

Editors:

J.-M. Morel, Cachan

B. Teissier, Paris

For further volumes:

<http://www.springer.com/series/304>

Alla Detinko • Dane Flannery
Eamonn O'Brien
Editors

Probabilistic Group Theory, Combinatorics, and Computing

Lectures from the Fifth de Brún Workshop



Springer

Editors

Alla Detinko
Department of Mathematics
National University of Ireland, Galway
Ireland

Dane Flannery
Department of Mathematics
National University of Ireland, Galway
Ireland

Eamonn O'Brien
Department of Mathematics
University of Auckland
Auckland, New Zealand

ISBN 978-1-4471-4813-5 ISBN 978-1-4471-4814-2 (eBook)

DOI 10.1007/978-1-4471-4814-2

Springer London Heidelberg New York Dordrecht

Lecture Notes in Mathematics ISSN print edition: 0075-8434

ISSN electronic edition: 1617-9692

Library of Congress Control Number: 2012956221

Mathematics Subject Classification (2010): 05-04; 05B05; 20B40; 20D06; 20P05

© Springer-Verlag London 2013

This work is subject to copyright. All rights are reserved by the Publisher, whether the whole or part of the material is concerned, specifically the rights of translation, reprinting, reuse of illustrations, recitation, broadcasting, reproduction on microfilms or in any other physical way, and transmission or information storage and retrieval, electronic adaptation, computer software, or by similar or dissimilar methodology now known or hereafter developed. Exempted from this legal reservation are brief excerpts in connection with reviews or scholarly analysis or material supplied specifically for the purpose of being entered and executed on a computer system, for exclusive use by the purchaser of the work. Duplication of this publication or parts thereof is permitted only under the provisions of the Copyright Law of the Publisher's location, in its current version, and permission for use must always be obtained from Springer. Permissions for use may be obtained through RightsLink at the Copyright Clearance Center. Violations are liable to prosecution under the respective Copyright Law.

The use of general descriptive names, registered names, trademarks, service marks, etc. in this publication does not imply, even in the absence of a specific statement, that such names are exempt from the relevant protective laws and regulations and therefore free for general use.

While the advice and information in this book are believed to be true and accurate at the date of publication, neither the authors nor the editors nor the publisher can accept any legal responsibility for any errors or omissions that may be made. The publisher makes no warranty, express or implied, with respect to the material contained herein.

Printed on acid-free paper

Springer is part of Springer Science+Business Media (www.springer.com)

Preface

This book is inspired by the workshop *Groups, Combinatorics, Computing*, held at National University of Ireland, Galway from April 11 to 16, 2011—the Fifth “de Brún Workshop” run under the auspices of Science Foundation Ireland’s Mathematics Initiative Programme. A principal theme of the workshop was interactions between group theory and combinatorics with algorithmic or computational aspects. Areas encompassed by this theme are currently the focus of intense research activity.

The core part of the workshop was formed by three lecture courses. These contained a wide and unique selection of material, for the first time providing an accessible introduction to frontier research in thematic areas. It became clear that the courses should be made available to a larger audience.

The book has three chapters, one per lecture course. Each chapter is self-contained; beginning with background material including historical roots, the reader is led to the latest results and open problems. Illustrative examples, some proofs and algorithms, and extensive bibliographies are given.

The first chapter, by Martin Liebeck, is an exposition of recent developments in probabilistic and asymptotic theory of finite groups, particularly finite simple groups. The first two sections are on random generation of finite groups and maximal subgroups. The next topic is representation varieties and character-theoretic methods. Finally, diameter and growth of Cayley graphs of simple groups are considered. The chapter traces progress on fundamental conjectures which have driven the development of this subject.

The second chapter is by Alice Niemeyer, Cheryl Praeger, and Ákos Seress. This chapter again has a strong probabilistic flavour. It discusses the role of estimation in the design and analysis of randomised algorithms for computing with finite groups, and approaches to estimating proportions of important element classes. Among the latter are geometric methods, the use of generating functions, and theory of Lie type groups. The chapter also surveys numerous results concerning estimation in permutation groups and finite classical groups. An application to the construction of involution centralisers, a key part of the constructive recognition of finite simple groups, is given. Connections with theoretical computer science are made.

In the final chapter, Leonard Soicher presents results from a different area at the interface of group theory and combinatorics. This chapter emphasises practical computation. Specifically, it considers how group theory may be used in the construction, classification, and analysis of combinatorial designs. Statistical optimality results for semi-Latin squares are reviewed. An account of the new theory of “uniform” semi-Latin squares and a construction which determines a semi-Latin square from a transitive permutation group are then given. The chapter describes use of the **GAP** package **DESIGN**. Along with an introduction to the package and samples of its operation, it is shown how package functions can be used to classify block designs and semi-Latin squares. In an extended example, new statistically efficient semi-Latin squares are determined.

We envisage that this book will be a resource for lecture or reading courses or for self-instruction. Indeed, each chapter is a ready-made graduate lecture course. All three chapters could serve as the foundation of an advanced graduate programme in algebra and computing.

The Fifth de Brún Workshop also featured research talks and short presentations. More details and pdf files of selected talks are available at

<http://www.maths.nuigalway.ie/~detinko/DeBrun5/>

We take this opportunity to record our gratitude to Charles Leedham-Green, who acted as scientific chair of the workshop. He gave the opening address, and his many other contributions helped to ensure the event’s success.

