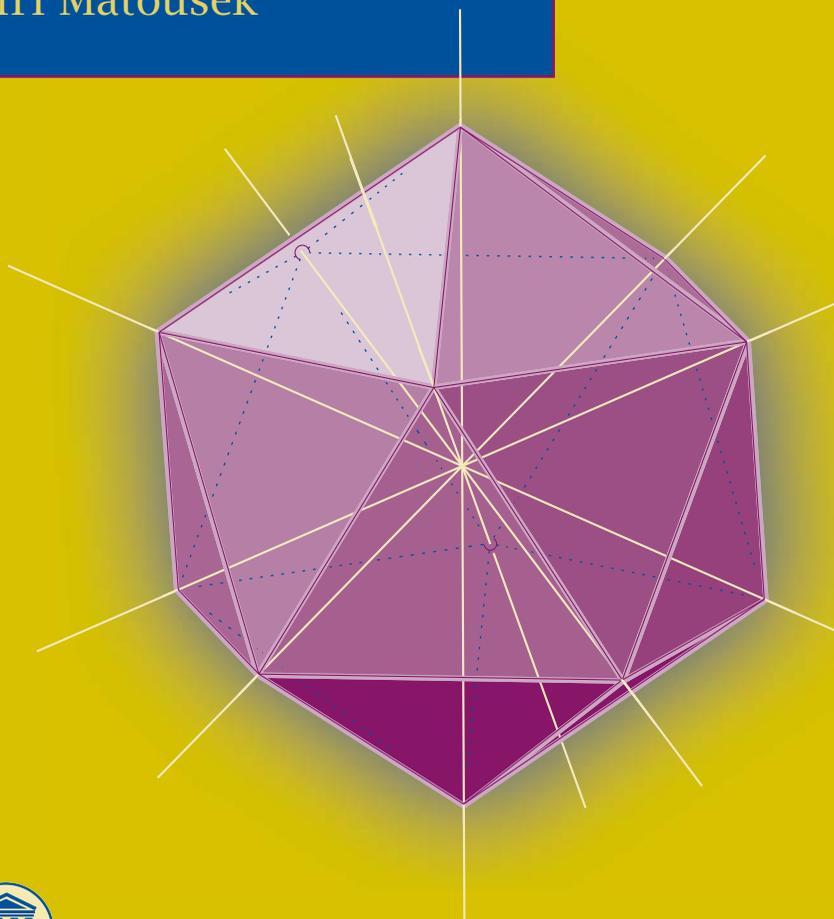


STUDENT MATHEMATICAL LIBRARY
Volume 53

Thirty-three Miniatures

Mathematical and
Algorithmic Applications
of Linear Algebra

Jiří Matoušek



American Mathematical Society

STUDENT MATHEMATICAL LIBRARY
Volume 53

Thirty-three Miniatures

Mathematical and Algorithmic
Applications of Linear Algebra

Jiří Matoušek



American Mathematical Society
Providence, Rhode Island

Editorial Board

Gerald B. Folland Robin Forman Brad G. Osgood (Chair)

2010 *Mathematics Subject Classification*. Primary 05C50, 68Wxx, 15–01.

For additional information and updates on this book, visit
www.ams.org/bookpages/stml-53

Library of Congress Cataloging-in-Publication Data

Matoušek, Jiří, 1963–

Thirty-three miniatures : mathematical and algorithmic applications of linear algebra / Jiří Matoušek.

p. cm. — (Student mathematical library ; v. 53)

Includes bibliographical references and index.

ISBN 978-0-8218-4977-4 (alk. paper)

1. algebras, Linear. I. Title.

QA184.2.M38 2010
512'.5—dc22

2009053079

Copying and reprinting. Individual readers of this publication, and nonprofit libraries acting for them, are permitted to make fair use of the material, such as to copy a chapter for use in teaching or research. Permission is granted to quote brief passages from this publication in reviews, provided the customary acknowledgment of the source is given.

