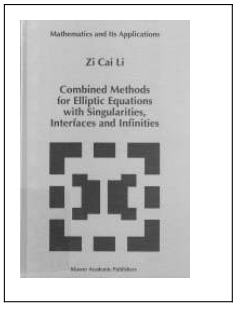
aardige, sprekende voorbeelden en anecdotes. Een boek als dit bevat onvermijdelijk de nodige onnauwkeurigheden: zo wordt niet of te laat opgemerkt dat de normale benadering van de binomiale verdeling alleen te gebruiken is als het aantal waarnemingen, n, voldoende groot is. Een geslaagd boek voor de doelgroep met heel bruikbare elementen voor ieder die statistiekonderwijs verzorgt. *J.Th.M. Wijnen*

B.S. Everitt

The Cambridge dictionary of statistics

Cambridge: Cambridge University Press, 1998.
360 p., prijs £19.95
ISBN 0-521-59346-8

Dit statistisch woordenboek geeft omschrijvingen voor termen uit alle gebieden van de statistiek voor zowel specialisten als niet-specialisten. Sommige definities bevatten alleen tekst, andere vereisen mathematische formules en nomenclatuur, hopelijk passend bij de behoefte van de lezer. Het boek beschrijft ongeveer 3000 lemma's en geeft een honderdtal korte biografieën van belangrijke statistici. Waar nodig wordt daarbij verwezen naar relevante boeken of tijdschriftartikelen en naar de door de auteur gebruikte bronnen. In zijn voorwoord geeft de auteur al aan dat zijn keuze van termen voor een deel bepaald wordt door zijn eigen interesses, zodat een lezer wel eens mis zal grijpen als zijn belangstelling op een ander terrein ligt. Dat geldt bijvoorbeeld voor iemand, die begrippen uit de industriële statistiek zoekt: de lemma's Pareto chart, EWMA chart, producers' risk, consumers' risk, capability index, noise factor staan er niet in. En er zijn er ongetwijfeld meer, ook uit andere gebieden van de statistiek. Niettemin lijkt dit boek me voor velen die zich op de een of andere manier met statistiek bezig houden een redelijk geprijsd en heel bruikbare aanvulling van de eigen bibliotheek. Ook iemand die in het bezit is van het bekende *A dictionary of statistical terms* van Kendall en Buckland (Marriott bewerkte de 5de editie) kan er zijn voordeel mee doen: de overlap tussen beide woordenboeken is merkwaardig klein (vergelijk een bespreking van dit boek door J. Dragt in Kwantitatieve Methoden, 20, 159-160, 1999). Bovendien bevat het boek van Marriott geen biografieën. *J.Th.M. Wijnen*



Z.C. Li

Combined methods for elliptic equations with singularities, interfaces and infinities

Dordrecht: Kluwer, 1998.
476 p., prijs NLG 395,–
(Mathematics and its Applications; 444).
ISBN 0-7923-5084-7

Voor het numeriek oplossen van elliptische partiële differentiaalvergelijkingen over begrensde domeinen, met bijpassende randvoorwaarden, zijn tal van methoden bekend. Ik noem slechts de Eindige differentiemethode, de Eindige volumemethode, Eindige elementen en collocatie. Elk van deze methoden heeft zijn specifieke sterke en zwakke kanten en het ligt voor de hand om problemen, waar de oplossing over deeldomeinen verschillend gedrag vertoont, met verschillende methoden per domein aan te pakken. Men kan hierbij denken aan een deeldomein rond een singulariteit, deeldomeinen waar de oplossing lokaal sterk varieert, en deeldomeinen waar de oplossing voldoende glad is.

Natuurlijk moeten de numerieke technieken goed op elkaar aansluiten; de verschillende deeldomeinen kunnen bijvoorbeeld met verschillende roostergroottes gediscretiseerd worden. Het is dan niet de bedoeling dat approximatiefouten op het ene deeldomein de oplossing op een ander deeldomein essentieel veranderen. Dit soort aansluitingsproblemen wordt wel gerangschikt onder de *interface* problemen. Het is een mooi onderwerp dat een zorgvuldige studie verdient.

