Cambridge studies in advanced mathematics 169

Geometry and Complexity Theory

J. M. LANDSBERG

Two central problems in computer science are P vs NP and the complexity of matrix multiplication. The first is also a leading candidate for the greatest unsolved problem in mathematics. The second is of enormous practical and theoretical importance. Algebraic geometry and representation theory provide fertile ground for advancing work on these problems and others in complexity.

This introduction to algebraic complexity theory for graduate students and researchers in computer science and mathematics features concrete examples that demonstrate the application of geometric techniques to real-world problems. Written by a noted expert in the field, it offers numerous open questions to motivate future research. Complexity theory has rejuvenated classical geometric questions and brought different areas of mathematics together in new ways. This book will show the beautiful, interesting, and important questions that have arisen as a result.

J. M. Landsberg is Professor of Mathematics at Texas A&M University. He is a leading geometer working in complexity theory, with research interests in differential geometry, algebraic geometry, representation theory, the geometry and application of tensors, and, most recently, algebraic complexity theory. The author of more than 60 research articles and 4 books, he has given numerous intensive research courses and lectures at international conferences. He co-organized the Fall 2014 semester "Algorithms and Complexity in Algebraic Geometry" at the Simons Institute for the Theory of Computing and served as the UC Berkeley Chancellor's professor during the program.

CAMBRIDGE UNIVERSITY PRESS
www.cambridge.org

ISBN 978-1-107-19923-1

9 781107 199231 >

169

Geometry and Complexity Theory

LANDSBERG

CAMBRIDGE

Geometry and Complexity Theory

J. M. LANDSBERG
Texas A&M University

CAMBRIDGE
UNIVERSITY PRESS

CAMBRIDGE
UNIVERSITY PRESS

University Printing House, Cambridge CB2 8BS, United Kingdom

One Liberty Plaza, 20th Floor, New York, NY 10006, USA

477 Williamstown Road, Port Melbourne, VIC 3207, Australia

4843/24, 2nd Floor, Ansari Road, Daryaganj, Delhi - 110002, India

79 Anson Road, #06-04/06, Singapore 079906

Cambridge University Press is part of the University of Cambridge.

It furthers the University's mission by disseminating knowledge in the pursuit of education, learning, and research at the highest international levels of excellence.

www.cambridge.org
Information on this title: www.cambridge.org/9781107199231
DOI: 10.1017/9781108183192

First published 2017

Printed in the United States of America by Sheridan Books, Inc.

A catalogue record for this publication is available from the British Library.

Library of Congress Cataloging-in-Publication Data
Names: Landsberg, J. M., author.
Title: Geometry and complexity theory / J.M. Landsberg, Texas A&M University.
Description: New York, NY, USA : Cambridge University Press, [2017] |
Includes bibliographical references and index.
Identifiers: LCCN 2017020187 | ISBN 9781107199231 (hardback : alk. paper)
Subjects: LCSH: Computational complexity. | Geometry, Algebraic.
Classification: LCC QA267.7 .L35 2017 | DDC 516.3/5–dc23
LC record available at https://lccn.loc.gov/2017020187

ISBN 978-1-107-19923-1 Hardback

GEOMETRY AND COMPLEXITY THEORY

Two central problems in computer science are P versus NP and the complexity of matrix multiplication. The first is also a leading candidate for the greatest unsolved problem in mathematics. The second is of enormous practical and theoretical importance. Algebraic geometry and representation theory provide fertile ground for advancing work on these problems and others in complexity.

This introduction to algebraic complexity theory for graduate students and researchers in computer science and mathematics features concrete examples that demonstrate the application of geometric techniques to real-world problems. Written by a noted expert in the field, it offers numerous open questions to motivate future research. Complexity theory has rejuvenated classical geometric questions and brought different areas of mathematics together in new ways. This book shows the beautiful, interesting, and important questions that have arisen as a result.

