Bij de wiskunde van het navigatiesysteem denkt vrijwel iedereen meteen aan GPS en bolmeetkunde. Maar er zijn nog veel meer wiskundige aspecten. **Jurjen Bos** navigeert ons door de

Onzichtbare wiskunde in een autonavigatiesysteem

Inleiding

Er zit meer wiskunde in de wereld dan de meeste mensen kunnen of willen zien. Soms zit ergens zelfs heel veel wiskunde in, terwijl je dat nauwelijks aan de buitenkant kunt zien. Dit stukje geeft een aardig voorbeeld van een ogenschijnlijk simpel apparaatje dat tjokvol met wiskunde zit: het navigatiesysteem. Niet alleen zit er veel wiskunde in, maar een groot gedeelte van deze wiskunde is relatief jong: er zit veel bij dat nog niet bestond toen ik op school zat.

Door het voorbereiden van dit artikel ben ik gaan nadenken waarom dit apparaat in deze tijd is uitgevonden. Ik ben tot de conclusie gekomen dat niet alleen de technologie die nodig is nog maar kort bestaat, maar ook dat de wiskunde die nodig is voor dit ding nog maar heel jong is, en dat het apparaat alleen al daarom niet eerder had kunnen bestaan. De rol van wiskunde in de ontwikkeling van de technologie is dus groter dan ik dacht. Maar voordat we te snel diep in de materie duiken, moet ik eerst maar eens uitleggen hoe zo'n apparaat werkt.

Hoe het werkt

Een navigatiesysteem moet iemand helpen om de weg te wijzen naar een punt. Dit proces bestaat uit een aantal stappen. Ruwweg is dit de volgorde van de stappen:

1. Voordat we op reis gaan: de juiste kaart in het geheugen van het apparaat zetten.
2. Voor vertrek: invoeren van het adres door de bestuurder.
3. Onderweg: kijken waar we op elk gegeven ogenblik zijn.
4. Uitzoeken welke kant we op moeten.
5. Op het scherm tekenen wat de route is.
6. Vertellen wat de bestuurder moet doen.

Het resultaat is een prettige manier van autorijden, waarbij de bestuurder alleen maar over het autorijden hoeft na te denken, en vooral niet over alle technologie daarachter. Maar nu zitten we stil, en kunnen we daar rustig over gaan denken.

Waar zit de wiskunde

In elk van de stappen van het proces dat ik hierboven heb genoemd, wordt wiskunde gebruikt, soms onopvallend, soms overduidelijk. Hieronder volgt een lijstje van de wiskunde die ik heb kunnen ontdekken. Ik heb geprobeerd uit te vogelen wanneer deze dingen ongeveer zijn uitgevonden.

- **1916** verschuiving van de tijd in een zwaartekrachtveld
- **1916** verschuiving van de tijd ten opzichte van een draaiende waarnemer
- **1947** berekening van nauwkeurigheid van berekeningen
- **1960** tekenen van driedimensionale gegevens
- **1968** zoeken van het kortste pad in een graaf
- **1970** zoeken van gegevens op een index
- **1976** publieke-sleutelcryptografie
- **1976** CDMA codering (een speciaal geval van *spread spectrum* dat al in de Tweede Wereldoorlog werd gebruikt)
- **1984** indexeren van gegevens op geografische locatie
- **1990** compressie van geluid (MP3)
- **1998** tekenen van tekst op een LCD-scherm

Je kunt twee van deze onderwerpen tot de natuurkunde rekenen, maar de hoeveelheid wiskunde in deze onderwerpen is niet te negeren. In de rest van dit verhaal laat ik de interessantste onderwerpen zien, in de volgorde die ik hierboven heb aangegeven.

Stap 1: Kaarten laden

Voordat je op reis gaat, wil je natuurlijk de juiste kaarten in het geheugen van je apparaat hebben. Mijn navigatiesysteem heeft de mogelijkheid om de kaarten via het internet aan te schaffen. Om een nieuwe kaart op te halen, vul ik op de website van de leverancier het serienummer in van mijn apparaatje, en daarna kan ik de kaarten ophalen. Om dit mogelijk te maken, worden de kaarten gecodeerd met een geheime sleutel, zodat alleen mijn apparaatje de kaarten kan gebruiken. Op deze manier zorgt de leverancier dat zijn kaarten eerlijk betaald worden.