Het te bespreken boek richt zich op het zinvol aaneenkoppelen van deeldomeinen voor elliptische problemen met singulariteiten (bijvoorbeeld in een hoek of ergens langs de rand van een domein). Het is wel jammer dat het boek beperkt blijft tot tweedimensionale problemen. Echter, ook zonder dit aspect wekte het boek bij mij al snel verbijstering op. Hoe kan een uitgever een wetenschappelijk werk zo onzorgvuldig doen uitgeven? Het boek zou geschikt moeten zijn voor *graduate courses*, maar als voorbeeld voor hoe het niet moet, lijkt het me veel te duur. Niet alleen is het Engels abominabel, ook bevat het boek tal van fouten en nietszeggende zinnen. De index is zeer onvolledig en de afwijkende symbolen zijn wel in een lijst opgenomen, evenwel zonder verwijzing naar de pagina waar ze gedefinieerd zijn. De referenties worden op bizarre wijze, vrijwel zonder enige toelichting, aan het eind van hoofdstukken op de lezer afgevuurd. Pagina 51 bestaat bijvoorbeeld vrijwel uitsluitend uit namen en jaartallen. Deze publicaties worden aangekondigd als *reports*, of voorafgegaan door een zin als *'The references on CM are given in . . .'*.

Stellingen en Lemma's volgen elkaar in hoog tempo op, vrijwel zonder commentaar, en vaak zonder bewijs of adequate verwijzing, en het komt niet zelden voor dat een sectie plompverloren eindigt met een stelling of corollarium. Die verwijzingen zijn, gezien het grote aantal fouten en onvolkomenheden in de formuleringen, wel van essentieel belang. Lemma's en stellingen worden dan vaak nog voorafgegaan door een verhelderende zin als *Below we give a lemma.* De lezer van deze recensie verwacht ongetwijfeld enkele voorbeelden. Die kan hij op vrijwel elke pagina van dit boek aantreffen, maar vooruit, hier een paar illustraties.

Op pagina 50 worden de *Tefttz procedures of Trefflz (1926)* genoemd. De auteur blijkt in de referentie *Trefftz* te heten maar wordt niettemin verder nog aangeduid als *trefftz* en *Trafftz*. Voor de numerieke vergelijking van verschillende technieken wordt het zogenaamde *Motz's problem* gebruikt. Rond een singulariteit op de rand wordt de oplossing in een reeks ontwikkeld en verschillende oplosmethoden worden beoordeeld op het aantal correcte decimalen, rekenend in ongeveer 15 decimalen, waarin de coëfficiënten van de reeks worden afgeleverd. Om dit te kunnen vergelijken zijn de eerste 10 coëfficiënten in ongeveer 1000 (!) decimalen afgedrukt (Tabel 2.1, blijkens het bijschrift berekend *. . .'using Mathematics with* 1000 *siginficent digits'*).

Ook een aardige opmerking, pagina 47, is *'. . .the mesh generation and entry evaluation of the associated matrix consume a lot of CPU time, although they can be done by computer'*. Dit mag nog als ongelukkig Engels overkomen, echter ook elders geeft de auteur blijk van zijn onwetendheid van het numerieke werk. We lezen op pagina 44 dat voor een groot overbepaald stelsel *'. . .a better method is . . .using the singular value recomposition in Go-*

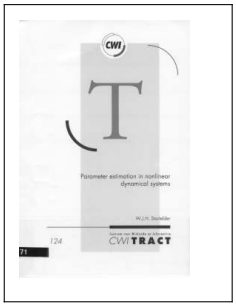
lub and Loan (1989) . . .'. Afgezien van het feit dat deze zin meerdere fouten bevat en naar een oude versie van het boek van Golub en Van Loan schijnt te verwijzen, wordt de meer efficiënte QR-decompositie niet eens genoemd, om over iteratieve technieken nog maar te zwijgen. Deze zijn cruciaal voor het oplossen van het soort stelsels dat in de besproken applicaties optreedt; de niet nader aangeduide stelsels zouden met SVD slechts voor relatief lage orde oplosbaar zijn. Halverwege pagina 119 merkt de auteur op: *'. . .we need to estimate the values of condition numbers using the least squares method (see Golub and Loan (1989).'*

Lineaire stelsels worden om de haverklap opgevoerd als $Ax = b$, keurig met formule nummer, evenwel zonder ook maar A, of b te specificeren (zie bijvoorbeeld pagina 8). Er zijn in het boek dus vele stelsels $Ax = b$, allemaal kennelijk verschillend en daarom allemaal van hun eigen nummer voorzien, maar vrijwel nergens gespecificeerd. Zo'n niet gespecificeerde matrix is dan bijvoorbeeld wel *'. . .M-Matrix-like (see Varga (1962))'*, zie pagina 33. Op pagina 59 lezen we *'In this book, the analytic functions are said if* $u \in X^{\infty}(S)$*; the singularity exists at some points if the solution derivatives there are unbounded, often being as* $u = \mathcal{O}(r^{\alpha})$*'*. Op pagina 50 leest men *Because of the fewer requirements A1 . . .*; bedoeld is waarschijnlijk dat *A1* een zwakkere aanname is. Overigens, men zoekt de aanname *A1* vergeefs in de Index; men komt twee verschillende aannamen in het boek tegen (pagina 49 en 214).