J. M. Landsberg is Professor of Mathematics at Texas A&M University. He is a leading geometer working in complexity theory, with research interests in differential geometry, algebraic geometry, representation theory, the geometry and application of tensors, and, most recently, algebraic complexity theory. The author of more than 60 research articles and 4 books, he has given numerous intensive research courses and lectures at international conferences. He co-organized the Fall 2014 semester "Algorithms and Complexity in Algebraic Geometry" at the Simons Institute for the Theory of Computing and served as the UC Berkeley Chancellor's professor during the program.

CAMBRIDGE STUDIES IN ADVANCED MATHEMATICS

All the titles listed below can be obtained from good booksellers or from Cambridge University Press. For a complete series listing, visit: www.cambridge.org/mathematics.

Already published

129 D. Goldfeld & J. Hundley *Automorphic representations and L-functions for the general linear group, I*
130 D. Goldfeld & J. Hundley *Automorphic representations and L-functions for the general linear group, II*
131 D. A. Craven *The theory of fusion systems*
132 J. Väänänen *Models and games*
133 G. Malle & D. Testerman *Linear algebraic groups and finite groups of Lie type*
134 P. Li *Geometric analysis*
135 F. Maggi *Sets of finite perimeter and geometric variational problems*
136 M. Brodmann & R. Y. Sharp *Local cohomology (2nd Edition)*
137 C. Muscalu & W. Schlag *Classical and multilinear harmonic analysis, I*
138 C. Muscalu & W. Schlag *Classical and multilinear harmonic analysis, II*
139 B. Helffer *Spectral theory and its applications*
140 R. Pemantle & M. C. Wilson *Analytic combinatorics in several variables*
141 B. Branner & N. Fagella *Quasiconformal surgery in holomorphic dynamics*
142 R. M. Dudley *Uniform central limit theorems (2nd Edition)*
143 T. Leinster *Basic category theory*
144 I. Arzhantsev, U. Derenthal, J. Hausen & A. Laface *Cox rings*
145 M. Viana *Lectures on Lyapunov exponents*
146 J.-H. Evertse & K. Győry *Unit equations in Diophantine number theory*
147 A. Prasad *Representation theory*
148 S. R. Garcia, J. Mashreghi & W. T. Ross *Introduction to model spaces and their operators*
149 C. Godsil & K. Meagher *Erdős–Ko–Rado theorems: Algebraic approaches*
150 P. Mattila *Fourier analysis and Hausdorff dimension*
151 M. Viana & K. Oliveira *Foundations of ergodic theory*
152 V. I. Paulsen & M. Raghupathi *An introduction to the theory of reproducing kernel Hilbert spaces*
153 R. Beals & R. Wong *Special functions and orthogonal polynomials*
154 V. Jurdjevic *Optimal control and geometry: Integrable systems*
155 G. Pisier *Martingales in Banach spaces*
156 C. T. C. Wall *Differential topology*
157 J. C. Robinson, J. L. Rodrigo & W. Sadowski *The three-dimensional Navier–Stokes equations*
158 D. Huybrechts *Lectures on K3 surfaces*
159 H. Matsumoto & S. Taniguchi *Stochastic analysis*
160 A. Borodin & G. Olshanski *Representations of the infinite symmetric group*
161 P. Webb *Finite group representations for the pure mathematician*
162 C. J. Bishop & Y. Peres *Fractals in probability and analysis*
163 A. Bovier *Gaussian processes on trees*
164 P. Schneider *Galois representations and (ϕ, Γ)-modules*
165 P. Gille & T. Szamuely *Central simple algebras and Galois cohomology* (2nd Edition)
166 D. Li & H. Queffelec *Introduction to Banach spaces, I*
167 D. Li & H. Queffelec *Introduction to Banach spaces, II*
168 J. Carlson, S. Müller-Stach & C. Peters *Period mappings and period domains* (2nd Edition)
169 J. M. Landsberg *Geometry and Complexity Theory*

Preface

This book describes recent applications of algebraic geometry and representation theory to complexity theory. I focus on two central problems: *the complexity of matrix multiplication* and *Valiant's algebraic variants of* **P** *versus* **NP**.