Uiteraard wil de leverancier niet voor ieder systeem dat ze maken een aparte sleutel maken en onderhouden, dus moet het slimmer. Dit kan globaal op twee verschillende manieren: met sleuteldifferentiatie, en met publieke-sleutelcryptografie. Over publieke-sleutelcryptografie is al zo vaak geschreven dat ik je doorverwijs naar een van de vele andere populaire artikelen over dit onderwerp.

Sleuteldifferentiatie is een veel eenvoudiger techniek die het mogelijk maakt voor een fabrikant van een groot aantal apparaten om met geheime sleutels te werken. Hierbij kun je denken aan bankpassen, maar ook aan bijvoorbeeld muziekspelers. Dit idee stamt waarschijnlijk uit de jaren '80, maar is misschien nog wel ouder. Het bestaat in elk geval zolang als ik met cryptografie bezig ben. De fabrikant heeft voor elk apparaat een aparte geheime sleutel, zodat hij vercijferde gegevens met deze apparaten kan uitwisselen, terwijl hij zelf maar één sleutel hoeft te onthouden. De fabrikant hoeft alleen het 'recept' te onthouden waarmee deze sleutels worden berekend om van ieder apparaat de sleutel te bepalen. Het apparaat hoeft alleen zijn eigen sleutel te onthouden. Toch is het niet mogelijk om de gegevens van de apparaten te combineren, omdat ieder apparaat zijn eigen code heeft. Deze wonderlijke techniek maakt gebruik van een blokvercijfering. Een blokvercijfering[1] is een functie met twee variabelen (dit zijn gegevens met een vaste lengte, bijvoorbeeld 128 bits). Normaal noteren we: $C = E_k(M)$, en dit lees je als: C is de vercijfering van de boodschap M met de sleutel k.

Een blokvercijfering combineert de volgende eigenschappen:
- vercijferen: het berekenen van C uit k en M is gemakkelijk.
- oncijferen: het berekenen van M uit k en C is gemakkelijk: je schrijft gewoonlijk $M = D_k(C)$.
- kraken: het bepalen van k uit M en C is zeer moeilijk. Je kunt natuurlijk alle 2128 mogelijke waarden van k uitproberen; bij een goede blokvercijfering is dit voor zover bekend de 'snelste' manier.

Gebruikmakend van de eigenschappen van zo'n blokvercijfering kan de fabrikant naar alle apparaten vercijferde gegevens doorsturen. Daarvoor hoeft de fabrikant maar één geheime sleutel te verzinnen; laten we die K_f noemen. Op het moment dat de fabrikant een apparaat met nummer A maakt, voorziet hij het apparaat van zijn geheime sleutel K_A. Hij berekent de sleutel van het apparaat uit het serienummer: $K_A = E_{K_f}(A)$.

De getallen A en K_A worden vervolgens in het apparaat opgeslagen; de geheime sleutel K_A kan vervolgens door de fabrikant worden gebruikt om informatie met het apparaat uit te wisselen. Dit gaat ongeveer zo: de kaart wordt in blokjes data van 128 bits gesplitst. Blokje B_i wordt dan vercijferd tot $G_i = E_{K_A}(B_i)$, en het apparaatje, dat sleutel K_A heeft, berekent dan de blokjes weer terug als $B_i = D_{K_A}(G_i)$.

In de praktijk gaat dit als volgt: als ik een nieuwe kaart in mijn apparaat wil laden, ga ik naar de webstek van de fabrikant, en tik daar het serienummer A van mijn apparaat in. Dan kan ik de nieuwe wegenkaart downloaden. Deze nieuwe wegenkaart wordt door de fabrikant vercijferd met geheime sleutel K_A. De vercijferde wegenkaart gaat in mijn apparaatje, en die kan het ontcijferen met de sleutel die hij zelf heeft.

