeeld van.

Referenties

[1] Erin Silversmith and Micheletb, Ancient Chinese characters project. Wikimedia Commons, http://commons.wikimedia.org/wiki/Commons:Ancient_Chinese_ characters.

[2] Jonathan Feinberg, Wordle. http://www.worlde.net.

[3] Julie Steele and Noah Iliinsky, Beautiful Visualization. O'Reilly Media (2010).

[4] Ivar Postma, Creating Representational Calligrams Through a Word Packing Approach (2012).

Studeren in het buitenland

DOOR **TIM VAN DER BEEK**

Op het moment van schrijven zit ik weer even in Groningen, om vakantie te vieren en familie en vrienden te bezoeken. Na een verder slechts eenmaal onderbroken halfjaar in Frankrijk te hebben gezeten, is het prettig om weer in Nederland overal mensen te zien die een begrijpelijk taaltje spreken. Ook vermakelijk is het om door dat oude, vertrouwde regenweer te fietsen.

Volgende maandag ga ik weer terug naar mijn studieoord: Parijs. Ik woon er in een vrijstaand buitenwijkhuisje, met een Duitse PhD-studente, zij doet iets met *sports management*, en twee Fransen, waarvan de oudste de huisbaas en kunstschilder [1] is. Studeren doe ik wat zuidelijker, aan de *semi-militaire Ecole Polytechnique*, door een enquête tot *"best university of Science and Technology in France"* benoemd. RER B, halte: Lozère, gevolgd door een ellenlange trap het Saclay plateau op. Ik doe er het eerste jaar van een master *en physique des hautes énergies* [2]. De master wordt in samenwerking met de ETH Zürich georganiseerd en draait in één woord samengevat om het CERN: het studieprogramma introduceert de experimentele en theoretische kant van dit slag experimenten.

Een gemiddelde studiedag, waar ik er vreemd genoeg maar drie van in de week heb, want de rest is weekend, begint met een kop koffie en een korte trein- en busrit zuidwaarts, om de traptreden van Lozère te omzeilen. Vervolgens sta ik met een paar voetstappen in het grootste gebouw op de campus: *le Grand Hall*, een hal die naar een ontwerp van kort voor de oliecrisis van

‘73 gebouwd is en die dus in het winterseizoen niet veel warmer is dan de buitenwereld. In de zalen daar volg ik ‘s ochtends hoor- en ‘s middags werkcolleges, o.a. *MAT 568: Géométrie métrique, une introduction avec la relativité générale à l’esprit*, en in het best redelijke, maar vooral goedkope restaurant geniet ik van het avondeten. ‘s Avonds zijn er geregeld voorstellingen, georganiseerd door studenten, zoals cabaret, klassieke muziek, etc. en, op dinsdag, Franse taallessen - die sinds het vertrek van de Serviër Bosco, die elke discussie bombastisch op het Belang van Vrijheid en de Verschrikkingen van Honger in Afrika wist te herleiden, ietwat saaier zijn geworden.

Toch, ondanks dat ik nu in Frankrijk woon, dat mijn huisgenoten Frans zijn, de vrolijke taallessen en Franse colleges die ik volg, is mijn Frans op zijn best roestig te noemen. Eén reden is het fantastische Engels dat iedereen spreekt die ik ontmoet, wat wel tegen de verwachting in is. Daarnaast ben ik op de dinsdagavond *Bôbaravond-Belgisch bierclubavond*, de lokale studentenbar, toch vooral omringd door de vlucht van internationale studenten die op de campus leven.

In de vierdaagse weekenden ben ik doorgaans, na wat studeerwerk, in de stad te vinden. Het is een mooie gelegenheid om een museum te bezoeken - dat is vaak gratis als je een EU-burger en jonger dan 26 bent – *l’Orangerie* en *le musée d’Orsay* zijn aanraders. Of om een jazzcafé in te duiken, zoals *le Duc des Lombards*, waar alles chique en duur is, maar met prachtmuziek. Verder volg ik er nog harmonicalessen bij dhr. Legendre in het 14de - overigens, aan een zekere Selwerdflat II-bewoonster, bedankt voor de harmonica.

Al met al vermaak ik me er prima. En gelukkig heb ik er nog een paar maanden om mijn Frans wat bij te schaven. Het vervolg van mijn studieplan is om volgend jaar verder te studeren aan de ETH Zürich, en daar fatsoenlijk Zwitserduits te leren spreken •

Referenties

[1] letsgiveatry.wordpress.com/2010/12/21/lhomme-qui-ne-parlait-quau-present
[2] hep.polytechnique.edu

An essay

On Higher Education in the Global Digital Economy

DOOR **BRUNO CARPENTIERI**

In the modern global world, the rapid circulation of information, ideas, people and capital is making knowledge even more vital to societies and economies than in the past. A growing number of people perceiving that higher education is absolutely necessary to achieve individual success and in general prosperity. Over a lifetime, a college-educated American earns about twice as much as one who has only a secondary diploma, and a PhD-educated American earns nearly three times as much. In 2007-08, universities contributed nearly 60 billion pounds to the economy of the United Kingdom, and international students and their dependants contributed around 18 billion dollars to the US economy.

These days the health of higher education is somewhat imperilled by the risks inherent in the recession. The financial crisis jeopardises the growth of post-secondary education programs, threatening the pillar concepts of global knowledge. Drastic budget cuts are forcing public universities to raise tuition fees and eliminate tenure programmes for professors, especially in the humanities and arts. Due to costsa-

ving measures, in British higher education "the position of non STEM (science, technology, engineering, maths) subjects is seriously threatened", according to the eminent Oxford historian, Keith Thomas [1]. But the relevance of the humanities is not devalued by the economic crisis. "At the heart of the liberal arts and fundamental to the humanities — and indeed central to much of scientific thought — is the capacity for interpretation, for making meaning and making sense out of the world around us. We are all bombarded with information. Education measured only as an instrument of economic growth neglects the importance of developing such capacities." [2]

Budget declines drive governments to fund risk-free proposals which offer tangible returns on the investments, in preference to basic scientific research with a high degree of adventure. As Carl Sagan explains very well in his book, "The Demon-Haunted World", curiosity-driven research has led to magnificent advances in the past: "Maxwell wasn't thinking of radio, radar and television when he first scratched out the fundamental equations of electromagnetism; Newton wasn't dreaming of space flight or communications satellites when he first understood the motion of the Moon; Roentgen wasn't contemplating medical diagnosis when he investigated a penetrating radiation so mysterious he called it 'X-rays'; Curie wasn't thinking of cancer therapy when she painstakingly extracted tiny amounts of radium from tons of pitchblende; Fleming wasn't planning on saving the lives of millions with antibiotics when he noticed a circle free of bacteria around a growth of mould; Watson and Crick weren't imagining the cure of genetic diseases when they puzzled over the X-ray diffractometry of DNA; Rowland and Molina weren't planning to implicate CFCs in ozone depletion when they began studying the role of halogens in stratospheric photochemistry." [3]. A substantial amount of these astonishing discoveries came out of the universities, and were not the result of targeted research.

However, in spite of the economic problems, disruptive innovation is opening the floodgates of learning, and this has an unstoppable momentum. The price of distributing knowledge is falling ever closer to zero. It started with the Internet and the World Wide Web, which made linkable documents publicly available for free to everyone in the world. Open licensing offered a legal way to freely modify, use and redistribute — without conventional copyright restrictions — all copyrightable works — software, photos, music, and writings — including all forms of educational content. This enormously raised the capability and opportunities offered by the Internet. Community tools, like blogs, wikis, online forums, instant messaging, and Web portals, allow people to collaborate and exchange information online more easily. Universities have adopted learning management systems to centralize and document training programs, and deliver learning content rapidly.

The transition from open software, to open content and to open teaching happens in the twinkling of an eye. Higher education systems are developing plans to promote and increase the use of open access textbooks, e.g., in Florida in 2009. Open access textbooks are digital textbooks that can be accessed online for free and printed at a nominal cost. In 2011, Professor Sebastian Thrun opened an online course on Artificial Intelligence at Stanford to anyone who was interested in participating. He taught the course to around 160,000 students. Those students who achieved a 100% score received an invitation to apply for a Job Placement Program in major companies in the Bay Area. In 2011, MITx started to offer online teaching of MIT courses free of charge, without an admission process. Everyone around the world is given the opportunity to gain a certification of mastery of MIT material. Those who have the ability to demonstrate mastery of the material of a subject can receive, for a modest fee, a credential issued by a not-for-profit body created within the institute.

