LONDON MATHEMATICAL SOCIETY LECTURE NOTE SERIES

The titles below are available from booksellers, or from Cambridge University Press at
www.cambridge.org/mathematics

287 Topics on Riemann surfaces and Fuchsian groups, E. BUJALANCE, A.F. COSTA & E. MARTÍNEZ (eds)
288 Surveys in combinatorics, 2001, J.W.P. HIRSCHFELD (ed)
289 Aspects of Sobolev-type inequalities, L. SALOFF-COSTE
290 Quantum groups and Lie theory, A. PRESSLEY (ed)
291 Tits buildings and the model theory of groups, K. TENT (ed)
292 A quantum groups primer, S. MAJID
293 Second order partial differential equations in Hilbert spaces, G. DA PRATO & J. ZABCZYK
294 Introduction to operator space theory, G. PISIER
295 Geometry and integrability, L. MASON & Y. NUTKU (eds)
296 Lectures on invariant theory, I. DOLGACHEV
297 The homotopy category of simply connected 4-manifolds, H.-J. BAUES
298 Higher operads, higher categories, T. LEINSTER (ed)
299 Kleinian groups and hyperbolic 3-manifolds, Y. KOMORI, V. MARKOVIC & C. SERIES (eds)
300 Introduction to Möbius differential geometry, U. HERTRICH-JEROMIN
301 Stable modules and the D(2)-problem, F.E.A. JOHNSON
302 Discrete and continuous nonlinear Schrödinger systems, M.J. ABLOWITZ, B. PRINARI & A.D. TRUBATCH
303 Number theory and algebraic geometry, M. REID & A. SKOROBOGATOV (eds)
304 Groups St Andrews 2001 in Oxford I, C.M. CAMPBELL, E.F. ROBERTSON & G.C. SMITH (eds)
305 Groups St Andrews 2001 in Oxford II, C.M. CAMPBELL, E.F. ROBERTSON & G.C. SMITH (eds)
306 Geometric mechanics and symmetry, J. MONTALDI & T. RATIU (eds)
307 Surveys in combinatorics 2003, C.D. WENSLEY (ed.)
308 Topology, geometry and quantum field theory, U.L. TILLMANN (ed)
309 Corings and comodules, T. BRZEZINSKI & R. WISBAUER
310 Topics in dynamics and ergodic theory, S. BEZUGLYI & S. KOLYADA (eds)
311 Groups: topological, combinatorial and arithmetic aspects, T.W. MÜLLER (ed)
312 Foundations of computational mathematics, Minneapolis 2002, F. CUCKER *et al* (eds)
313 Transcendental aspects of algebraic cycles, S. MÜLLER-STACH & C. PETERS (eds)
314 Spectral generalizations of line graphs, D. CVETKOVIĆ, P. ROWLINSON & S. SIMIĆ
315 Structured ring spectra, A. BAKER & B. RICHTER (eds)