Republication, systematic copying, or multiple reproduction of any material in this publication is permitted only under license from the American Mathematical Society. Requests for such permission should be addressed to the Acquisitions Department, American Mathematical Society, 201 Charles Street, Providence, Rhode Island 02904-2294 USA. Requests can also be made by e-mail to reprint-permission@ams.org.

© 2010 by the American Mathematical Society. All rights reserved.

The American Mathematical Society retains all rights
except those granted to the United States Government.
Printed in the United States of America.

∞ The paper used in this book is acid-free and falls within the guidelines
established to ensure permanence and durability.

Visit the AMS home page at <http://www.ams.org/>

10 9 8 7 6 5 4 3 2 1 15 14 13 12 11 10

Contents

Preface	v
Notation	ix
Miniature 1. Fibonacci Numbers, Quickly	1
Miniature 2. Fibonacci Numbers, the Formula	3
Miniature 3. The Clubs of Oddtown	5
Miniature 4. Same-Size Intersections	7
Miniature 5. Error-Correcting Codes	11
Miniature 6. Odd Distances	17
Miniature 7. Are These Distances Euclidean?	19
Miniature 8. Packing Complete Bipartite Graphs	23
Miniature 9. Equiangular Lines	27
Miniature 10. Where is the Triangle?	31
Miniature 11. Checking Matrix Multiplication	35
Miniature 12. Tiling a Rectangle by Squares	39

Miniature 13.	Three Petersens Are Not Enough	41
Miniature 14.	Petersen, Hoffman–Singleton, and Maybe 57	45
Miniature 15.	Only Two Distances	51
Miniature 16.	Covering a Cube Minus One Vertex	55
Miniature 17.	Medium-Size Intersection Is Hard To Avoid	57
Miniature 18.	On the Difficulty of Reducing the Diameter	61
Miniature 19.	The End of the Small Coins	67
Miniature 20.	Walking in the Yard	71
Miniature 21.	Counting Spanning Trees	77
Miniature 22.	In How Many Ways Can a Man Tile a Board?	85
Miniature 23.	More Bricks—More Walls?	97
Miniature 24.	Perfect Matchings and Determinants	107
Miniature 25.	Turning a Ladder Over a Finite Field	113
Miniature 26.	Counting Compositions	119
Miniature 27.	Is It Associative?	125
Miniature 28.	The Secret Agent and the Umbrella	131
Miniature 29.	Shannon Capacity of the Union: A Tale of Two Fields	139
Miniature 30.	Equilateral Sets	147
Miniature 31.	Cutting Cheaply Using Eigenvectors	153
Miniature 32.	Rotating the Cube	163
Miniature 33.	Set Pairs and Exterior Products	171
Index		179

Preface

Some years ago I started gathering nice applications of linear algebra, and here is the resulting collection. The applications belong mostly to the main fields of my mathematical interests—combinatorics, geometry, and computer science. Most of them are mathematical, in proving theorems, and some include clever ways of computing things, i.e., algorithms. The appearance of linear-algebraic methods is often unexpected.

At some point I started to call the items in the collection “miniatures”. Then I decided that in order to qualify for a miniature, a complete exposition of a result, with background and everything, should not exceed four typeset pages (A4 format). This rule is absolutely arbitrary, as rules often are, but it has some rational core—namely, this extent can usually be covered conveniently in a 90-minute lecture, the standard length at the universities where I happened to teach. Then, of course, there are some exceptions to the rule, such as six-page miniatures that I just couldn’t bring myself to omit.

The collection could obviously be extended indefinitely, but I thought thirty-three was a nice enough number and a good point to stop.

The exposition is intended mainly for lecturers (I’ve taught almost all of the pieces on various occasions) and also for students interested in nice mathematical ideas even when they require some

thinking. The material is hopefully class-ready, where all details left to the reader should indeed be devil-free.

I assume a background in basic linear algebra, a bit of familiarity with polynomials, and some graph-theoretical and geometric terminology. The sections have varying levels of difficulty, and generally I have ordered them from what I personally regard as the most accessible to the more demanding.