Open teaching will break the barriers to education and to the traditional concepts of a degree. As soon as big employers start officially accepting these alternative credentials in place of a Bachelors, there will be a flourishing market in open teaching models. This will happen because there is an ever increasing need for knowledge, especially in developing countries the job market is demanding fine-grained labour competence, and students prefer individual, short-term and cost-effective curricula. Sebastian Thrun gave up his teaching position at Stanford this year to found Udacity, a new online university that expands his efforts to a wider range of topics. He hopes that 500,000 students will enroll his seven-week course called "Building a Search Engine."

The mission for universities is much broader than for for-profit competitors in the knowledge industry. It is about "interpretation for making meaning and making sense out of the world around us, combining innovation and interpretation. We need the best of both, and it is universities that best provide them" [2]. However, ignoring the impending transformations of the global knowledge economy might be an error. Some universities are responding by innovating internally e.g. by taking steps to strengthen their graduate and postdoctoral programs, supporting a professional approach to teaching, rewarding good teaching as much as good research, and finding new strategies to sell general education, acquire talented students, offer individual course credentials. The transition may not be straightforward, but it may help to weather the storm and find challenges and opportunities amidst a period of economic uncertainty. What's next ? •

Referenties

[1] Keith Thomas. "What are Universities for?" Times Literary Supplement, May 7, 2010: 13-15.

[2] Catherine Drew Gilpin Faust."The Role of the University in a Changing World", public speech at the Royal Irish Academy, Trinity College, Dublin, June 30, 2010.

[3] Carl Sagan. "The Demon-Haunted World: Science as a Candle in the Dark", Ballantine Books, 1997.

Bruno Carpentieri joined the Institute of Mathematics and Computing Science, University of Groningen, in January 2010 as tenure track assistant professor in the Computational Modelling Group. He grew up in Trani (Italy), and received his bachelor's degree in Applied Mathematics from University of Bari (Italy) and a Ph.D degree in Computer Science from Institut National Polytechnique of Toulouse (France). Bruno began his journey in education and research as post-doctoral researcher at CERFACS Institute in Toulouse (France). He also worked as a teacher and research fellow at Karl-Franzens University in Graz (Austria), and served as a consultant on European projects at CRS4 in Sardinia (Italy). His areas of interests include computer science, matrix computation and numerical analysis, that is the study of algorithms for the problems of continuous mathematics. One significant achievement in his research was the modelling of a full aircraft for radar applications in civil aviation. He currently supervises a PhD student, who started in summer 2011.

Vorig Breinwerk

DOOR **DE REDACTIE**

De winnaar van het vorige breinwerk was Arnette Vogelaar, zij wint het boek “Forbidden Knowledge”. Door crimenele hackers was de online-versie van de encrypted tekst anders dan de gedrukte versie. De vertaling van de gedrukte versie was te vinden door alle letters te substitueren met andere letters volgens een bepaalde sleutels. De vertaling ervan volgt zo. Uiteindelijk stond er een fout in de vraagstelling, waardoor er een antwoord was dat wij, de redactie, zochten en een juist antwoord. Omschreven stond namelijk dat x uniek moet zijn en bedoeld was dat x^y uniek moet zijn. Beide hebben we goed gerekend, en de antwoorden zijn respectievelijk 11 en 50.

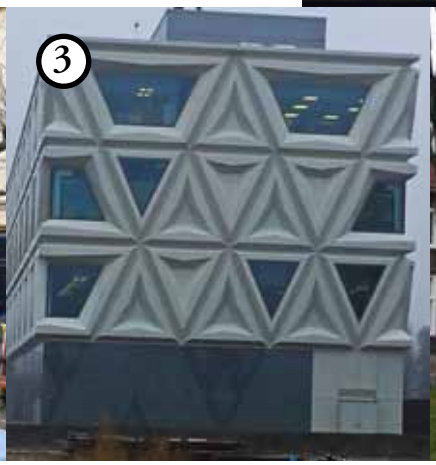
poorten van gevangenissen in vaticaanstad die naast allemaal aardappelsequoias staan zijn belast met bugs. bugs in het programma van de poorten veroorzaaken dat opgesloten misdadigers zon poort kunnen hacken aan de hand van getallen. het getal moet den gevangen misdadiger kunnen schrijven als x tot den macht y maar moet ook exact y nummers lang zijn. illustraties van zulke getallen zijn 32768 dat schrijfbaar is als acht tot de macht vijf maar ook 416777216 dat schrijfbaar is als acht tot de macht acht echter kan een zon x slechts een maal gebruikt worden de bewaarders van de gevangenissen vragen zich af of hun gevangenis veilig bewaakt wordt zodat uitbraakrisicos draagbaar blijven.

welk aantal poorten moeten in zon gevangenis tussen alle misdadigers en de vrijheid zitten zodat de misdadigers nooit kunnen ontsnappen. •

Nieuw Breinwerk

DOOR **CORINE MEINEMA**

Bepaal voor ten minste vier foto´s waar hij genomen is en win een het boek “Groningen verandert 2, Oude en nieuwe stadsgezichten”. Onder de inzendingen met de meeste goede locaties wordt de prijs verloot. Stuur je inzending voor 15 juni op naar perio@fmf.nl •




6


7


9


A


B


E


8


C


F


D


G


I


J

Kan dat ook Anoniem?

DOOR **WOUTER LUEKS**

Jaap is student en houdt wel van een lekkere fles wijn. Deze haalt hij bij de plaatselijke slijterij waar hij ter controle van zijn leeftijd altijd zijn identiteitsbewijs voor een elektronische lezer moet houden. Natuurlijk maakt zo'n elektronische lezer veel minder fouten dan een verkoper. Zijn vriend Paul gaat elke dag sporten. Bij binnenkomst van het sportcentrum houdt hij zijn fitnesskaart voor de kaartlezer zodat hij door het poortje kan. In het nieuwe jaar klaagt Jaap over de verhoging van zijn zorgpremie, terwijl Paul juist zeer content is met de verlaging van zijn premie. Heeft de zorgverzekeraar stiekem gedifferentieerd op basis van de levensstijlen van Jaap en Paul?

Natuurlijk bestaan Jaap en Paul niet echt, en maken zorgverzekeraars voor zover ik weet nog niet op grote schaal onderscheid in premies op basis van levensstijl. Verleidelijk is het echter wel. Door handig te selecteren valt veel geld te besparen. Niet alleen voor zorgverzekeraars is het combineren van informatie interessant, dit geldt ook voor andere instanties, zoals DUO. Alle reizen die studenten met hun OV-chipkaart maken worden sinds 1 januari geregistreerd; je moet immers altijd in- en uitchecken. Dit is natuurlijk een ideaal middel om studenten op te sporen die onterecht een uitwonendenbeurs ontvangen. Hoewel ook dit toekomstmuziek lijkt, gebruiken gemeentes een vergelijkbare aanpak om bijstandsfraude op te sporen [1].

Een uitgebeide discussie over de wenselijkheid van het koppelen van gegevens is zeker belangrijk, maar in dit stukje wil ik me richten op een onderliggend probleem. In de inleiding zagen we hoe informatie over drankgebruik en sportgewoontes opgeslagen worden, terwijl dat voor het doel niet noodzakelijk is. Als de elektronische lezer kan constateren dat de houder van het identiteitsbewijs ten minste 16 is, dan is dat voldoende. Hetzelfde geldt voor het bezitten van een sportabonnement. Extra informatie zoals een naam en exacte geboortedatum is hierbij irrelevant.

Bij voorkeur zouden we pasjes willen maken die volledig anoniem zijn. Dan is het immers niet meer mogelijk om gedetailleerde informatie te verzamelen over het gebruik van zo'n kaart. Hoewel er een anonieme OV-chipkaart bestaat, zou deze door veel privacydeskundigen niet anoniem, maar pseudoniem genoemd worden. Immers, bij de anonieme OV-chipkaart is de kaart als zodanig nog wel herkenbaar, maar is alleen niet bekend wie de houder van de kaart is. De kaart fungeert dus als een pseudoniem voor de kaarthouder. Bij een echt anonieme kaart zouden we zelfs niet kunnen zien of twee reizen met dezelfde kaart gemaakt zijn.