I have attempted to make this book accessible to both computer scientists and geometers and the exposition as self-contained as possible. Two goals are to convince computer scientists of the utility of techniques from algebraic geometry and representation theory and to show geometers beautiful, interesting, and important geometry questions arising in complexity theory.

Computer scientists have made extensive use combinatorics, graph theory, probability, and linear algebra. I hope to show that even elementary techniques from algebraic geometry and representation theory can substantially advance the search for lower bounds, and even upper bounds, in complexity theory. I believe such additional mathematics will be necessary for further advances on questions discussed in this book as well as related complexity problems. Techniques are introduced as needed to deal with concrete problems.

For geometers, I expect that complexity theory will be as good a source for questions in algebraic geometry as has been modern physics. Recent work has indicated that subjects such as Fulton-McPherson intersection theory, the Hilbert scheme of points, and the Kempf-Weyman method for computing syzygies all have something to add to complexity theory. In addition, complexity theory has a way of rejuvenating old questions that had been nearly forgotten but remain beautiful and intriguing: questions of Hadamard, Darboux, Lüroth, and the classical Italian school. At the same time, complexity theory has brought different areas of mathematics together in new ways: for instance, combinatorics, representation theory, and algebraic geometry all play a role in understanding the coordinate ring of the orbit closure of the determinant.

This book evolved from several classes I have given on the subject: a spring 2013 semester course at Texas A&M; summer courses at Scuola Matematica Inter-universitaria, Cortona (July 2012), CIRM, Trento (June 2014), the University of Chicago (IMA sponsored) (July 2014), KAIST, Deajeon (August 2015), and Obergurgul, Austria (September 2016); a fall 2016 semester course at Texas A&M; and, most importantly, a fall 2014 semester course at the University of California, Berkeley, as part of the semester-long program Algorithms and Complexity in Algebraic Geometry at the Simons Institute for the Theory of Computing.

Since I began writing this book, even since the first draft was completed in fall 2014, the research landscape has shifted considerably: the two paths toward Valiant's conjecture that had been considered the most viable have been shown to be unworkable, at least as originally proposed. On the other hand, there have been significant advances in our understanding of the matrix multiplication tensor. The contents of this book are the state of the art as of January 2017.

Prerequisites

Chapters 1–8 only require a solid background in linear algebra and a willingness to accept several basic results from algebraic geometry that are stated as needed. Nothing beyond [Sha07] is used in these chapters. Because of the text [Lan12], I am sometimes terse regarding basic properties of tensors and multilinear algebra. Chapters 9 and 10 contain several sections requiring further background.

Layout

All theorems, propositions, remarks, examples, etc., are numbered together within each section; for example, Theorem 1.3.2 is the second numbered item in Section 1.3. Equations are numbered sequentially within each chapter. I have included hints for selected exercises, those marked with the symbol ◎ at the end, which is meant to be suggestive of a life preserver. Exercises are marked with (1), (2), or (3), indicating the level of difficulty. Important exercises are also marked with an exclamation mark, sometimes even two, e.g., (1!!) is an exercise that is easy and very important.

Acknowledgments

Numerous people have given me help with this book over the years. These include Malek Abdesselam, Harold Boaz, Emmanuel Briand, Michel Brion, Peter Bürgisser, Klim Efremenko, Skip Garibaldi, Josh Grochow, Jesko Hüttenhain, Anthony Iarrobino, Suil Kang, Pascal Koiran, Shrawan Kumar, Laurent Manivel, Maximilliano Mella, Ketan Mulmuley, Giorgio Ottaviani, Victor Pan, Gregory Pearlstein, Kristian Ranestad, Nick Ryder, Anna Seigal, Anne Shiu, Alistair Sinclair, Les Valient, Jerzy Weyman, Avi Wigderson, Ryan Williams, and Virginia Vassilevaska Williams. I am especially indebted to Markus Bläser, Jarek Buczynski and Mateusz Michalek, Michael Forbes and Amir Shpilka, and Christian Ikenmeyer, respectively, for help with Chapters 5, 10, 7, and 9. The book was helped tremendously by Fulvio Gesmundo, who gave a careful reading and corrections to the entire text.

