Elem. Math. 61 (2006) 179 – 180
0013-6018/06/040179-2

Elemente der Mathematik

Bücher und Computersoftware

A. Beutelspacher, H.B. Neumann und T. Schwarzpaul: Kryptografie in Theorie und Praxis. Mathematische Grundlagen für elektronisches Geld, Internetsicherheit und Mobilfunk. xiii + 319 Seiten, sFr 43.70. Vieweg, Wiesbaden, 2005; ISBN 3-528-03168-9.

De nombreux ouvrages publiés ces dernières années traitent de la cryptographie; en revanche, ils ne sont pas nombreux à aborder à parts égales les aspects théorique et pratique dans un même volume. *Kryptografie in Theorie und Praxis* est découpé en trois volets de pondérations plus ou moins égales: chiffrements symétriques, cryptographie asymétrique et applications. En 300 pages, les auteurs présentent les concepts fondamentaux des systèmes passés et présents, touchent aux questions actuelles de la sécurité et présentent des méthodes utilisées dans la technologie actuelle.

La première partie inclut une description des principaux chiffrements à caractère historique; les auteurs abordent ensuite, après avoir introduit un certain formalisme, les concepts de sécurité parfaite et sécurité performante. Finalement, des exemples de chiffrements par blocs (essentiellement DES et AES) sont présentés et critiqués.

La deuxième partie de l'ouvrage (cryptographie asymétrique) aborde essentiellement l'algorithme RSA et le problème du logarithme discret, mais présente aussi d'autres systèmes à clé publique comme le chiffrement et la signature de Rabin ou le problème du knapsack; dans chaque cas, les idées principales sont présentées et des références complètent l'exposé.

Finalement, le livre présente de nombreux protocoles utilisés dans la technologie actuelle (argent électronique, sécurité internet, téléphonique mobile). Ne sont pas oubliés les protocoles les plus courants liés à la sécurité sur internet comme Secure Sockets Layer.

Cet ouvrage constitue une bonne référence de départ pour aborder les systèmes ou algorithmes usuels en cryptographie; ces derniers sont généralement accompagnés de figures explicatives. Des exercices en fin de chapitre permettent de vérifier ses connaissances. Bien que les concepts (et non la technique) soient mis en avant dans l'ouvrage, ce dernier présente aussi les fondements mathématiques: par exemple, le chapitre sur l'algorithme RSA contient tous les résultats mathématiques nécessaires à justifier sa construction. La grande force de cet ouvrage est d'aborder une riche palette de protocoles et d'algorithmes sans entrer dans les détails, tout en donnant de nombreuses références récentes. Dans cette optique, ce livre se prête bien à un cours d'introduction.

Marc-Adrien Schnetzer, Fribourg

D.A. Grier: When Computers Were Human. 411 Seiten, $ 35.00. Princeton University Press, 2005; ISBN 0-691-09157-9.

Ce livre intéressant nous montre les relations qu'il y a entre les différentes révolutions industrielles et les mathématiques, ces dernières permettant d'améliorer les processus industriels. Pour ceci, il était nécessaire de faire énormément de calculs répétitifs en parallèle. Un premier exemple de ce type de calcul a été utilisé en 1758 afin de prédire à quelle date la comète de Halley serait de retour vers la Terre. Afin améliorer la rapidité et la précision des calculs, et pour diminuer leurs erreurs, différentes calculatrices mécaniques ont été réalisées durant le 19e siècle: Babbage, Scheutz, Hollenrith, ...

Ce livre montre aussi l'influence qu'a eue la première guerre mondiale sur les méthodes de calcul durant le projet Aberdeen qui était l'équivalent du projet Manhattan de la 2e guerre mondiale. Ces méthodes ont permis de mieux gérer la production agricole des Etats-Unis d'Amérique afin de pouvoir nourrir l'Europe durant ce conflit. Lors de la récession des années 1930, le projet WPA (Work Projects Administration) a permis à des personnes sans emploi de calculer différentes tables mathématiques de grande précision. Lors de l'arrivée des premiers ordinateurs, les ≪calculateurs humains≫ se sont convertis et ont montré comment décomposer des algorithmes complexes en différentes étapes plus simples et facilement programmables.

Jean–Roland Schuler, Fribourg

Olivier Gascuel (Hrsg.): Mathematics of Evolution and Phylogeny. 448 Seiten, £45.00. Oxford University Press, UK, 2005; ISBN 0-19-856610-7.