Stap 2: Adres invoeren

Nu we een kaart in ons apparaat hebben, kunnen we een adres invoeren waar we naartoe willen. Het apparaat bevat een enorme hoeveelheid adressen, die bliksemsnel worden opgezocht tijdens het invoeren van het adres. Bij mijn apparaat kun je de eerste paar letters van een stad invoeren, en in een fractie van een seconde verschijnt de lijst van alle steden in Europa die met deze letters beginnen. Dit valt onder indexeren van databases, en wordt normaliter gerekend tot de informatica[2]. Meestal wordt er gebruik gemaakt van een index, die voor alle combinaties van twee of drie letters een lijst bevat met de relevante plaatsnamen. Dit is op zich een ingewikkeld probleem, omdat je niet heel veel informatie wilt opslaan, terwijl je het opzoeken zo veel mogelijk wilt versnellen. Het ultieme voorbeeld is natuurlijk een zoekmachine, die miljarden internetpagina's in een index heeft staan en in een fractie van een seconde de relevante pagina's laat zien.

Meerdimensionaal zoeken

Nog interessanter wordt het als je bijvoorbeeld de dichtstbijzijnde parkeerplaats of restaurant bij een gegeven bestemming zoekt. (De meeste navigatiesystemen kunnen ook naar andere dingen zoeken, maar voor dit voorbeeld hebben we het over parkeerplaatsen.) Een alfabetische index is in zo'n geval betrekkelijk zinloos. Sterker nog, je kunt de plaatsen op geen enkele manier op een lineaire volgorde zetten waar je in kan zoeken. Het eerste waar je aan denkt, is om alle parkeerplaatsen in de database op te halen en dan op afstand te sorteren, maar dit is veel te tijdrovend, omdat het aantal parkeerplaatsen in het geheugen van het apparaatje zo groot is. Hier is dus wiskunde nodig.

Sinds er adressen in computers worden gestopt, was er behoefte aan het zoeken van dichtbijzijnde punten op een kaart. In het jargon heet dit *nearest neighbour search*. Dit onderzoek is in de jaren tachtig op gang gekomen. Een van de eerste efficiënte algoritmen is de zogenaamde *R-tree*, ontwikkeld door A. Guttman in 1984 (zie figuur 1).

Dit algoritme is één van de meest gebruikte op het ogenblik, en het is aan te nemen dat het navigatiesysteem dat ook gebruikt. Bij een *R-tree* wordt de kaart in een klein

aantal rechthoeken onderverdeeld; ieder van deze rechthoeken wordt weer in rechthoeken verdeeld, totdat je een klein rechthoekje hebt met alleen maar parkeerplaatsen. Als je iets op de kaart zoekt in de buurt van een punt, kijk je dus in welke rechthoeken dit punt ligt. Elk van deze rechthoeken is weer in kleinere rechthoeken verdeeld, en zo verder, tot je bij rechthoekjes komt van enkele kilometers groot met een paar parkeerplaatsen erin. Als je nu een parkeerplaats in de buurt zoekt, hoef je maar een paar rechthoeken te bekijken (van groot naar klein) om het rechthoekje te vinden waar je zelf zit; de parkeerplaatsen in de buurt zijn zo gevonden. Omdat de wereld niet netjes in rechthoeken is verdeeld, zullen de rechthoeken af en toe moeten overlappen. Een andere complicerende factor is dat je soms helemaal aan de rand van een rechthoek zit, zodat je de rechthoek ernaast ook moet proberen. Daarom moet je soms meerdere mogelijkheden proberen om de parkeerplaats te vinden. Ondanks deze complicaties levert deze manier van zoeken vrij snel een lijstje op van parkeerplaatsen in de buurt, die je dan verder kunt sorteren om een lijstje precies op afstand te krijgen.