I also thank all the students in the classes I have given, the organizers of the various summer courses, as well as my collaborators. Finally, I thank the Simons Center for hosting the fall 2014 semester-long program Algorithms and Complexity in Algebraic Geometry, for an inspiring semester where the first draft of this book was completed.

Contents

1
Introduction

A dramatic leap for signal processing occurred in the 1960s with the implementation of the fast Fourier transform, an algorithm that surprised the engineering community with its efficiency.[1] Is there a way to predict the existence of such fast unexpected algorithms? Can we determine when they do not exist? *Complexity theory* addresses these questions.

This book is concerned with the use of *geometry* toward these goals. I focus primarily on two central questions: the complexity of matrix multiplication and algebraic variants of the famous **P** versus **NP** problem. In the first case, a surprising algorithm exists, and it is conjectured that even better algorithms exist. In the second case, it is conjectured that no surprising algorithm exists.

In this chapter I introduce the main open questions discussed in this book, establish notation that is used throughout the book, and introduce fundamental geometric notions.

1.1 Matrix Multiplication

Much of scientific computation amounts to linear algebra, and the basic operation of linear algebra is matrix multiplication. All operations of linear algebra – solving systems of linear equations, computing determinants, etc. – use matrix multiplication.

1.1.1 The Standard Algorithm

The standard algorithm for multiplying matrices is row-column multiplication: let A, B be 2×2 matrices

$$A = \begin{pmatrix} a^1_1 & a^1_2 \\ a^2_1 & a^2_2 \end{pmatrix}, \quad B = \begin{pmatrix} b^1_1 & b^1_2 \\ b^2_1 & b^2_2 \end{pmatrix}.$$

[1] To this day, it is not known if there is an even more efficient algorithm than the FFT. See [Val77, Lok08, KLPSMN09, GHIL16].

Remark 1.1.1.1 While computer scientists generally keep all indices down (to distinguish from powers), I use the convention from differential geometry that in a matrix X, the entry in the ith row and jth column is labeled x^i_j.

The usual algorithm to calculate the matrix product $C = AB$ is

$$c^1_1 = a^1_1 b^1_1 + a^1_2 b^2_1,$$
$$c^1_2 = a^1_1 b^1_2 + a^1_2 b^2_2,$$
$$c^2_1 = a^2_1 b^1_1 + a^2_2 b^2_1,$$
$$c^2_2 = a^2_1 b^1_2 + a^2_2 b^2_2.$$

It requires 8 multiplications and 4 additions to execute, and applied to $\mathbf{n} \times \mathbf{n}$ matrices, it uses $\mathbf{n}^3$ multiplications and $\mathbf{n}^3 - \mathbf{n}^2$ additions.

This algorithm has been around for about two centuries.

In 1968, V. Strassen set out to prove the standard algorithm was optimal in the sense that no algorithm using fewer multiplications exists (personal communication). Since that might be difficult to prove, he set out to show it was true at least for 2×2 matrices – at least over $\mathbb{Z}_2$. His spectacular failure opened up a whole new area of research.

1.1.2 Strassen's Algorithm for Multiplying 2 × 2 Matrices using 7 Scalar Multiplications [Str69]

Set

$$\begin{aligned} I &= (a^1_1 + a^2_2)(b^1_1 + b^2_2), \\ II &= (a^2_1 + a^2_2)b^1_1, \\ III &= a^1_1(b^1_2 - b^2_2), \\ IV &= a^2_2(-b^1_1 + b^2_1), \\ V &= (a^1_1 + a^1_2)b^2_2, \\ VI &= (-a^1_1 + a^2_1)(b^1_1 + b^1_2), \\ VII &= (a^1_2 - a^2_2)(b^2_1 + b^2_2). \end{aligned} \tag{1.1.1}$$

Exercise 1.1.2.1 (1) Show that if $C = AB$, then

$$c^1_1 = I + IV - V + VII,$$
$$c^2_1 = II + IV,$$
$$c^1_2 = III + V,$$
$$c^2_2 = I + III - II + VI.$$