316 Linear logic in computer science, T. EHRHARD, P. RUET, J.-Y. GIRARD & P. SCOTT (eds)
317 Advances in elliptic curve cryptography, I.F. BLAKE, G. SEROUSSI & N.P. SMART (eds)
318 Perturbation of the boundary in boundary-value problems of partial differential equations, D. HENRY
319 Double affine Hecke algebras, I. CHEREDNIK
320 L-functions and Galois representations, D. BURNS, K. BUZZARD & J. NEKOVÁŘ (eds)
321 Surveys in modern mathematics, V. PRASOLOV & Y. ILYASHENKO (eds)
322 Recent perspectives in random matrix theory and number theory, F. MEZZADRI & N.C. SNAITH (eds)
323 Poisson geometry, deformation quantisation and group representations, S. GUTT *et al* (eds)
324 Singularities and computer algebra, C. LOSSEN & G. PFISTER (eds)
325 Lectures on the Ricci flow, P. TOPPING
326 Modular representations of finite groups of Lie type, J.E. HUMPHREYS
327 Surveys in combinatorics 2005, B.S. WEBB (ed)
328 Fundamentals of hyperbolic manifolds, R. CANARY, D. EPSTEIN & A. MARDEN (eds)
329 Spaces of Kleinian groups, Y. MINSKY, M. SAKUMA & C. SERIES (eds)
330 Noncommutative localization in algebra and topology, A. RANICKI (ed)
331 Foundations of computational mathematics, Santander 2005, L.M PARDO, A. PINKUS, E. SÜLI & M.J. TODD (eds)
332 Handbook of tilting theory, L. ANGELERI HÜGEL, D. HAPPEL & H. KRAUSE (eds)
333 Synthetic differential geometry (2nd Edition), A. KOCK
334 The Navier–Stokes equations, N. RILEY & P. DRAZIN
335 Lectures on the combinatorics of free probability, A. NICA & R. SPEICHER
336 Integral closure of ideals, rings, and modules, I. SWANSON & C. HUNEKE
337 Methods in Banach space theory, J.M.F. CASTILLO & W.B. JOHNSON (eds)
338 Surveys in geometry and number theory, N. YOUNG (ed)
339 Groups St Andrews 2005 I, C.M. CAMPBELL, M.R. QUICK, E.F. ROBERTSON & G.C. SMITH (eds)
340 Groups St Andrews 2005 II, C.M. CAMPBELL, M.R. QUICK, E.F. ROBERTSON & G.C. SMITH (eds)
341 Ranks of elliptic curves and random matrix theory, J.B. CONREY, D.W. FARMER, F. MEZZADRI & N.C. SNAITH (eds)
342 Elliptic cohomology, H.R. MILLER & D.C. RAVENEL (eds)
343 Algebraic cycles and motives I, J. NAGEL & C. PETERS (eds)
344 Algebraic cycles and motives II, J. NAGEL & C. PETERS (eds)