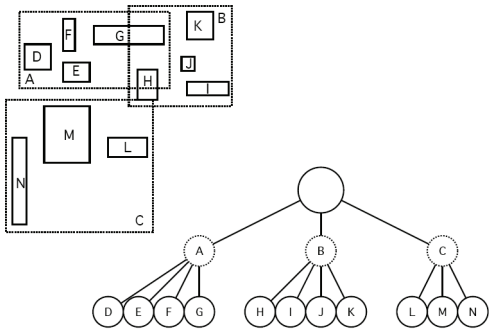

fig. 1 een R-tree

Stap 3: Kijken waar we zijn

Tijdens de reis moet het apparaatje weten waar we zijn. Daarvoor wordt uiteraard gebruik gemaakt van het inmiddels welbekende GPS: Global Positioning System. Hoewel GPS inmiddels heel 'gewoon' is, houdt dat niet in dat het een eenvoudig systeem is. Er wordt gebruik gemaakt van een aantal takken van wiskunde, waaronder:

– meetkunde
– coderingstheorie
– numerieke wiskunde

maar ook van de relativiteitstheorie uit de fysica.

De meetkunde van GPS

De precieze meetkunde van GPS wordt op allerlei plaatsen uitgelegd, maar niet altijd even correct. Ik zal het proberen losjes te doen, zonder de waarheid al te veel geweld aan te doen. Ruwweg gesproken zenden de satellieten van GPS een signaal uit dat de tijd aangeeft. Iedere satelliet is daarvoor uitgerust met een supernauwkeurige klok (met een absolute precisie van 1 nanoseconde!). De ontvanger krijgt van alle satellieten die hij kan zien een tijd te horen. Omdat hij zelf niet zo nauwkeurig weet hoe laat het is, kan hij alleen maar de verschillen in de tijd meten. Gebruikmakend van de bekende waarde van de lichtsnelheid, kan hij de relatieve afstanden bepalen.
Nu moeten we even wat meetkunde doen. In het platte vlak is de verzameling van punten die een gegeven verschil in afstand hebben tot twee gegeven punten een hyperbool. In de ruimte wordt dit een hyperboloïde (zie figuur 2). Als je het signaal van twee satellieten ontvangt, weet je dus dat je op een gekromd oppervlak zit, maar niet waar. Hier heb je dus niks aan: je weet nu nog steeds niet waar je bent, zelfs als je weet dat je op het aardoppervlak zit. Om een beetje een idee te hebben waar je bent, heb je minstens drie satellieten nodig.

Die drie satellieten leveren drie combinaties op, en daarmee drie gekromde oppervlakken. Die drie oppervlakken gaan door één (kromme) lijn[3], en weet je dus nog niet waar je bent. Als je rekening houdt met het feit dat je op de aarde staat, zijn er altijd nog twee verschillende oplossingen van de vergelijkingen. Daarom heeft een GPS in principe *vier* satellieten nodig om je positie te bepalen.

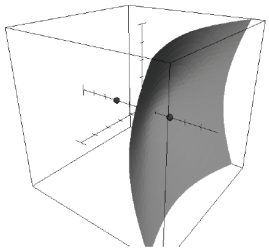

fig. 2 de verzameling van punten met een vast afstandsverschil

Omdat het vrijwel onmogelijk is om hier een duidelijk plaatje van te tekenen, laat ik de tweedimensionale variant zien; zie figuur 3. Iemand staat op een weiland, met op drie hoeken van het weiland een koekoeksklok. Hij heeft geen horloge om, maar hij heeft wel een stopwatch bij zich. Door goed te luisteren kan hij de drie klokken horen koekoeken, en de relatieve verschillen in tijd bepalen.

De koekoeksklokken heten *A*, *B* en *C*. Als hij de tijd tussen twee klokken weet, weet hij dat hij zich op een hyperbool bevindt. Deze krommen zijn de dikke lijnen aangegeven met *XA*-*XB*, *XA*-*XC*, en *XB*-*XC*. De lijnen gaan door één punt: het punt waar hij staat.