Geloofsbrieven

We hebben het wel de hele tijd over pasjes, kaartjes en ID-bewijzen, en natuurlijk begrijpen we allemaal wat daarmee bedoeld wordt. Voor de rest van het verhaal is het echter belangrijk dit wat preciezer te maken. De bovengenoemde documenten bevatten uitspraken als "Piet is tenminste 18 jaar oud" of in het geval van een paspoort misschien wat specifieker "Piet is geboren op 14 februari 1989." Maar zo'n uitspraak alleen is niet voldoende. Ik kan ook wel beweren dat ik nog 18 ben, maar dat gelooft niemand. Als echter de gemeente dat zou beweren, dan geloven we dat wel.

We vertrouwen informatie op een paspoort omdat we weten dat een paspoort alleen door de overheid gemaakt kan worden. In zekere zin bevestigt de gemeente dus de informatie in het paspoort juist

omdat zij de enige is die het paspoort kan produceren. Deze combinatie van uitspraak en bevestiging van een vertrouwde instantie noemen we een geloofsbrief.

In de rest van dit stuk kijken we alleen nog maar naar elektronische geloofsbrieven, deze kunnen dus bijvoorbeeld op een chipkaart gezet worden. Voor mijn masterscriptie heb ik gewerkt met een speciale variant van deze geloofsbrieven, de zogenaamde zelf-randomiseerbare geloofsbrieven. Het idee is dat deze geloofsbrieven, iedere keer dat ze gelezen worden door een machine, er totaal anders uitzien, terwijl de lezer toch nog de geldigheid kan controleren. Als we dit netjes doen krijgen we de door ons gewenste volledige anonimiteit gratis.

Helaas hebben zelf-randomiseerbare geloofsbrieven, net als vele andere volledige anonieme geloofsbrieven, een belangrijk nadeel: het is erg lastig om ze te blokkeren, bijvoorbeeld nadat misbruik is gedetecteerd. Immers, als een geloofsbrief er iedere keer anders uitziet, hoe kan een lezer dan nog zien of hij met een geblokkeerde kaart te maken heeft? Dit is een van de problemen die ik in mijn masterscriptie heb opgelost.

Cryptografie

Cryptografie betekent letterlijk *'geheim schrijven*', en is de studie naar vragen als "hoe kan Anne een bericht versleutelen zodat alleen Bas het kan lezen en niemand anders?" Het doel is dus dat Anne en Bas met elkaar kunnen praten zonder dat ze afgeluisterd kunnen worden. Als echter het bericht van Anne "lanceer de atoomraket" is, dan wil Bas misschien ook zeker weten dat het bericht ook echt van Anne afkomstig is. Hiertoe kan Anne het bericht ondertekenen met een digitale handtekening.

Een digitale handtekening is een eenvoudige manier om een geloofsbrief te maken. Een handtekening van het CBR bij jouw naam dient dan als geloofsbrief voor het behalen van een rijbewijs. Zo'n handtekening is natuurlijk alleen maar nuttig als we weten dat alleen het CBR die kan maken en iedereen hem kan controleren.

Om dit te doen heeft het CBR een privésleutel die alleen zij kent. Deze sleutel wordt gebruikt om handtekeningen te maken. Een bijbehorende publieke sleutel, die iedereen kent, wordt gebruikt om een handtekening te controleren.

In ons systeem is een privésleutel a altijd een getal modulo een priemgetal p, oftewel a zit in het lichaam $\mathbb{F}_p$ (zie kader over Groepen en (eindige) lichamen op de volgende pagina). Sterker nog, in het vervolg zitten alle variabelen met een kleine letter in het lichaam $\mathbb{F}_p$. Neem P een punt op een elliptische kromme, dan is $A = aP$ de publieke sleutel die bij a hoort.

Natuurlijk kun je, als je heel veel tijd hebt, a terugvinden als je A en P kent. Het probleem van het terugvinden van a is zo bekend, dat het een naam heeft gekregen:

Het discrete-logaritmeprobleem: Gegeven een punt P en een punt $A = aP$, vind a.

In de cryptografie is het heel normaal om aan te nemen dat zo'n probleem lastig is. Daarmee bedoelen we dat het verschikkelijk lang duurt om het probleem op te lossen. In de praktijk zorgen we er vaak voor dat p ongeveer zo groot is als 2^{160}. Het beste bekende algoritme heeft dan alsnog ongeveer 2^{80} stapjes nodig om a terug te vinden. Zelfs op een snelle computer duurt dit meer dan een miljoen jaar. Onze keuze voor p is daarmee ruim voldoende, tenminste, zolang niemand opeens een veel slimmer algoritme bedenkt om het discrete-logaritmeprobleem op te lossen…

Laten we voor het gemak wat namen introduceren: Anne, Bas en Carla. Anne speelt de rol van de autoriteit of gemeente en heeft het hierboven genoemde sleutelpaar $a, A = aP$. Ze deelt geloofsbrieven uit. Bas ontvangt een dergelijke geloofsbrief en probeert daarna aan Carla, de controleur, te bewijzen dat hij inderdaad een geldige geloofsbrief heeft.

Ook Bas heeft een eigen sleutelpaar: $b, B = bP$. Als Anne een geloofsbrief aan Bas wil geven moet ze een handtekening zetten over een sleutel van Bas. In dit

Groepen en (eindige) lichamen

Wiskundigen houden van structuur. Een van de eenvoudigere structuren is die van een groep. Een groep heeft vier eigenschappen die we zullen illustreren aan de hand een voorbeeld: de gehele getallen, oftewel $\mathbb{Z} = \{\ldots, -2, -1, 0, 1, 2, \ldots\}$. De operatie plus ($+$) combineert twee groepselementen, oftewel getallen, en produceert een nieuw getal. Bijvoorbeeld: $3 + 5 = 8$. Dit werkt voor iedere twee gehele getallen (geslotenheid). Het getal 0 fungeert als eenheidselement; 0 ergens bij optellen geeft datzelfde getal (bijv. $3 + 0 = 3$). Om ons het werk makkelijk te maken mogen we zelf bepalen waar we de haakjes zetten (associativiteit), dus $3 + (4 + 5) = (3 + 4) + 5$. Tot slot bestaat er van ieder element een inverse (invertibiliteit). De inverse van 7 is -7 want $7 + (-7) = 0$, oftewel gelijk aan het eenheidselement.

De vermenigvuldigingsoperator geeft *geen* groep over de gehele getallen. De meeste gehele getallen hebben immers geen gehele inverse. De multiplicatieve inverse van 2 ($= \frac{1}{2}$) is bijvoorbeeld geen geheel getal. Bij breuken ligt dit anders. Hier kunnen we zowel een groep met optellen als een groep met vermenigvuldigen maken. Natuurlijk moeten we 0 weglaten voor het vermenigvuldigen, want die heeft geen multiplicatieve inverse. Een structuur waarin we zowel kunnen optellen als vermenigvuldigen wordt wel een lichaam genoemd.

De verzamelingen van gehele getallen en van breuken zijn natuurlijk prachtig, maar ze zijn ook oneindig groot. Dit is lastig voor een computer, die immers liever met eindige dingen werkt. Een favoriet eindig lichaam zijn de getallen modulo een priem p: $\mathbb{F}_p = \{0, 1, 2, \ldots, p-1\}$. Dat optellen een groepsstructuur geeft is weinig verrassend. Dat dit echter ook voor vermenigvuldigen geldt, is dat misschien wel. Neem als voorbeeld $p = 13$, dan is natuurlijk $3 \cdot 12 \equiv 36 \equiv 10 \pmod{13}$ weer een getal modulo p. Echter, de inverse van 3 is 9, want $3 \cdot 9 \equiv 27 \equiv 1 \pmod{13}$. En inderdaad, voor ieder element (behalve 0) bestaat zo'n inverse.

geval gebruiken we daarvoor voor het gemak de privésleutel, b, van Bas. De handtekening G ziet er in dat geval als volgt uit:

$$G = (a + b)^{-1} Q .$$

Zoals het hoort kan alleen Anne (en niet Bas of iemand anders) deze handtekening maken. Hier is immers a voor nodig. Merk op dat $(a + b)^{-1}$ inderdaad bestaat omdat $a + b$ in het lichaam $\mathbb{F}_p$ zit en dus inverteerbaar is. Laten we nu eens kijken hoe Carla de handtekening kan controleren. Carla krijgt van Bas zijn publieke sleutel B en de handtekening G. Dan controleert Carla de handtekening van Anne met behulp van de bilineare afbeelding e (zie kader over Elliptische Krommen):

$$e(B + A, G) \stackrel{?}{=} e(P, Q) .$$

Als de gelijkheid geldt, dan klopt de handtekening. Dit systeem is oorspronkelijk bedacht door Boneh en Boyen [2].