I wanted each section to be essentially self-contained. With a good undergraduate background you can as well start reading at Section 24. This is kind of opposite to a typical mathematical textbook, where material is developed gradually, and if one wants to make sense of something on page 123, one usually has to understand the previous 122 pages, or with luck, some suitable 38 pages.

Of course, the anti-textbook structure leads to some boring repetitions and, perhaps more seriously, it puts a limit on the degree of achievable sophistication. On the other hand, I believe there are advantages as well: I gave up reading several textbooks well before page 123, after I realized that between the usually short reading sessions I couldn't remember the key definitions (people with small children will know what I'm talking about).

After several sections the reader may spot certain common patterns in the presented proofs, which could be discussed at great length, but I have decided to leave out any general accounts on linear-algebraic methods.

Nothing in this text is original, and some of the examples are rather well known and appear in many publications (including, in a few cases, other books of mine). Several general reference books are listed below. I've also added references to the original sources where I could find them. However, I've kept the historical notes at a minimum, and I've put only a limited effort into tracing the origins of the ideas (apologies to authors whose work is quoted badly or not at all—please let me know about such cases).

I would also appreciate learning about mistakes and hearing suggestions of how to improve the exposition.

Further reading. An excellent textbook is

L. Babai and P. Frankl, *Linear Algebra Methods in Combinatorics (Preliminary version 2)*, Department of Computer Science, The University of Chicago, 1992.

Unfortunately, it has never been published officially. It can be obtained, with some effort, as lecture notes of the University of Chicago. It contains several of the topics discussed here, a lot of other material in a similar spirit, and a very nice exposition of some parts of linear algebra.

Algebraic graph theory is treated, e.g., in the books

N. Biggs, *Algebraic Graph Theory*, 2nd edition, Cambridge University Press, Cambridge, 1993

and

C. Godsil and G. Royle, *Algebraic Graph Theory*, Springer, New York, NY, 2001.

Probabilistic algorithms in the spirit of Sections 11 and 24 are well explained in the book

R. Motwani and P. Raghavan, *Randomized Algorithms*, Cambridge University Press, Cambridge, 1995.

Acknowledgments. For valuable comments on preliminary versions of this booklet, I would like to thank Otfried Cheong, Esther Ezra, Nati Linial, Jana Maxová, Helena Nyklová, Yoshio Okamoto, Pavel Paták, Oleg Pikhurko, and Zuzana Safernová, as well as all other people whom I may have forgotten to include in this list. Thanks also to David Wilson for permission to use his picture of a random lozenge tiling in Miniature 22, and to Jennifer Wright Sharp for careful copy-editing. Finally, I'm grateful to many people at the Department of Applied Mathematics of the Charles University in Prague and at the Institute of Theoretical Computer Science of the ETH Zurich for excellent working environments.

Notation

Most of the notation is defined in each section where it is used. Here are several general items that may not be completely unified in the literature.

The integers are denoted by \mathbb{Z} , the rationals by \mathbb{Q} , the reals by \mathbb{R} , and \mathbb{F}_q stands for the q -element finite field.

The transpose of a matrix A is written as A^T . The elements of that matrix are denoted by a_{ij} , and similarly for all other Latin letters. Vectors are typeset in boldface: $\mathbf{v}, \mathbf{x}, \mathbf{y}$, and so on. If \mathbf{x} is a vector in \mathbb{K}^n , where \mathbb{K} is some field, x_i stands for the i th component, so $\mathbf{x} = (x_1, x_2, \dots, x_n)$.