345 Algebraic and analytic geometry, A. NEEMAN
346 Surveys in combinatorics 2007, A. HILTON & J. TALBOT (eds)
347 Surveys in contemporary mathematics, N. YOUNG & Y. CHOI (eds)
348 Transcendental dynamics and complex analysis, P.J. RIPPON & G.M. STALLARD (eds)
349 Model theory with applications to algebra and analysis I, Z. CHATZIDAKIS, D. MACPHERSON, A. PILLAY & A. WILKIE (eds)
350 Model theory with applications to algebra and analysis II, Z. CHATZIDAKIS, D. MACPHERSON, A. PILLAY & A. WILKIE (eds)
351 Finite von Neumann algebras and masas, A.M. SINCLAIR & R.R. SMITH
352 Number theory and polynomials, J. MCKEE & C. SMYTH (eds)
353 Trends in stochastic analysis, J. BLATH, P. MÖRTERS & M. SCHEUTZOW (eds)
354 Groups and analysis, K. TENT (ed)
355 Non-equilibrium statistical mechanics and turbulence, J. CARDY, G. FALKOVICH & K. GAWEDZKI
356 Elliptic curves and big Galois representations, D. DELBOURGO
357 Algebraic theory of differential equations, M.A.H. MACCALLUM & A.V. MIKHAILOV (eds)
358 Geometric and cohomological methods in group theory, M.R. BRIDSON, P.H. KROPHOLLER & I.J. LEARY (eds)
359 Moduli spaces and vector bundles, L. BRAMBILA-PAZ, S.B. BRADLOW, O. GARCÍA-PRADA & S. RAMANAN (eds)
360 Zariski geometries, B. ZILBER
361 Words: Notes on verbal width in groups, D. SEGAL
362 Differential tensor algebras and their module categories, R. BAUTISTA, L. SALMERÓN & R. ZUAZUA
363 Foundations of computational mathematics, Hong Kong 2008, F. CUCKER, A. PINKUS & M.J. TODD (eds)
364 Partial differential equations and fluid mechanics, J.C. ROBINSON & J.L. RODRIGO (eds)
365 Surveys in combinatorics 2009, S. HUCZYNSKA, J.D. MITCHELL & C.M. RONEY-DOUGAL (eds)
366 Highly oscillatory problems, B. ENGQUIST, A. FOKAS, E. HAIRER & A. ISERLES (eds)
367 Random matrices: High dimensional phenomena, G. BLOWER
368 Geometry of Riemann surfaces, F.P. GARDINER, G. GONZÁLEZ-DIEZ & C. KOUROUNIOTIS (eds)
369 Epidemics and rumours in complex networks, M. DRAIEF & L. MASSOULIÉ
370 Theory of p-adic distributions, S. ALBEVERIO, A.YU. KHRENNIKOV & V.M. SHELKOVICH
371 Conformal fractals, F. PRZYTYCKI & M. URBAŃSKI
372 Moonshine: The first quarter century and beyond, J. LEPOWSKY, J. MCKAY & M.P. TUITE (eds)
373 Smoothness, regularity and complete intersection, J. MAJADAS & A. G. RODICIO
374 Geometric analysis of hyperbolic differential equations: An introduction, S. ALINHAC
375 Triangulated categories, T. HOLM, P. JØRGENSEN & R. ROUQUIER (eds)
376 Permutation patterns, S. LINTON, N. RUŠKUC & V. VATTER (eds)
377 An introduction to Galois cohomology and its applications, G. BERHUY
378 Probability and mathematical genetics, N. H. BINGHAM & C. M. GOLDIE (eds)
379 Finite and algorithmic model theory, J. ESPARZA, C. MICHAUX & C. STEINHORN (eds)
380 Real and complex singularities, M. MANOEL, M.C. ROMERO FUSTER & C.T.C WALL (eds)
381 Symmetries and integrability of difference equations, D. LEVI, P. OLVER, Z. THOMOVA & P. WINTERNITZ (eds)
382 Forcing with random variables and proof complexity, J. KRAJÍČEK
383 Motivic integration and its interactions with model theory and non-Archimedean geometry I, R. CLUCKERS, J. NICAISE & J. SEBAG (eds)
384 Motivic integration and its interactions with model theory and non-Archimedean geometry II, R. CLUCKERS, J. NICAISE & J. SEBAG (eds)
385 Entropy of hidden Markov processes and connections to dynamical systems, B. MARCUS, K. PETERSEN & T. WEISSMAN (eds)
386 Independence-friendly logic, A.L. MANN, G. SANDU & M. SEVENSTER
387 Groups St Andrews 2009 in Bath I, C.M. CAMPBELL *et al* (eds)
388 Groups St Andrews 2009 in Bath II, C.M. CAMPBELL *et al* (eds)
389 Random fields on the sphere, D. MARINUCCI & G. PECCATI
390 Localization in periodic potentials, D.E. PELINOVSKY
391 Fusion systems in algebra and topology M. ASCHBACHER, R. KESSAR & B. OLIVER
392 Surveys in combinatorics 2011, R. CHAPMAN (ed)
393 Non-abelian fundamental groups and Iwasawa theory, J. COATES *et al* (eds)
394 Variational problems in differential geometry, R. BIELAWSKI, K. HOUSTON & M. SPEIGHT (eds)
395 How groups grow, A. MANN
396 Arithmetic differential operators over the p-adic integers, C.C. RALPH & S.R. SIMANCA
397 Hyperbolic geometry and applications in quantum chaos and cosmology, J. BOLTE & F. STEINER (eds)
398 Mathematical models in contact mechanics, M. SOFONEA & A. MATEI
399 Circuit double cover of graphs, C.-Q. ZHANG
400 Dense sphere packings: a blueprint for formal proofs, T. HALES