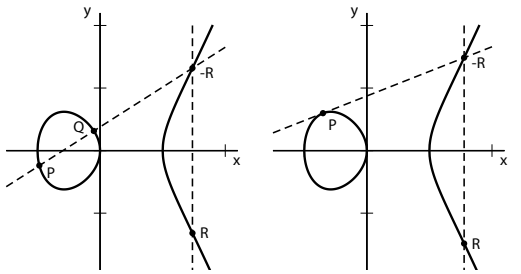
Een anonieme oplossing

We hebben nu een paar bouwstenen, maar daarmee hebben we ons oorspronkelijke probleem nog niet opgelost. De hierboven geschetste oplossing blijkt namelijk niet veilig te zijn.

Als je protocollen ontwerpt, moet je met veel situaties rekening houden. Beschouw het hiervoor geschetste protocol. Bas overhandigt zijn publieke sleutel en certificaat aan Carla, en zij controleert deze. Afgezien van het feit dat dit niet anoniem is, lijkt dit op het eerste gezicht een prima protocol. Maar niets is minder waar. Stel dat Sonja het gesprek tussen Bas en Carla afluistert, dan kan Sonja daarna opeens doen alsof ze Bas

Elliptische krommen

Rond 1986 bedachten Koblitz en Miller [2] dat elliptische krommen gebruikt kunnen worden voor cryptografische doeleinden. We geven hier een heel korte introductie. Een elliptische kromme wordt gegeven door de oplossingen van een vergelijking van de vorm $y^2 = x^3 + ax + b$ samen met een punt O dat we het punt op oneindig noemen. In het figuur zijn de oplossingen reëel, maar voor onze toepassingen kiezen we altijd $x,\ y$ in een eindig lichaam $\mathbb{F}_p$.



elliptische krommen, links: P+Q=R, rechts: P+P=R

Dat elliptische krommen heel interessant kunnen zijn, zien we pas als we ze als groepen zien in plaats van als verzamelingen van oplossingen. Een oplossing zullen we om voor de hand liggende redenen een punt noemen, en aanduiden met een hoofdletter. Het figuur hiernaast laat zien hoe je punten kan optellen en inverses bepaalt.

Een flinke berg rekenwerk toont aan dat we op deze manier echt een groep krijgen, met nette formules voor het optellen van twee punten. We kunnen natuurlijk een punt P vaker bij zichzelf optellen, dus schrijven we nP voor de som van n punten P.

Het grote voordeel, voor ons, is dat sommige elliptische krommen bilineaire afbeeldingen toestaan. Een bilineaire afbeelding e is een niet-triviale afbeelding met de eigenschap dat $e(aP, bQ) = e(P, Q)^{ab}$, waar P en Q ieder op een kromme liggen.

is *met* een geldige geloofsbrief. Sterker nog, wie zegt dat Carla te vertrouwen is? Ook Carla kan zich nu voordoen als Bas.

Bas		**Carla**
Publieke sleutel B		Anna's Publieke sleutel A
Privésleutel b		
Geloofsbrief G		
ontvang N	←	stuur nP
stuur B, G, bN →		ontvang B, G, M
		$e(B + A, G) \stackrel{?}{=} e(P, Q)$
		$M \stackrel{?}{=} nB$

Welke fout hebben we hier gemaakt? Iedereen kan zomaar met een publieke sleutel zwaaien, die is immers publiek! Wat belangrijk is, is dat *alleen* Bas de privésleutel kent. Maar hoe kan hij dit aantonen? Hij kan moeilijk zijn privésleutel weggeven. Gelukkig blijkt hier een trucje voor te bestaan, zie het bovenstaande protocol. Carla bedenkt een willekeurig getal n, en stuurt $N = nP$ naar Bas. Bas stuurt vervolgens niet alleen B en G terug, maar ook $M = bN (= bnP)$. Carla controleert of Bas M goed geconstrueerd heeft door te testen of $M = nB$.

Maar, kan niet iedereen met behulp van $B = bP$ en $N = nP$ het juiste antwoord $M = bnP$ maken? In dit geval nemen we eenvoudig aan dat dit niet mogelijk is, oftewel het volgende probleem is ook lastig:

Het computationele Diffie-Hellman probleem: Gegeven punten $P, A = aP$ en $B = bP$, bepaal abP.

Hieruit volgt dan ook dat de conversatie niet zomaar herhaald kan worden, tenminste zolang Carla telkens een willekeurige n kiest.

Het protocol dat we nu geconstrueerd hebben is de traditionele manier om aan te tonen dat je bent wie je zegt dat je bent. Sterker nog, dit is precies de structuur die ook gebruikt wordt voor het communiceren met beveiligde webpagina's. Het onderliggende systeem is anders, maar het idee is gelijk.

We hadden bedacht dat als een geloofsbrief er iedere keer anders uit ziet, hij ook anoniem is. Dat is nu nog niet het geval want B en G veranderen nooit. We gaan nu zien hoe we dat kunnen doen. De publieke sleutel kunnen we randomiseren door hem te vermenigvuldigen met een willekeurig gekozen α. We versturen dus $\overline{B} = \alpha B$ in plaats van B. Om het controleren van de handtekening goed te laten werken moeten we ook $\overline{A} = \alpha A$ versturen in plaats van A. Zolang α onbekend is, is $\overline{B}$ geheel willekeurig. Tot slot vermenigvuldigen we G met een ander willekeurig getal β en sturen we $\overline{G} = \beta G$ in plaats van G.

We kunnen nu ons protocol zo aanpassen dat Bas telkens andere waardes verstuurt, maar Carla moet natuurlijk nog wel kunnen controleren dat ze kloppen. Als we de waardes $\overline{B}$, $\overline{A}$ en $\overline{G}$ invullen krijgen we (als ze tenminste kloppen):

$$e(\overline{B} + \overline{A}, \overline{G}) = e(P, Q)^{\alpha\beta} = e(\alpha P, \beta Q)\,.$$

Carla krijgt daarom ook nog $\overline{P} = \alpha P$ en $\overline{Q} = \beta Q$ van Bas zodat ze het resultaat kan controleren. Carla vertrouwt Bas natuurlijk niet helemaal, en wil dus weten of $\overline{A}$ inderdaad bij A hoort. Dit doet ze door te controleren of $e(\overline{A}, Q) = e(\overline{P}, A_Q)$, waarbij $A_Q = aQ$ een andere versie van Annes publieke sleutel is. Het hele protocol staat beschreven in onderstaand figuur.

In het begin vroegen we ons af of je zo'n zelf-randomiseerbare geloofsbrief kan blokkeren. Nu kunnen we zien hoe dat moet. We krijgen $\overline{B} = \alpha b P = b\alpha P = b\overline{P}$. Om een kaart te blokkeren sturen we de privésleutel b van die kaart naar Carla. Dan kan Carla daarna altijd controleren of ze een geblokeerde kaart te pakken heeft. Dit is namelijk precies geval als $\mathsf{b}\overline{P} = \overline{B}$.