In het plaatje is de afstand tussen *B* en zowel *A* als *C* gelijk aan vier geluidsseconden (ongeveer 1,3 km), met een rechte hoek. Voor het gemak gaan we ervan uit dat het geluid ook zo ver draagt. De afstand tussen de dunne lij-

nen is 1 geluidseconde (ongeveer 330 m). Hij hoort eerst klok *A*, na één seconde klok *B*, en dan na 0,6 seconde *C*. Nadat onze held zijn positie heeft bepaald, kan hij ook de tijd bepalen: twee seconden voordat hij klok *A* hoorde, was op het hele uur.

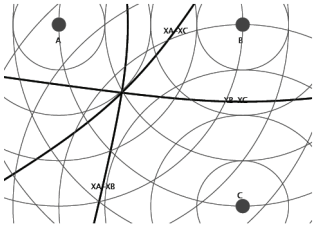

fig. 3 tweedimensionale versie van GPS

Ontvangen van het signaal

Een navigatiesysteem heeft geen richtinggevoelige antenne, en kan dus niet in de richting van een satelliet 'kijken'. De signalen van alle satellieten komen door elkaar binnen. Om het nog moeilijker te maken, zenden de satellieten ook nog allemaal op dezelfde frequentieband uit, zodat je ze ook niet door afstemmen uit elkaar kan houden. Verder is het signaal zo zwak dat het nauwelijks boven de ruis uit komt.

Om de signalen van de satellieten uit elkaar te houden, heeft iedere satelliet een eigen 'handtekening': de satelliet zendt een signaal uit dat bestaat uit een willekeurige lijkende reeks bits, die steeds wordt herhaald. Om het signaal van een satelliet te herkennen, moet het navigatiesysteem die reeks bits 'opvissen' uit de ruis door op de juiste manier naar het signaal te luisteren. Dit werkt min of meer op dezelfde manier als wat we zelf gebruiken als we in een ruimte met veel geluid naar een bekende stem luisteren.

Opvissen van het signaal

Het geheim van het opvissen van zo'n signaal is het gebruikmaken van het bekende patroon om het signaal te herkennen. Laten we eerst eens precies kijken hoe het signaal eruit ziet. Het signaal is een combinatie van drie signalen. Figuur 4 laat zien hoe deze signalen worden gecombineerd.

– draaggolf: een sinusgolf van 1,57542 GHz;
– de code: om het signaal te herkennen wordt een reeks van 1023 bits gecodeerd, de C/A-code[4], herhaald met een frequentie van 1023 kilobits/s (dus hij herhaalt precies iedere milliseconde, en dit zijn precies 1540 golven van de draaggolf);
– navigatiebericht: een signaal van 50 bits per seconde (dus iedere bit bevat precies 20 herhalingen van de C/A-code).

De draaggolf is een sinusgolf, die 1540 cycli doorloopt, en bij een 1 bit van de C/A-code wordt 'omgeklapt'. (Als er dus een overgang is van 0 naar 1 of omgekeerd, zie je de draaggolf een rare bult krijgen.) Omdat er zo veel storing is, kun je de C/A-code pas goed detecteren als je de code al weet.

Deze zendtechniek wordt *carrier division multiple access* (CDMA) genoemd. De C/A-codes zijn zodanig ontworpen dat je de verschillende berichten door elkaar kan ontvangen. Hiervoor moeten de codes zó zijn dat ze minimaal zijn als ze met elkaar worden vermenigvuldigd, of met een verschuiving van zichzelf. Dit is een onderdeel van de *coderingstheorie*.

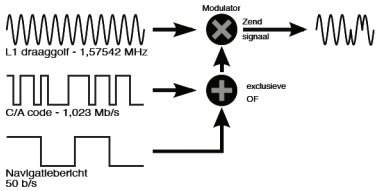

fig. 4 hoe het GPS signaal in elkaar zit

Het decoderen van het signaal is in principe eenvoudig: de ontvanger vergelijkt een zelfgemaakte draaggolf met C/A-code met het ontvangen signaal erop, en hij neemt het gemiddelde over een bepaalde periode; alleen bij de juiste C/A-code komt er een sterk signaal uit.