Die schnelle Entwicklung molekularer Methoden, die in den letzten Jahren stattgefunden hat, ermöglicht es, immer grössere Anteile der DNA-Struktur von Tier- und Pflanzenarten zu entschlüsseln. Nach der Sequenzierung des menschlichen Genoms und des Gencodes zahlreicher weiterer Modellorganismen (wie zum Beispiel der Maus) können nun die Analysen erweitert und neue Erkenntnisse gewonnen werden. Um die geschichtliche Entwicklung von Arten und Populationen zu verstehen, werden Informationen über Populations- und Sequenzunterschiede in den Kontext der Evolutionstheorie gesetzt. Seit den Untersuchungen von Avery in den vierziger Jahren des vorigen Jahrhunderts wissen wir, dass die DNA die Trägerin der Erbinformation ist. Sie ist aber mehr, sie ist (in den Worten von Linus Pauling) „ein Dokument der Evolutionsgeschichte". Sie hat sich im Verlauf der Evolution verändert, und der Prozess hat in den Genen der heute lebenden Organismen Spuren hinterlassen. Mittels mathematischer Modelle und statistischer Verfahren versuchen die Evolutionsgenetiker, diesen Prozess zu rekonstruieren und die Mechanismen herauszufiltern, die zur heutigen Vielfalt des Lebendigen geführt haben. Mit der zunehmenden Komplexität dieser Modelle steigen auch die Anforderungen an die zu evaluierenden Daten. Für den Anwender wird es daher immer wichtiger, Annahmen und Limitierungen der Modelle genau zu kennen. Das vorliegende Buch gibt einen guten Überblick über die meistbenutzten Grundkonzepte von evolutionären und phylogenetischen Studien.

Mathematics of Evolution and Phylogeny entstand im Anschluss an eine internationale Konferenz, die im Jahre 2003 am Institut Henri Poincaré in Paris stattfand. Die Hauptvortragenden wurden gebeten, in einem Übersichtsartikel die wichtigsten Erkenntnisse ihres Fachgebiets zusammenzufassen. So entstand eine Sammlung von Artikeln zu diversen Themen der molekularen Phylogenetik. Da alle Autoren auf ihrem Gebiet ausgewiesene Experten sind, repräsentiert das Buch den *state of art* dieser rasant sich entwickelnden Wissenschaft. Die Artikel erläutern die Methoden, mit denen die gesammelten genetischen Daten – diese sind grösstenteils in öffentlichen Datenbanken zugänglich – interpretiert werden. Die heute bekannten Analysen und ihre mathematischen Grundlagen werden auf vielen verschiedenen Ebenen beschrieben; neben den gebräuchlichen statistischen Tests zu Sequenzunterschieden und Genvergleichen werden auch Analysen von ganzen Genomen und Arten diskutiert. Einen sehr guten Überlick bietet die Einführung des Herausgebers, in der die vierzehn Kapitel des Buches in kurzen Abschnitten zusammengefasst und die wichtigsten Punkte hervorgehoben werden. Die Einführungen zu den verschiedenen Themen am Anfang jedes Kapitels sind sehr umfassend, so dass man das Buch sowohl als allgemeine Einführung in das Gesamtgebiet als auch als Nachschlagewerk für Informationen zu Einzelthemen gebrauchen kann. Die Texte sind verständlich geschrieben, die Abbildungen und Formeln klar erläutert. Die übersichtliche Gliederung der einzelnen Themen ermöglicht ein rasches Auffinden der mathematischen Erklärungen, welche in diesem Umfang in anderen Werken zur Genetik und in Programmierhandbüchern oft fehlen. Das Buch ist insbesondere geeignet für jene Anwender evolutionärer und phylogenetischer Modelle, welche den Aufbau derselben nachvollziehen und ihre mathematischen Hintergründe besser verstehen möchten. Doch auch Bioinformatiker und Mathematiker, die sich für biologische Themen interessieren, werden ihr Wissen aufbauen oder erweitern können. Das Buch schlägt eine Brücke zwischen der modernen Biologie und der Mathematik und liefert in diesem Sinne einen wichtigen Beitrag zu einer noch engeren interdisziplinären Zusammenarbeit.

Sabine Fink, Bern

Typesetting & Layout: *mathScreen online, CH-4123 Allschwil*