Bas		**Carla**
Annes publ. sleutel A		Annes Publieke sleutel A_Q
Publieke sleutel B		
Privésleutel b		
Geloofsbrief G		
Bedenk $\mathsf{a}, \beta \in \mathbb{F}_p$		Bedenk getal $n \in \mathbb{F}_p$
ontvang N	$\leftarrow$	stuur nP
stuur aB, aP, aA	$\rightarrow$	ontvang $\overline{B}$, $\overline{P}$, $\overline{A}$
stuur βG, βQ, abN	$\rightarrow$	ontvang $\overline{G}$, $\overline{Q}$, $\overline{M}$
		$e(\overline{B} + \overline{A}, \overline{G}) \stackrel{?}{=} e(\overline{P}, \overline{Q})$
		$e(\overline{A}, Q) \stackrel{?}{=} e(\overline{P}, A_Q)$
		$\overline{M} \stackrel{?}{=} n\overline{B}$

Hoe hard we ook ons best hebben gedaan, het protocol uit het vorige figuur is onvolledig. De uiteindelijke versie van het protocol is nog wat uitgebreider, maar kort voor het ter perse gaan van deze Periodiek hebben we zelfs daarin een fout ontdekt. Hoewel dit meer werk betekent voor mij, geeft het maar weer eens aan hoe lastig het is om echt veilige protocollen te bedenken.

We hebben gezien hoe cryptografie techniek en wiskunde combineert. Aan de ene kant moet je iets nieuws bedenken en bouwen, maar aan de andere kant wil je ook de veiligheid van je bouwwerk kunnen aantonen. Dit laatste is zeker niet altijd makkelijk, en dwingt je soms om concessies te doen aan je protocol.

Ik heb dit afstudeeronderzoek gedaan bij TNO. De insteek van onderzoek bij TNO is noodzakelijkerwijs praktischer dan die van een universiteit. Voor mij heeft dit tot een inspirerend jaar geleid met een mooi contrast tussen deze praktischere insteek en mijn meer theoretische onderzoek. •

Referenties

[1] Marije Willems, "Pakkans bijstandsfraudeurs vergroot," NRC Handelsblad, http://www.nrc.nl/nieuws/2012/03/13/pakkans-bijstandsfraudeurs-vergroot/

[2] Dan Boneh and Xavier Boyen, "Short signatures without random oracles and the SDH assumption in bilinear groups", J. Cryptol, 21:149–177, 2 2008

[3] Menezes , Van Oorschot en Vanstone,"Handbook of Applied Cryptography", Crc Press, 1997

[4] Wouter Lueks, "Revocable self-blindable credentials," Master's thesis, Rijksuniversiteit Groningen, 2011

Caloriebom: de Kapsalon

DOOR **ARMIN PALAVRA**

De kapsalon is tegewoordig niet meer weg te denken als vette hap na het uitgaan. Het zilveren bakje met daarin genoeg caloriën en vet voor de hele week heeft iedereen wel eens voorbij zien komen bij de Hasret of Ozan. Maar waar komt het fenomeen met de gekke naam vandaan en hoe maak je het zelf?

Het idee van de kapsalon begon ooit in (je raadt het al) een kapsalon. Om precies te zijn in de kapsalon "Tati" op de schiedamse weg in Rotterdam. In 2003 had Nathaniël Gomes, de eigenaar van de kapperszaak zin in lunch. Hij ging naar de snackbar "El Aviva" om de hoek en besloot om een gerecht samen te stellen van zijn favoriete ingredienten: schoarma, patat, sla en knoflooksaus. Op aanraden van de snackbar eigenaar kwam daar ook nog kaas bij. En zo was de eerste kapsalon geboren.[1] In het vervolg vroeg Gomes om "het vaste recept van de kapsalon". Al snel was "kapsalon" voldoende. De klanten van El Aviva werden nieuwschierig naar het recept met de rare naam. De dappersten durfden er zelf ook een te bestellen. Vervolgens kregen snackbars en shoarmatenten in de buurt de vraag of ze kapsalons verkochten. Een aantal jaar later en het fenomeen is in heel Nederland bekend.

Zelf maken

Gelukkig hoef je geen keukenprinces te zijn om je eigen kapsalon te maken. Hetgeen wat je vooral nodig hebt is grote trek. Want in een traditionele kapsalon zitten 1000 kilocaloriën voor een kleine portie, in een grote portie (gangbaar formaat) zitten 1800 kilocaloriën, bijna genoeg om de rest van de dag niks te eten. Voor de zelfgemaakte kapsalon wijken we iets af van het traditionele recept. In plaatst van patat kunnen (bij gebrek aan frituurpan) ook aardappelpartjes gebruikt worden. De knoflooksaus kan vervangen worden door whiskey-cocktailsaus, zodat na het eten van de kapsalon mensen nog fatsoenlijk met je kunnen praten (na het uitgaan is dit meestal geen probleem omdat je dan toch meteen je bed in kruipt). Hiernaast het recept voor ongeveer 3 personen.

Recept voor Kapsalon

Ingrediënten:

- 500 gram shoarma vlees (of kebab)
- 600 gram aardappalpartjes (of patat)
- cocktailsaus (of knoflooksaus)
- (geraspte) kaas
- sla

Optioneel (voor extra luxe)

- cheddar smeltkaas (in stukjes)
- extra groente (tomaat, komkommer, augurk paprika etc.)
- sambalsaus

Materiaal:

- koekenpan
- ovenschaal
- oven

Bereiding:

1) Verwarm de oven op 200° en bak de aardappelpartjes en de shoarma in twee verschillende pannen.

2) Gooi de shoarma en aardappelpartjes bij elkaar in een ovenschaal. Meng de saus er doorheen en eventuele cheddar kaas.

3) Leg de groente en sla er bovenop en bedek alles met een laag geraspte kaas. Leg de schaal in de oven tot de kaas goed gesmolten is (ongeveer 10 min.) Je kan er ook voor kiezen om de groente en sla achteraf bij te doen.

4) Klaar! Haal de kapsalon uit de oven en serveer hem met een lekker koud biertje voor een optimale smaak •

Moeilijkheid: 
Aantal personen: 3 à 4
Bereidingstijd: +/- 25 min

Referenties:

[1] Culinair moordwapen, Sterre Lindhout., Volkskrant 14-9-2011,

Techniek die het leven eenvoudiger en aangenamer maakt

Bij Philips in Drachten zijn we ervan overtuigd dat technologie tegelijk zinvol en eenvoudig moet zijn. Wij brengen dat dagelijks in de praktijk met de ontwikkeling en productie van producten als de shaver, stofzuiger, Senseo, Wake-up Light en Airfryer. Producten die het leven van mensen vereenvoudigen en veraangenamen.

Groei mee met Philips. Kom werken bij een innovatief bedrijf dat een verschil maakt in de gezondheid en het welzijn van mensen. Je gaat deel uitmaken van één van de grootste ontwikkel- en productiecentra van Philips. Op deze site werken 2000 medewerkers, waaronder 600 ontwikkelaars van meer dan 35 verschillende nationaliteiten. De samenwerking in multidisciplinaire teams binnen de onderdelen High Impact Innovation Center, Innovation Personal Care, Innovation Domestic Appliances en Shaver Production Center biedt interessante loopbaanmogelijkheden.

Meer weten over een mogelijke start van je carrière? Bezoek dan **www.philips.com/careers** of **www.philips.com/engineers** voor traineeships, stages of een vaste baan, er is altijd wel een start die bij je past.

PHILIPS
sense and simplicity

Topologische Materialen

DOOR **KASPER DUIVENVOORDEN**

We kunnen tal van eigenschappen van materialen meten. Deze definieren de fase waarin een materiaal zich bevindt. Verandert een eigenschap discontinu, dan is er sprake van een fase-overgang. Neem bijvoorbeeld de opgeslage energie in water of waterdamp. Tijdens het koken verandert de opgeslagen energie, met de latente warmte, terwijl de temperatuur niet veranderd. De opgeslagen energie is dus discontinu als functie van de temperatuur en koken is een fase overgang van een vloeistof naar een gas.