De truc is om het signaal met een sinusgolf te *vermenigvuldigen*, en het resultaat over de tijd te middelen. Als je twee identieke sinussignalen, vermenigvuldigt, wordt het resultaat steeds positief. Het 'omgeklapte' signaal wordt negatief; je kunt de bits van de C/A-code dan zien. Het signaal is te zwak om dit zo maar te zien; als hij de juiste C/A-code 'raadt', kan hij het signaal wel herkennen door te kijken hoe vaak de werkelijke code klopt met het ontvangen signaal. Bovendien zal als gevolg van het Doppler-effect het signaal een hogere of lagere frequentie krijgen, dus ook daar moet hij naar zoeken. Als je op een GPS-ontvanger de signaalsterkte afleest, kijk je feitelijk naar het gedeelte van de tijd dat de C/A-code klopt met de juiste code.

Samenvattend is het een beetje te vergelijken met een vlieg vangen in het donker. En dan te bedenken dat moderne GPS-ontvangers meerdere satellieten tegelijk bijhouden. Bovendien gebruiken ze het signaal van de satellieten die ze al hebben opgepikt om het zoekwerk van de andere satellieten te verkleinen! Voor het gemak gaan we er van nu af aan van uit dat deze problemen zijn opgelost.

Het navigatiebericht

Iedere twintig herhalingen van de C/A-code wordt dit op zijn beurt ook weer 'omgeklapt' als de bijbehorende bit van het navigatiebericht een 1 is. Dit navigatiebericht bevat de informatie die nodig is voor de ontvanger om de plaatsbepaling te doen. Het bericht, dat steeds wordt herhaald, bestaat uit 1500 bits, die in dertig seconden worden uitgezonden. Dit bericht bevat de volgende informatie:

– de tijd;
– datum in de vorm van het GPS-weeknummer;
– status van de satelliet;
– exacte beschrijving van de baan van de satelliet (de *ephemeris*), deze wordt iedere paar uur bijgewerkt;
– $\frac{1}{25}$ deel van de *almanak*: een lijst van alle satellieten (met grove baanbeschrijving) en beschrijving van de ionosfeer. Het duurt dus $12\frac{1}{12}$ minuut om de hele lijst te ontvangen; een slimme ontvanger onthoudt de almanak natuurlijk om de volgende keer sneller te kunnen opstarten.

Als de ontvanger ondanks alle moeilijkheden een navigatiebericht van een satelliet heeft weten te ontvangen, weet hij de exacte positie van de satelliet op het moment dat het bericht is verstuurd.

Als hij op deze manier van vier satellieten met voldoende nauwkeurigheid de berichten heeft ontvangen, kan hij aan het rekenen gaan slaan om de vier gebogen oppervlakken met elkaar te snijden.

Nauwkeurigheid
Hoewel het gemakkelijk lijkt om de plaats te bepalen, is er nog een aantal complicerende factoren die de nauwkeurigheid van GPS beïnvloeden:

1. om te beginnen loopt een klok onder invloed van de zwaartekracht ietsje langzamer, als gevolg van de relativiteitstheorie;
2. verder, ook als gevolg van de relativiteitstheorie, loopt een klok die door de ruimte beweegt langzamer;
3. als gevolg van het Sagnac-effect, wordt de tijd 'verbogen' door de draaiing van de aarde (sterker nog: het begrip 'tegelijk' verliest zijn betekenis!);
4. de klok van het apparaat zelf loopt relatief onnauwkeurig voor dit soort precisieberekeningen (bedenk dat zelfs een supernauwkeurig kristal van 1 ppm na één seconde al een afwijking van een μs geeft, overeenkomend met 300 meter!);
5. de snelheid van het licht in de ionosfeer is iets langzamer dan de andere luchtlagen, waardoor de signalen worden vertraagd en verbogen;
6. het signaal wordt soms gereflecteerd door nabijstaande gebouwen;
7. om het maar niet over zonnevlekken, geomagnetische stormen, andere elektronica, en andere dingen te hebben die het signaal moeilijk te ontvangen maken.