In conclusion, we hope that the reader will find these lectures as interesting and valuable as workshop participants did.

Galway, Ireland
Auckland, New Zealand
January 2012

Alla Detinko and Dane Flannery
Eamonn O’Brien

Acknowledgements

We thank the authors for agreeing to publication of their courses, and for their efforts in preparing the courses for this book. The useful and prompt feedback from our referees is also very much appreciated.

The workshop received funding from Science Foundation Ireland grant 07/MI/007. NUI Galway provided further support. We are especially indebted to Mary Kelly and Padraig Ó Catháin, for assistance with many tasks involved in running the workshop.

Contents

1 Probabilistic and Asymptotic Aspects of Finite Simple Groups	1
Martin W. Liebeck	
1.1 Random Generation of Simple Groups and Maximal Subgroups	1
1.1.1 Alternating Groups	1
1.1.2 Groups of Lie Type	4
1.1.3 Other Results on Random Generation	8
1.1.4 Generation of Maximal Subgroups	10
1.2 Random Generation of Arbitrary Finite Groups	11
1.3 Representation Varieties and Character-Theoretic Methods	15
1.3.1 Fuchsian Groups	16
1.3.2 Character Theory	17
1.3.3 Symmetric and Alternating Groups	19
1.3.4 Groups of Lie Type	20
1.3.5 Representation Varieties	21
1.3.6 Triangle Groups	23
1.4 Cayley Graphs of Simple Groups: Diameter and Growth	26
1.4.1 Conjugacy Classes	28
1.4.2 Babai's Conjecture	29
References	31
2 Estimation Problems and Randomised Group Algorithms	35
Alice C. Niemeyer, Cheryl E. Praeger, and Ákos Seress	
2.1 Estimation and Randomization	35
2.1.1 Computation with Permutation Groups	35
2.1.2 Recognising the Permutation Group Giants	36
2.1.3 Monte Carlo Algorithms	37
2.1.4 What Kinds of Estimates and in What Groups?	39
2.1.5 What Group is That: Recognising Classical Groups as Matrix Groups	39
2.1.6 What Group is That: Recognising Lie Type Groups in Arbitrary Representations	42

2.2	Proportions of Elements in Symmetric Groups	42
2.2.1	Notation	42
2.2.2	Historical Notes	42
2.2.3	Orders of Permutations	43
2.2.4	Number of Cycles	44
2.2.5	Generating Functions	44
2.2.6	Solutions to $x^m = 1$ in Symmetric and Alternating Groups	48
2.2.7	The Münchhausen Method (Bootstrapping)	51
2.2.8	Algorithmic Applications of Proportions in Symmetric Groups	54
2.2.9	Restrictions on Cycle Lengths	56
2.3	Estimation Techniques in Lie Type Groups	57
2.3.1	p -Singular Elements in Permutation Groups	57
2.3.2	Quokka Subsets of Finite Groups	58
2.3.3	Estimation Theory for Quokka Sets	59
2.3.4	Strong Involutions in Classical Groups	61
2.3.5	More Comments on Strong Involutions	63
2.3.6	Regular Semisimple Elements and Generating Functions ...	65
2.4	Computing Centralisers of Involutions	68
2.4.1	Applications of Centralisers of Involutions Computations ...	69
2.4.2	Constructive Membership in Lie Type Groups	70
2.4.3	Constructive Recognition of Lie Type Groups	72
2.4.4	Computation of an Element Centralising an Involution	74
2.4.5	Computation of the Full Centraliser	75
	References	78
3	Designs, Groups and Computing	83
	Leonard H. Soicher	
3.1	Introduction	83
3.2	Background Material	84
3.2.1	Block Designs	84
3.2.2	Efficiency Measures of 1-Designs	85
3.2.3	Permutation Groups	86
3.2.4	Latin Squares	87
3.2.5	Semi-Latin Squares	88
3.3	Optimality Results for Semi-Latin Squares	89
3.4	Uniform Semi-Latin Squares	90
3.5	Semi-Latin Squares from Transitive Permutation Groups	91
3.5.1	The Canonical Efficiency Factors of $SLS(G)$	92
3.6	The DESIGN Package	94
3.6.1	The BlockDesigns Function	95
3.6.2	The BlockDesignEfficiency Function	97

3.7 Classifying Semi-Latin Squares 98

3.8 Efficient Semi-Latin Squares as Subsquares of Uniform
Semi-Latin Squares 102

3.9 Some Open Problems 105

References 106

Contributors

Martin W. Liebeck Department of Mathematics, Imperial College, London, UK

Alice C. Niemeyer Centre for the Mathematics of Symmetry and Computation, School of Mathematics and Statistics, The University of Western Australia, Crawley, WA, Australia

Cheryl E. Praeger Centre for the Mathematics of Symmetry and Computation, School of Mathematics and Statistics, The University of Western Australia, Crawley, WA, Australia

King Abdulaziz University, Jeddah, Saudi Arabia

Ákos Seress Centre for the Mathematics of Symmetry and Computation, School of Mathematics and Statistics, The University of Western Australia, Crawley, WA, Australia

The Ohio State University, Columbus, OH, USA

Leonard H. Soicher School of Mathematical Sciences, Queen Mary University of London, London, UK