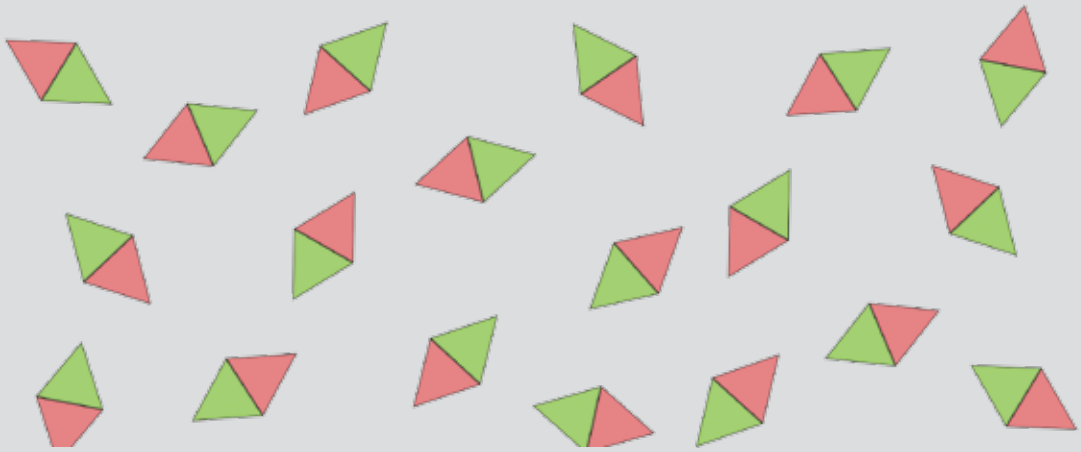
Naast de gas, vloeibaar en vaste stof fase zijn er nog tal van andere *vastestof*-fasen, gedefinieerd door onder andere electrische en magnetische eigenschappen. Eigenschappen die een fase definieren worden order parameters genoemd. Niet alleen is bekend welke fasen allemaal voorkomen in de natuur, we begrijpen ze ook. We hebben effectieve modellen opgesteld die voorspellen hoe order parameters veranderen gedurende een fase overgang. Maar dat is nog niet alles, we begrijpen fase-overgangen op een veel dieper niveau.

Landau had 60 jaar geleden een model opgesteld die een type fase-overgangen, namelijk die van de tweede orde, beschrijft. Hij kon hiermee universele uitspraken doen die voor alle tweede orde fase-overgangen gelden. Eén van die uitspraken is dat deze fase-overgangen gepaard gaan met een breking van symmetrie. Het klassieke voorbeeld hiervan is de overgang van de paramagnetische fase naar de ferromagnetische fase. In de paramagnetische fase is er nog sprake van rotatiesymmetrie terwijl deze is gebroken in de ferromagnetisch fase, dit is te zien in figuur 1.

Onlangs is gebleken dat het idee van Landau, dat fase-overgangen worden vergezeld met een symmetriebreking, niet volledig is. De ontdekking van het kwantum Hall effect in 1980 en het fractionele kwantum Hall effect in 1982 geeft ons twee tegenvoorbeelden. In een poging deze verschijnselen te begrijpen is het concept van de topologische fase ingevoerd.

Een topologische fase ontleent zijn naam aan de theorie die hem beschrijft. In het geval van het kwantum Hall effect is de weerstand een topologische invariant $\rho_{xy} = n\frac{h}{e^2}$.

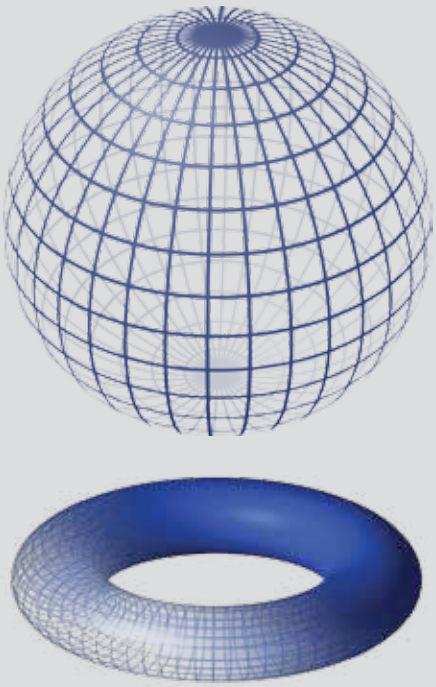
FIGUUR 1 In de ferromagnetische fase, bij lage temperaturen, zijn de magnetische momenten van elektronen geordend, om de energie te minimaliseren. Hiervoor hebben ze spontaan een richting gekozen en is rotatiesymmetrie gebroken.



FIGUUR 2 In de paramagnetische fase, bij hoge temperaturen, zijn de magnetische momenten van elektronen ongeordend, om de entropie te maximaliseren. Hierdoor is het totale magnetisch moment nul (in alle richtingen) en is er dus sprake van rotatie symmetrie

De integer n verandert alleen van waarde bij een fase-overgang. Afgezien daarvan is de resistentie ongevoelig voor continue veranderingen. Hij is enorm robuust, en kan met enorme nauwkeurigheid, namelijk negen significante cijfers, gemeten worden. Dit is zo precies dat sinds de ontdekking ervan, de kwantum Hall weerstand wordt gebruikt als standaard voor elektrische weerstanden.

Topologische fasen worden beschreven door een topologische invariant, een fysische eigenschap die alleen verandert bij het ondergaan van een (topologische) fase-overgang. Dit geeft enorme mogelijkheden. Een toepassing zou de kwantumcomputer kunnen zijn. Het grootste struikelblok bij het maken van zo'n computer is dat kwantumtoestanden heel instabiel zijn, waardoor informatie binnen een mum van tijd verlo-



Topologie

Topologie gaat over de studie naar eigenschappen van ruimtes die behouden zijn onder continue afbeeldingen. Ruimtes waartussen zo'n afbeelding bestaat zijn topologisch equivalent. Neem bijvoorbeeld een bol en een torus. Hiertussen bestaat geen continue afbeelding en deze zijn dus niet equivalent. Topologische invarianten zijn eigenschappen van ruimtes die behouden zijn onder alle continue afbeeldingen. In het voorbeeld van de bal en de torus is het aantal gaten een topologische invariant. En omdat de bal geen gaten heeft en de torus wel een gat heeft, volgt daar direct uit dat de bal en de torus niet topologisch equivalent zijn.

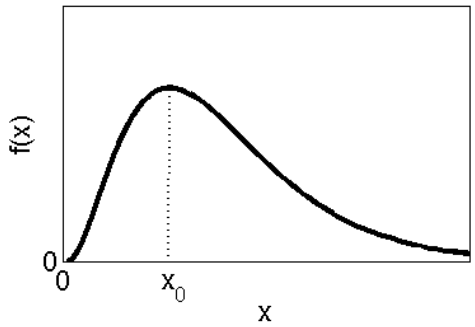
ren gaat. Door topologische invarianten te gebruiken voor informatie opslag, is dit probleem in één klap opgelost.

Tot slot een klein speelgoed model om een indruk te geven hoe topologie een rol speelt in de beschrijving van een topologische fase. Beschouw de onderstaande Hamiltoniaan:

$$\begin{aligned} H(k) = (1 - f(|k|)(k_1^2 + k_2^2))\sigma_3 \\ + f(|k|)k_3(k_1\sigma_1 + k_2\sigma_2) \\ + l^{-2}f'(|k|)(k_1\sigma_2 - k_2\sigma_1) \end{aligned}$$

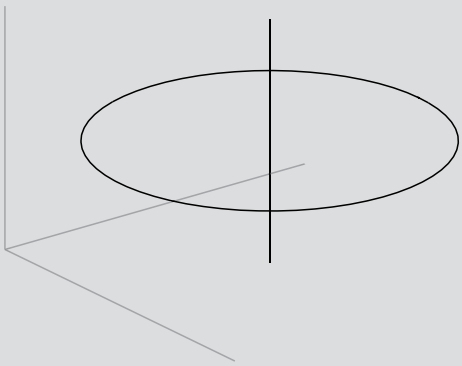
Deze Hamiltoniaan beschrijft een drie-dimensionaal materiaal met twee elektronenbanden: een geleidingsband en een valentieband. Verder is k het momentum van de elektron, deze heeft drie componenten k_i. De functie $f(x)$ heeft een maximum bij x_0, welke groter is dan 1 (zie de grafiek), σ_i zijn de Pauli matrices en l is een lengteschaal. Van belang is alleen de eerste term. De andere twee termen zorgen ervoor dat de Hamiltoniaan twee banden beschrijft die elkaar niet snijden.