We write $\langle \mathbf{x}, \mathbf{y} \rangle$ for the standard scalar (or inner) product of vectors $\mathbf{x}, \mathbf{y} \in \mathbb{K}^n$: $\langle \mathbf{x}, \mathbf{y} \rangle = x_1y_1 + x_2y_2 + \dots + x_ny_n$. We also interpret such \mathbf{x}, \mathbf{y} as $n \times 1$ (single-column) matrices, and thus $\langle \mathbf{x}, \mathbf{y} \rangle$ could also be written as $\mathbf{x}^T \mathbf{y}$. Further, for $\mathbf{x} \in \mathbb{R}^n$, $\|\mathbf{x}\| = \langle \mathbf{x}, \mathbf{x} \rangle^{1/2}$ is the Euclidean norm (length) of the vector \mathbf{x} .

Graphs are simple and undirected unless stated otherwise; i.e., a graph G is regarded as a pair (V, E) , where V is the vertex set and E is the edge set, which is a set of unordered pairs of elements of V . For a graph G , we sometimes write $V(G)$ for the vertex set and $E(G)$ for the edge set.

Some conventions. When an important notion is defined in the text, it appears in **boldface**, which should help in looking it up. Less important terms, or general mathematical notions that are only reminded, are marked in *italics*.

In the index, mathematical notation involving a specific letter, such as S_n for the symmetric group or $E(G)$ for the edge set of a graph, is listed at the beginning of the corresponding letter's section. Only notation composed of special symbols or Greek letters appears at the beginning of the index.

Index

- \equiv (congruence), 18
- $\|\cdot\|$ (Euclidean norm), xi
- $\|\cdot\|_1$ (ℓ_1 norm), 148
- $\|\cdot\|_\infty$ (ℓ_∞ norm), 164
- $\langle \cdot, \cdot \rangle$ (standard scalar product), xi
- A^T (transposed matrix), xi
- $\mathbf{u} \wedge \mathbf{v}$ (exterior product), 174
- \overline{G} (graph complement), 141
- $G \cdot H$ (strong product), 133
- $\alpha(G)$ (independence number), 133
- $\vartheta(G)$ (Lovász theta function), 136
- $\Theta(G)$ (Shannon capacity), 133

- adjacency matrix, 32, 42, 48
 - bipartite, 86, 102
- algebra
 - exterior, 173
 - Grassmann, 173
- algorithm, probabilistic, 35, 36, 110, 121, 126
- alphabet, 12
- arctic circle, 94
- associativity, 125

- Bertrand's postulate, 109
- binary operation, 125
- Binet's formula, 4
- bipartite adjacency matrix, 86, 102
- bipartite graph, 86, 101, 107
- bits, parity check, 14

- Borsuk's conjecture, 62
- Borsuk's question, 61

- capacity, Shannon, 133, 139
- Cauchy–Schwarz inequality, 149, 159
- characteristic vector, 59, 62
- checking matrix multiplication, 35
- checking, probabilistic, 107, 126
- Cheeger–Alon–Milman inequality, 156
- Cholesky factorization, 21
- chromatic number, 136
- code, 12
 - error-correcting, 11
 - generalized Hamming, 15
 - Hamming, 12
 - linear, 14
- color class, 23
- complement (of a graph), 141
- complete bipartite graph, 23
- congruence, 17
- conjecture
 - Borsuk's, 62
 - Keakeya's, 116
- corrects t errors, 13
- cosine theorem, 17, 21
- covering, 55
 - of edges of K_n , 41
- cube, 55