Pagina 81: *The conception of infinity element methods is interesting, since the refinements can go over and over without an end. However, from the viewpoint of application, the local refinements do not need to go to the limitation, for the accuracy required in application is not very small, though. Note that the examples shown in Thatcher (1976, 1978) are a kind of combinations, the combinations of FEM and the infinitesmall elements methods.'*

Ach, ik kan zo wel door blijven gaan, ik heb pagina's vol met aantekeningen over de meest opvallende eigenaardigheden. Wat dacht u van het volgende begin van een bewijs (pagina 314): *'Let* u *be the exact solution of* u*.'*? Het vervelende is dat het ook niet eenvoudig is om na te gaan wat de auteur dan wel bedoeld kan hebben.

Wellicht kan de uitgever de reeds verspreide exemplaren nog terugnemen en vernietigen. Ik zou me als koper van dit boek, afgaand op de goede naam van de uitgever en het onderwerp, toch redelijk opgelicht voelen. *H.A. van der Vorst*



W.J.H. Stortelder

Parameter estimation in nonlinear dynamical systems

Amsterdam: CWI, 1998.
176 p., NLG 40,–
(CWI-tract; 124).
ISBN 90-6196-482-2

This monograph studies statistical and numerical aspects in the estimation of parameters in sets of nonlinear differential algebraic equations (DAEs). Often, on the basis of physical modeling principles a model class is identified that describes some dynamical process. One basic premise in the modeling is that the proposed class is rich enough as to include the 'true' system; in other words, it is assumed there exists a specific model in the model class that matches with the measurements available. In the above text, the model class consists of parametrized DAEs, and thus the basic problem studied is that of 'identifying' the parameters on the basis of — possibly noisy — discrete time measurements. Different fitness criteria that may be used for the parameter estimation are discussed. These include the weighted least squares, where as to be minimised criterion the weighted mean square error is used, or the total least squares method (Chapter 2), maximum likelihood estimation and L1-estimation methods (Chapter 3). Some further aspects on nonlinear regression theory are reviewed in Chapter 4. A short discussion on optimal experiment design — for example, how to improve the measurements — is given in Chapter 5. A large part of the book is dedicated to the case studies given in Chapter 6. These (practical) examples are from various areas and include bio-chemical models, macroeconomic time series and chemical processes. Finally, Chapter 7 describes the software used in the worked examples, which is contained in the software package simulation and parameter Identification in dynamical systems (spIds). For the specialist, this book — a rewrite of the author's dissertation — may offer interesting and useful reading. *H. Nijmeijer*

O. Goldreich

Modern cryptography, probabilistic proofs and pseudorandomness

Berlin: Springer-Verlag, 1999.
182 p., prijs DM 29,–
(Algorithms and combinatorics; 17).
ISBN 3-540-64766-X

This is the first book entirely devoted to theoretical aspects of modern cryptography and some closely related topics. Modern cryptography is about rigorous analysis of cryptosystems, digital signatures schemes and protocols for more general tasks, often relying on number-theoretic intractability assumptions or the assumption that $P \neq NP$. Since the introduction of public cryptography by Diffie and Hellman in 1976 and the subsequent invention of RSA, a huge amount of work has been done to deal with these fundamental cryptographic tasks. Over the past ten years an increasing number of cryptography textbooks have been written, opening up the topic to a wide audience of practitioners.

The present book aims at extending the horizon to the advances that have been made in establishing suitable foundations for cryptographic systems. Here, Goldreich distinguishes the *definitional activity*, which strives to find the right concepts and definitions, and the *constructive activity*, which shows what kind of tasks can be feasibly implemented, how and under which assumptions. For instance, when exactly a signature scheme is to be considered secure, falls in the first category; corresponding results from the second category are that signature schemes exist iff one-way functions exist, and also what signature schemes can be constructed assuming that the RSA function cannot be inverted.

Chapter 1 elaborates on these aspects and gives an impression on what has been achieved in this area, not by showing the detailed results but by focusing on the essentials. The general frame-