Bij $k_1 = k_2 = 0$ vereenvoudigt de Hamiltoniaan zich tot $H(k) = \sigma_3$ waardoor in de grondtoestand de valentieband gevuld is met *spin down* elektronen. Bij $k_3 = 0$ en $k_1^2 + k_2^2 = x_0^2$ vereenvoudigt de Hamiltoniaan



zich tot $H(k) = -a\sigma_3$ (waarbij $a = 1 - f(|k|)$ positief is) waardoor in de grondtoestand de valentieband gevuld is met *spin up* elektronen. Deze twee banden zijn gegeven in figuur 3. Het feit dat deze twee banden in de knoop zitten wil zeggen dat de Hamiltoniaan een topologische fase beschrijft.

Ik ben op het moment dat deze Periodiek uitkomt bezig met een promotie-onderzoek aan de Universiteit van Keulen. Hoewel het model hierboven een topologische fase beschrijft, is het nog geen sinds een kwantumcomputer. De eerste stap is om te begrijpen welke topologische fasen voor kunnen komen in de natuur. Dit is het onderwerp van mijn promotie onderzoek in Keulen. Daar houd ik me bezig met het zetten van deze eerste stap. •



FIGUUR 3 De brillouinzone van een drie dimensionale isolator. De rechte verticale lijn (1) beschrijft alle momenta k waarvoor de valentie band uit *spin down* electronen bestaat. De cirkelvormige curve (2) beschrijft alle momenta k waarvoor de valentie band uit *spin up* elektronen bestaat. Het feit dat (1) door (2) gaat, zodat ze een knoop vormen, geeft aan dat de isolator in een topologische fase is.

perio*diek

schrijf een stuk win een Kindle e-reader

Stel een onderwerp voor

Je mag zelf een onderwerp uitkiezen, om vervolgens aan de redactie voor te stellen. Je stuk en het onderwerp moeten namelijk voldoen aan een aantal eisen.

Schrijf een stuk

Als je onderwerp is goedgekeurd, dan kun je natuurlijk gaan schrijven. Er zijn nog wel een paar dingen waar je aan moet denken.

Win een e-reader

Als we je stuk gaan plaatsen, dan krijg je sowieso een Perio-vulpen. Maar als je tot de beste drie stukken behoort, dan win je daarnaast een gloednieuwe Kindle e-reader.

Kijk voor voor meer informatie en de voorwaarden op schrijfwedstrijd.fmf.nl

Energie onder onze voeten

DOOR **ARNETTE VOGELAAR**

Jaarlijks gebruiken we in Nederland ongeveer 195 GJ per persoon aan energie en dit wordt elk jaar meer. Deze energie wordt voornamelijk gewonnen uit aardgas, aardolie, steenkool en in mindere mate op duurzame schaal door middel van bijvoorbeeld windmolens [1]. De naam aardolie of aardgas suggereert dat deze vorm van energie te vinden is onder het aardoppervlak. Daarnaast is het algemeen bekend dat deze energiebronnen pas bruikbaar zijn na diverse bewerkingen. Heel wat minder bekend is hoe deze energiebronnen ooit zijn ontstaan. Welke bronnen zitten er in de diepe ondergrond en hoe kan deze energie worden gewonnen?

Oorspronkelijk zijn olie en gas slechts afbraakproducten van organische materialen; dieren en planten bestaande uit koolstofketens. Op het aardoppervlak zou dit materiaal wegrotten onder invloed van de aanwezige zuurstof, maar wanneer het bedolven raakt onder aardlagen, is dit niet mogelijk [2]. De organische sedimenten worden samengedrukt en raken steeds verder verwijderd van het aardoppervlak in de loop van miljoenen jaren. Uiteindelijk vormen ze iets wat bekend staat als het moedergesteente: de bron voor olie en gas. De temperatuur in de aarde neemt toe met de diepte en deze temperatuurtoename zorgt ervoor dat de koolstofketens gekraakt worden. Olie wordt meestal gevormd bij temperaturen tussen de 100 en 150 °C, terwijl voor gas temperaturen boven de 150 °C nodig zijn [3].

Olie en gas bewegen zich graag naar het oppervlak, omdat ze lichter zijn dan water. Een samenspel tussen de geometrie van de ondergrond en de eigenschappen van de verschillende aardlagen bepaalt of de gevormde moleculen kunnen worden opgeslagen: in een gas- of olieveld. Alleen bij de aanwezigheid van een bepaalde afdekking is het onmogelijk te ontsnappen naar het aardoppervlak. De moleculen zullen zich dan nestelen in een gesteente dat voldoende poreus is om de fossiele brandstof vast te houden. Een dergelijk gesteente wordt een reservoir genoemd en is meestal zandsteen of kalksteen. In Noord-Nederland bestaan de meeste reservoirs uit Rotliegend zandsteen en zijn ze afgedekt met een ondoorlaatbare laag Zechstein zout [3].

Boren naar fossiele brandstoffen

Het aardoppervlak kan in kaart worden gebracht met behulp van 'remote sensing' technieken, zoals het meten van de weerkaatsing van pulsen door de verschillende aardlagen. Aan de hand van deze methode kan er worden bepaald of er mogelijk een veld aanwezig is. Wanneer een mogelijk veld is gevonden, kan worden besloten om een proefput te boren. Op deze manier kan er worden gekeken of de hypothese klopt en of het economisch aantrekkelijk is om dit veld te gaan exploiteren. Dit wordt gedaan door het meten van de druk, de temperatuur en de stroomsnelheid van de fossiele brandstof. Deze stroomsnelheid wordt bepaald door de permeabiliteit van het reservoir [3]. Permeabiliteit is gedefinieerd als de mogelijkheid van het gesteente om vloeistoffen door te laten en heeft de unit Darcy (D); ($9.869233 \cdot 10^{-13} m^2$). De permeabiliteit neemt over het algemeen af met de diepte: hoe dieper je gaat, hoe meer de gesteentes samengedrukt zijn. Het is essentieel dat het reservoir permeabel is, zodat de fossiele brandstof zelf naar het oppervlak beweegt [4].

De gewonnen fossiele brandstoffen moeten altijd schoon gemaakt worden, omdat er ook kleine deeltjes en water mee worden geproduceerd. Door het produceren van de fossiele brandstof raakt het reservoir steeds leger. Hierdoor wordt de druk in het reservoir lager, dan deze initieel was, en wordt het vervolgens steeds moeilijker om te blijven produceren. Normaal gesproken neemt de hydrostatische druk met 10 bar toe elke 100 meter dieper. Dit betekent dat er op een diepte van 3000 meter een druk van ongeveer 300 bar zou zijn. Na het produceren van de fossiele brandstof kan de druk in het veld wel dalen tot rond de 100 bar [3]. Op een bepaald moment wordt het dan ook (economisch) onaantrekkelijk om verder te produceren en wordt een put verlaten en afgesloten. Zo'n veld is dan op het End-Of-Field-Life (EOFL) [4].

Aardwarmte

Naast dat er fossiele brandstoffen in de aarde te vinden zijn op bepaalde dieptes, is het er ook een stuk warmer: gemiddeld neemt de temperatuur toe met 30 °C per kilometer. Tegenwoordig zijn er al diverse toepassingen die gebruik maken van aardwarmte, zoals warmte-koude-opslag (WKO). In Groningen is d0eze toepassing te vinden in onze universiteitsbibliotheek [5], maar WKO- toepassingen zijn relatief ondiep in vergelijking met grotere projecten. Deze hebben namelijk putten van een aantal kilometers diep nodig. Hierbij beginnen de temperaturen bij 70 °C aantrekkelijkere toepassingen geven, zoals het verwarmen van broeikassen of huizen.