-
- curve, moment, 172
 - cut, 154
 - sparsest, 154
 - cycle
 - evenly placed, 89
 - properly signed, 89
 - decoding, 13
 - degree, 78
 - minimum, 45
 - δ -dense set, 166
 - density, 154
 - determinant, 18, 77, 85, 107, 176
 - Vandermonde, 172
 - diagonalizable matrix, 21
 - diagram, Ferrers, 97
 - diameter, 61
 - diameter-reducing partition, 61
 - digraph, 79
 - functional, 82
 - dimension, 142
 - Hausdorff, 116
 - dimer model, 94
 - directed graph, 79
 - discrepancy theory, 67
 - disjoint union (of graphs), 140
 - distance
 - Euclidean, 19
 - Hamming, 13
 - ℓ_1 , 148
 - minimum (of a code), 13
 - odd, 17
 - only two, 51
 - divide and conquer, 153
 - $E(G)$, xi
 - eigenvalue, 149
 - eigenvalue (of a graph), 41, 45, 49
 - eigenvector, 155
 - encoding, 13
 - equiangular lines, 27
 - equilateral set, 147
 - Erdős–Ko–Rado theorem, 57
 - error-correcting code, 11
 - Euclidean distance, 19
 - Euclidean norm, xi
 - Euler’s formula, 92
 - evenly placed cycle, 89
 - exponent of matrix multiplication, 33
 - exterior algebra, 173
 - exterior product, 171, 174
 - extremal set theory, 171
 - \mathbb{F}_q , xi
 - factorization, Cholesky, 21
 - fast matrix multiplication, 33, 35, 110, 121
 - Ferrers diagram, 97
 - Fibonacci number, 1, 3
 - Fiedler value, 156
 - finite field, xi, 59, 116
 - Fisher inequality, generalized, 7
 - formula
 - Binet’s, 4
 - Euler’s, 92
 - Frankl–Wilson inequality, 60
 - function, Lovász theta, 136
 - functional digraph, 82
 - functional representation, 141
 - general position, 172
 - generalized Fisher inequality, 7
 - generalized Hamming code, 15
 - generalized polygon, 46
 - generator matrix (of a code), 14
 - girth, 45
 - Gottlieb’s theorem, 103
 - Gram matrix, 22, 147
 - graph, xi
 - bipartite, 86, 101, 107
 - complete bipartite, 23
 - directed, 79
 - Hoffman–Singleton, 47
 - honeycomb, 86
 - Moore, 46
 - Petersen, 41, 47
 - Pfaffian, 89
 - planar, 88
 - square grid, 85
 - 2-connected, 88
 - graph isomorphism, 42, 104
 - Grassmann algebra, 173
 - group
 - action, 100
 - symmetric, 86, 119

- groupoid, 125
- Hamming code, 12
- Hamming distance, 13
- Hausdorff dimension, 116
- Hoffman–Singleton graph, 47
- honeycomb graph, 86
- hyperplane, 55
- I_n , 24
- icosahedron, regular, 27
- independence number (of a graph), 133
- independent set, 133
- inequality
 - Cauchy–Schwarz, 149, 159
 - Cheeger–Alon–Milman, 156
 - Frankl–Wilson, 60
 - generalized Fisher, 7
 - triangle, 19
- integer partition, 97
- inversion, 173
- isometry, 165
- isomorphism, graph, 42, 104
- J_n , 24
- K_n (complete graph), 24
- Makeya needle problem, 113
- Makeya set, 114
- Makeya’s conjecture, 116
- Kasteleyn signing, 88
- Knaster’s question, 163
- ℓ_1 distance, 148
- Laplace matrix, 77, 155
- lemma
 - rank, 149
 - Sperner, 57
 - Steinitz, 74
- linear code, 14
- Lovász theta function, 136
- Lovász umbrella, 134
- lozenge tiling, 86
- matching, 107
 - perfect, 85, 107
 - random, 93
- matrix
 - adjacency, 32, 42, 48
 - adjacency, bipartite, 86, 102
 - diagonalizable, 21
 - generator (of a code), 14
 - Gram, 22, 147
 - Laplace, 77, 155
 - multiplication
 - checking, 35
 - fast, 33, 35, 110, 121
 - orthogonal, 21
 - parity check, 15
 - positive semidefinite, 20, 156
- matrix-tree theorem, 77
- minimum degree, 45
- minimum distance (of a code), 13
- model, dimer, 94
- moment curve, 172
- Moore graphs, 46
- norm
 - Euclidean, xi
 - ℓ_1 , 148
 - ℓ_∞ , 164
- number
 - chromatic, 136
 - Fibonacci, 1, 3
- odd distances, 17
- Oddtown, 5
- operation, binary, 125
- orthogonal matrix, 21
- orthogonal representation, 133
- parity check bits, 14
- parity check matrix, 15
- partition
 - diameter-reducing, 61
 - integer, 97
- partitioning, spectral, 155
- PCP theorem, 37
- perfect matching, 85, 107
 - random, 93
- permanent, 87
- permutation, 119
- Petersen graph, 41, 47
- Pfaffian graph, 89
- planar graph, 88
- polygon, generalized, 46
- polynomial, 52, 60, 108, 116, 129, 172