De verschijnselen 1 en 2, die elkaar gedeeltelijk opheffen, worden gecorrigeerd door de klok van de satellieten een tikje verkeerd te laten lopen. Op het moment dat de satellieten worden gelanceerd, lopen ze 38μs per dag (of 1 seconde per 72 jaar) achter; nadat ze zijn gelanceerd lijken ze precies goed te lopen. Hoewel dit verschil miniem lijkt, zou je er een paar kilometer naast zitten als dit niet werd gedaan!

Verschijnsel 3, het Sagnac-effect, wordt gecorrigeerd door de tijd om te rekenen met een Lorentz-transformatie (de details zal ik u besparen).

De nauwkeurigheid van het kwartskristal in de klok van het apparaat, punt 4, kan worden gemeten (er is immers een zeer precieze tijdmeting uit het satellietsignaal te halen) en er kan een schatting worden berekend van de afwijking.

De afwijking als gevolg van de ionosfeer, punt 5, wordt door de ontvanger gecorrigeerd; vandaar dat er een model van de ionosfeer in de almanak zit.

Onnauwkeurigheid en numerieke wiskunde
Het is duidelijk dat we met een bepaalde onnauwkeurigheid moeten leven. Deze afwijking kan worden verkleind door meerdere satellieten in de berekening mee te nemen; de kunst is om de tegenstrijdige informatie zó te interpreteren dat je de meest waarschijnlijke uitkomst vindt. Het gaat dus om het zoeken van de mogelijke afwijkingen van de *invoergegevens* die de uitkomst verklaren: dit heet een *foutanalyse*. De techniek om de nauwkeurigheid van een berekening in te schatten is een onderdeel van de numerieke wiskunde. In de negentiende eeuw is men begonnen met het maken van dit soort berekeningen voor de landmeetkunde, maar pas nadat de computer is uitgevonden, heeft dit zich verder ontwikkeld. Het eerste artikel over 'moderne' numerieke wiskunde heette *Numerical Inverting of Matrices of High Order* en is gepubliceerd in het *Bulletin of the American Mathematical Society* in november 1947. Het was geschreven door één van de briljantste wiskundigen ooit: John von Neumann. Hij introduceerde het 'conditiegetal': een getal dat aangeeft hoe moeilijk de inverse van een matrix is te bepalen; dit is nog steeds standaardkost voor wiskundestudenten. Voor dit artikel dachten veel wiskundigen dat de uitkomsten van bepaalde berekeningen onnauwkeurig waren omdat de computer te veel fouten maakte; John von Neumann liet zien dat een afwijking in de nauwkeurigheid een gevolg kon zijn van de onnauwkeurigheid van de gegevens zelf. Vanaf dat moment is men zich serieus met numerieke wiskunde gaan bezighouden.

Het principe van het gebruik van meerdere satellieten is dat de ontvanger bepaalt wat een gegeven onnauwkeurigheid in bijvoorbeeld de dikte van de ionosfeer als gevolg heeft voor de plaatsbepaling. De hele berekening wordt als het ware 'achteruit' gedaan; op die manier kan de meest waarschijnlijke oorzaak van de afwijking worden bepaald, zodat de plaatsbepaling zo nauwkeurig mogelijk is. Een goede GPS kan ook nog schatten hoe nauwkeurig de uitkomst uiteindelijk wordt. Deze berekening is veel te moeilijk voor mij, en die laat ik in dit verhaal dus maar weg.

Stap 4: De route uitzoeken

Nu weet het apparaat waar je naar toe wilt, en waar je bent. Het eenvoudige geval van het bepalen van het kortste pad naar een gegeven punt in een graaf is opgelost door Edsger Dijkstra in 1959. Het speciale geval van het bepalen van het kortste pad tussen twee punten in een graaf, gebruikmakend van schattingen van de kosten naar het eindpunt, heet het A* algoritme en stamt uit 1968.

Hoewel het A* algoritme nog steeds het meest gebruikte algoritme is, zijn er nog tientallen andere algoritmen en varianten bedacht. Ook de laatste paar jaar gaat de research nog verder, bijvoorbeeld rekening houdend met verboden afslagen, tijdverlies van afslaan ten opzichte van doorrijden, en dergelijke.