Productie van aardwarmte kan alleen plaatsvinden als er een geothermisch systeem aanwezig is. Een dergelijk systeem bestaat uit een warmtebron, een warmtedrager en een reservoir. De warmtebron is in dit geval het binnenste van de aarde, wat een constante warmtestroom naar het oppervlak geeft van 65 mW/m^2 in Nederland [3]. In het geval van een natuurlijk geothermisch systeem is neerslagwater de warmtedrager, maar bij een kunstmatig systeem wordt het water in het systeem gepompt vanaf het oppervlak. In figuur 1 is te zien hoe zo'n kunstmatig systeem er ongeveer uit zou zien voor twee putten. Het reservoir wordt ook wel een aquifer genoemd en bestaat uit een permeabele steenlagen en is meestal bedekt door impermeabel gesteente. De maximale hoeveelheid energie H_{th}[J] die kan worden gewonnen uit een bepaald volume V_r [m^3] hangt af van de dichtheid $\rho_r[kg/m^3]$ en warmte capaciteit van het gesteente $C_r[J/kg^oC]$ met $\Delta T[^oC]$ het temperatuur verschil van het geïnjecteerde en geproduceerde water:

$$H_{th} = \rho_r C_r V_r \Delta T$$

Om gedurende een bepaalde periode aardwarmte te produceren moet er een optimum worden gevonden tussen het injecteren/produceren van water en de afkoeling van het reservoir.

Hergebruik van EOFL?

De techniek die wordt gebruik voor het boren naar aardwarmte is gelijk aan gas- en/of olieproductie. Een slimme lezer zal hebben misschien wel hebben opgemerkt dat zowel voor de vorming van een gasveld als de productie van aardwarmte een reservoir nodig is. Na het produceren van de fossiele brandstof is zo'n reservoir niet meer nuttig End-of-field-life, kortom zou het niet interessant zijn om 'lege' gasvelden te hergebruiken voor de productie van aardwarmte?

Het grootste obstakel om aardwarmte te produceren ligt voornamelijk aan de financiële kant: het boren van putten beslaat ongeveer 60 procent van de totale investeringskosten [6]. Dit obstakel zou dus zijn opgelost bij het hergebruiken van oude gasputten: de geboorde putten worden immers hergebruikt. Andere vereisten om oude gasvelden te hergebruiken zijn de permeabiliteit van het veld, deze moet goed genoeg zijn, zodat het water gemakkelijk van de injectie naar de productieput kan stromen, maar dat het water tegelijkertijd ook voldoende opwarmt. Problemen liggen ook op de loer, aangezien er overgebleven gas mee zal worden geproduceerd. Deze gasresten zullen moeten worden gefilterd uit het water, wat weer technische en maar ook juridische uitdagingen geeft. Verder is het nog

onbekend hoe lang de oude gasputten kunnen worden hergebruikt en hoe het veld exact reageert op injectie van (koud) water.

Zelf heb ik onderzoek gedaan naar het gedrag van een leeg gasveld tijdens de productie van aardwarmte. De conclusie is dat het hergebruiken van 'lege' gasvelden mogelijk is, maar dat er nog veel onderzoek nodig is. Dit alles gebeurt in de groep Geo-energie onder leiding van Professor Rien Herber. Naar mijn mening een erg interessant vakgebied, waar veel onderzoek wordt gedaan naar onze energievoorziening van in de toekomst •

Referenties

[1] IEA (2010) Energy balances of OECD countries, 2010 edition. International Energy Agency, Paris, France

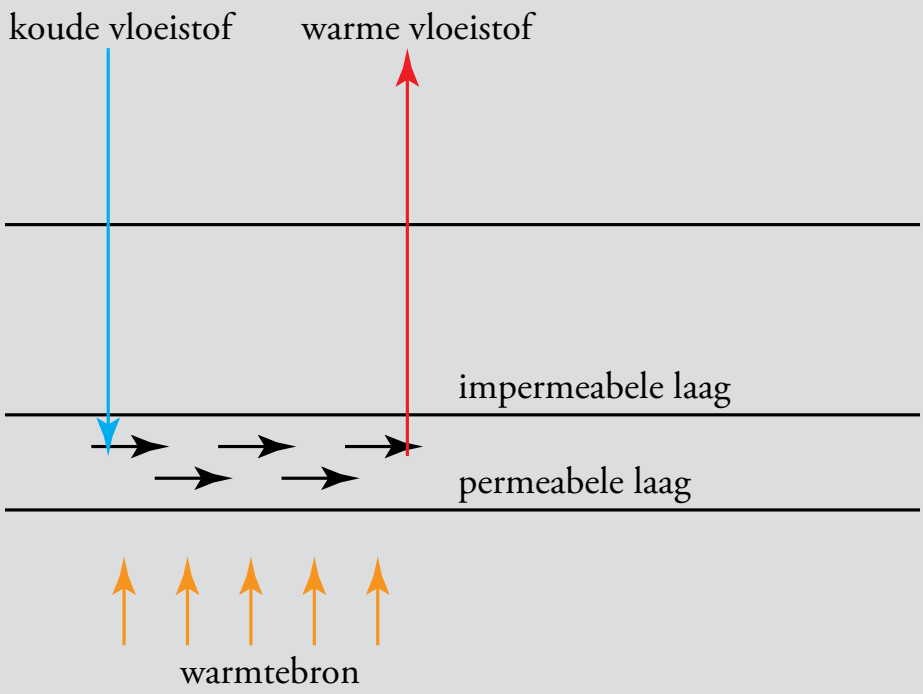
[2] Kennislink (2009). Nederland, het olie- en gascentrum van West-Europa. Beschikbaar op: http://www.kennislink.nl/publicaties/nederland-het-olie-en-gascentrum-van-west-europa Geraadpleegd op: 24 februari 2012

[3] Herber, R. (2010). Geo-energie, Colleges van het vak Geo-energie. Rijksuniversiteit Groningen.

[4] Schlumberger (2011). Oilfield Glossary. Beschikbaar op http://www.glossary.oilfield.slb.com/ Geraadpleegd op: 21 September 2011

[5] Rijksuniversiteit Groningen (2011). Sustainable Construction. Beschikbaar op: http://www.rug.nl/duurzaamheid/Nieuwbouw/duurzameNieuwbouw?lang=en Geraadpleegd op: 27 februari 2012

[6] Tester, J.W. et al. (2006). The future of geothermal energy. Massachusetts Institute of Technology



FIGUUR 1 Een schematische weergave van een geothermisch systeem, koud water wordt in het systeem gepompt en warm water wordt er weer uit gehaald.

Schut Geometrische Meettechniek is een internationale organisatie met vijf vestigingen in Europa en de hoofdvestiging in Groningen. Het bedrijf is ISO 9001 gecertificeerd en gespecialiseerd in de ontwikkeling, productie en verkoop van precisie meetinstrumenten en -systemen.

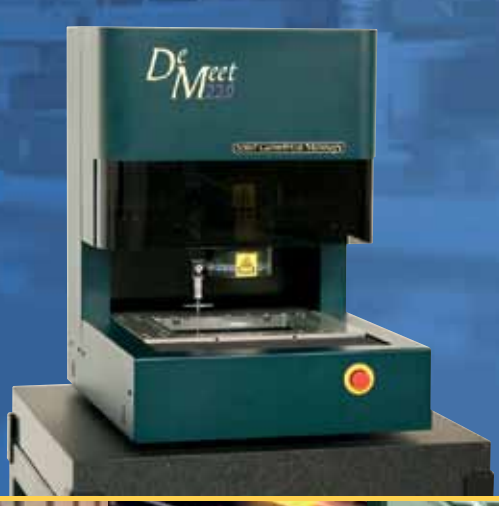
Aangezien we onze activiteiten uitbreiden, zijn we continu op zoek naar enthousiaste medewerkers om ons team te versterken. Als jij wilt werken in een bedrijf dat mensen met ideeën en initiatief waardeert, dan is Schut Geometrische Meettechniek de plaats. De bedrijfsstructuur is overzichtelijk en de sfeer is informeel met een “no nonsense” karakter.

Op onze afdelingen voor de technische verkoop, software support en ontwikkeling van onze 3D meetmachines werken mensen met een academische achtergrond. Hierbij gaat het om functies zoals ***Sales Engineer***, ***Software Support Engineer***, ***Software Developer (C++)***, ***Electronics Developer*** en ***Mechanical Engineer***.

Er zijn bij ons ook mogelijkheden voor een technisch interessant **stage-** of **afstudeerproject**. Dit kan in overleg met de docent worden afgestemd.

Open sollicitaties zijn ook zeer welkom. Voor echt talent is altijd ruimte.

Voor meer informatie kijk op **www.Schut.com** en **Vacatures.Schut.com**, of stuur een e-mail naar **Sollicitatie@Schut.com**.



APPROVE for DeMeet