-
- polynomials, vector space, 52, 56
 - positive definite matrix, 8
 - positive semidefinite matrix, 20, 156
 - postulate, Bertrand's, 109
 - probabilistic algorithm, 35, 36, 110, 121, 126
 - probabilistic checking, 37, 107, 126
 - problem, Kakeya needle, 113
 - product
 - exterior, 171, 174
 - standard scalar, xi
 - strong, 133, 139
 - tensor, 63, 136, 143
 - wedge, 174
 - properly signed cycle, 89
 - question
 - Borsuk's, 61
 - Knaster's, 163
 - random perfect matching, 93
 - rank, 5, 8, 24, 99, 147
 - rank lemma, 149
 - recurrence, 2
 - representation
 - functional, 141
 - orthogonal, 133
 - rhombic tiling, 86
 - S^n , 163
 - S_n , 86, 119
 - scalar product, standard, xi
 - Schwartz–Zippel theorem, 109
 - application, 117, 121, 129
 - semigroup, 125
 - set
 - δ -dense, 166
 - equilateral, 147
 - independent, 133
 - Kakeya, 114
 - set-pair method, 171, 178
 - Shannon capacity, 133, 139
 - sign (of a permutation), 78, 173
 - signing, Kasteleyn, 88
 - skew Bollobás theorem, 172
 - spanning tree, 77
 - sparsest cut, 154
 - spectral partitioning, 155
 - Sperner lemma, 57
 - square grid graph, 85
 - Steinitz lemma, 74
 - Strassen algorithm, 32
 - strong product, 133, 139
 - symmetric group, 86, 119
 - tensor product, 63, 136, 143
 - theorem
 - cosine, 17, 21
 - Erdős–Ko–Rado, 57
 - Gottlieb's, 103
 - matrix-tree, 77
 - PCP, 37
 - Schwartz–Zippel, 109
 - application, 117, 121, 129
 - skew Bollobás, 172
 - theta function, Lovász, 136
 - thinning, 114
 - tiling
 - lozenge, 86
 - of a board, 85
 - of a rectangle, 39
 - rhombic, 86
 - trace, 49, 150
 - tree, spanning, 77
 - triangle, 31
 - triangle inequality, 19
 - 2-connected graph, 88
 - umbrella, Lovász, 134
 - unimodal, 99
 - $V(G)$, xi
 - value, Fiedler, 156
 - Vandermonde determinant, 172
 - vector, characteristic, 59, 62
 - vector space of polynomials, 52, 56
 - wall-equivalence, 100
 - wedge product, 174
 - word, 12

This volume contains a collection of clever mathematical applications of linear algebra, mainly in combinatorics, geometry, and algorithms. Each chapter covers a single main result with motivation and full proof in at most ten pages and can be read independently of all other chapters (with minor exceptions), assuming only a modest background in linear algebra.

The topics include a number of well-known mathematical gems, such as Hamming codes, the matrix-tree theorem, the Lovász bound on the Shannon capacity, and a counterexample to Borsuk's conjecture, as well as other, perhaps less popular but similarly beautiful results, e.g., fast associativity testing, a lemma of Steinitz on ordering vectors, a monotonicity result for integer partitions, or a bound for set pairs via exterior products.

The simpler results in the first part of the book provide ample material to liven up an undergraduate course of linear algebra. The more advanced parts can be used for a graduate course of linear-algebraic methods or for seminar presentations.



 For additional information
and updates on this book, visit
www.ams.org/bookpages/stml-53

AMS *on the Web*
www.ams.org