Ingrid Flinsenberg is op 30 september 2004 gepromoveerd op het onderwerp routeplanning van autonavigatiesystemen: nieuwsgierige lezers kunnen dit gemakkelijk op het internet vinden. Zij laat zien dat je in ongeveer evenveel tijd als het standaardalgoritme een weg kan berekenen die altijd optimaal is, met een geringe extra hoeveelheid geheugengebruik. In haar experimenten scheelt dit al gauw enkele procenten op de lengte van de route!

Om het A* algoritme in de praktijk te gebruiken, gebruikt het apparaat een vereenvoudigde versie van de kaart, door de kleinere wegen alleen in de buurt van vertrek- en eindpunt in beschouwing te nemen. Hiervoor zijn alle wegen op de kaart geclassificeerd, zodat het apparaat efficiënt de juiste wegen kan weglaten om de rekentijd binnen de perken te houden. (Dit betekent dat zo'n navigatiesysteem moeite heeft met routes die ergens in het midden een 'kleine' weg hebben.)

Nog meer. . .

Ik heb nog lang niet alles laten zien, maar het verhaal is al aan de lange kant. De volgende onderdelen zal ik alleen maar noemen:

- Tekenen van letters op een beeldscherm, gedraaid en vergroot of verkleind.
- Compressie van het geluid (MP3) zodat al deze zinnetjes in het beperkte geheugen van het apparaat passen (Fouriertheorie).
- Het bewerken van het geluid zodat het zelfs door het kleine luidsprekertje nog duidelijk verstaanbaar er uit komt.

In elk geval heeft het apparaat mij een tijdje leuk bezig-gehouden.

Jurjen Bos
Interpay Nederland BV, Utrecht

Noten

[1] Op het ogenblik is de meest voorkomende blokvercijfering aes: de Advanced Encryption Standard. Bij aes zijn zowel k als m getallen van 128 bits.

[2] Sommigen vinden informatica ook een tak van wiskunde; daar ga ik verder geen ruzie over maken.

[3] In het algemeen gaan drie oppervlakken niet door één lijn, maar hier wel, omdat de drie vlakken niet onafhankelijk zijn.

[4] c/a staat voor 'Coarse/Acquisition': dit duidt aan dat de code wordt gebruikt voor 'grove' positionering en het ophalen van gegevens over de andere satellieten. Er is ook een gecodeerd P-signaal, dat het voor militaire toepassingen mogelijk maakt om nog veel nauwkeuriger de plaats te bepalen.

Wintersymposium KWG – 10 januari 2009 te Utrecht

Wiskunde een Kunst

Dit wintersymposium van het Koninklijk Wiskundig Genootschap staat in het teken van wiskunde en kunst.

Ferdinand Verhulst, hoogleraar (em.) dynamische systemen aan de Universiteit Utrecht, opent het symposium met een voordacht over wiskunde en literatuur.

Aline Honingh, *research fellow* in de Music Informatics Research Group aan de City University in Londen, zal spreken over wiskunde en muziek.

Albert van der Schoot, als kunst- en cultuurfilosoof verbonden aan de faculteit Geesteswetenschappen van de Universiteit van Amsterdam, en als lector Kunst en Reflectie aan ArtEZ Hogeschool voor de Kunsten, sluit het symposium af met een lezing over de geschiedenis van de gulden snede.

Het symposium wordt gehouden in het Academiegebouw van de Universiteit Utrecht. Het programma start om 10.00 uur en eindigt ca. 14.45 uur.

U wordt verzocht u van te voren on line aan te melden via de website van het Koninklijk Wiskundig Genootschap www.wiskgenoot.nl ('wat doet het KWG' -> 'congressen en symposia'). Daar is ook het volledige programma, inclusief samenvattingen van de lezingen, te vinden.

De kosten voor het symposium bedragen € 17 voor KWG-leden en € 22 voor niet-leden. Deze bijdrage is onder andere voor een lunch en andere consumpties gedurende de dag.

Nadere inlichtingen bij Iris van Gulik:
gulikgulikers@home.nl of 038-4536366