London Mathematical Society Lecture Note Series: 400

Dense Sphere Packings

A blueprint for formal proofs

THOMAS C. HALES
University of Pittsburgh

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

314-321, 3rd Floor, Plot 3, Splendor Forum, Jasola District Centre, New Delhi - 110025, India

103 Penang Road, #05-06/07, Visioncrest Commercial, Singapore 238467

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/9780521617703

First published 2012

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

ISBN 978-0-521-61770-3 Paperback

Contents

Preface

"I think there's a revolution in mathematics around the corner. I think that . . . people will look back on the fin-de-siècle of the twentieth century and say 'Then is when it happened' (just like we look back at the Greeks for inventing the concept of proof and at the nineteenth century for making analysis rigorous). I really believe that. And it amazes me that no one seems to notice.

"Never before have the Platonic mathematical world and the physical world been this similar, this close. Is it strange that I expect leakage between these two worlds? That I think the proof strings will find their way to the computer memories?. . .

"What I expect is that some kind of computer system will be created, a proof checker, that all mathematicians will start using to check their work, their proofs, their mathematics. I have no idea what shape such a system will take. But I expect some system to come into being that is past some threshold so that it is practical enough for real work, and then quite suddenly some kind of 'phase transition' will occur and everyone will be using that system."

–Freek Wiedijk [49]

Alecos: Christos has a problem with the 'foundational quest'!

Christos: Wrong! I have two problems with your version *of it! One, it didn't fail and, two, it wasn't a tragedy! Granted, there are some tragic parts! But the ending is happy, as in the 'Oresteia'!*

Apostolos: Happy for whom? Cantor, going insane? Gödel starving himself to death out of paranoia? Hilbert or Russell and their psychotic sons? Or Frege with–

Christos: 'The meaning is in the ending!' you said so yourself! So, follow the quest for ten more years and you get a brand-new triumphant finale with the creation of the computer, which is the quest's real hero! Your problem is, simply, that you see it as a story of people!

Apostolos: Well, stories do tend to be about people!

Christos: So, choose the right people! And show what they really did! All we we learn of the great von Neumann is he said 'It's over' when he heard Gödel!

Alecos: But it was over in a sense, wasn't it? Pop went Hilbert's 'no ignorabimus'!

Christos: But then came the quest's jeune premier, its parsifal … Alan Turing! He said 'Ok, we can't prove everything! So, let's see what we can prove!' and to define proof, he invented, in 1936, a theoretical machine which contains all the ideas of the computer!… which, after the war, he and von Neumann, the quest's proudest sons, brought to full life!

–Doxiadis and Papadimitriou, Logicomix [10]

"Despite the unusual nature of the proof, the editors of the Annals of Mathematics agreed to publish it, provided it was accepted by a panel of twelve referees. In 2003, after four years of work, the head of the referee's panel Gábor Fejes Tóth (son of László Fejes Tóth) reported that the panel were '99% certain' of the correctness of the proof."

– Wikipedia entry on the Kepler conjecture

"Sometimes fixing a 1 percent defect takes 500 percent effort."

– Joel Spolsky, Joel on Software [42]

"Every one fully persuaded is a fool."

– Barthasar Gracián, the Art of Worldly Wisdom [17]

The Kepler Conjecture

In 1611, Johannes Kepler wrote a booklet in which he asserted that the familiar cannonball arrangement of congruent balls in space achieves the highest possible density. This assertion has become known as the Kepler conjecture. This book presents a proof.

As early as 1831, Gauss established a special case of the conjecture, by proving that the cannonball arrangement is optimal among all *lattices* [14]. Later in the nineteenth century, Thue solved the corresponding problem in two dimensions, showing that the hexagonal arrangement of disks in the plane achieves optimal density [45] and [46]. Hilbert, in his famous list of mathematical problems, made the Kepler conjecture part of his eighteenth problem. In 1953, Fejes Tóth formulated a general strategy to confirm the Kepler conjecture, but lacked the computational resources to carry it out [12]. The conjecture was finally resolved in 1998, even though the full proof was not published until 2006 [22]. Section 1.1 gives additional historical background.

The Kepler conjecture has become a test of the capability of computers to deliver a reliable mathematical proof. The original proof involved many long computer calculations that led a team of referees to exhaustion. This book has redesigned the proof in a way that makes the correctness of the computer proof as transparent as possible.

Formal Proofs

After all is said and done, a proof is only as reliable as the processes that are used to verify its correctness. The ultimate standard of proof is a formal proof, which is nothing other than an unbroken chain of logical inferences from an explicit set of axioms. While this may be the mathematical ideal of proof, actual mathematical practice generally deviates significantly from the ideal.

In recent years, as part of this project, I have been increasingly preoccupied by the processes that mathematicians rely on to ensure the correctness of complex proofs. A century ago, Russell's paradox and other antinomies threatened set theory with fires of destruction. Researchers from Frege to Gödel solved the problem of rigor in mathematics and found a theoretical solution but did not extinguish the fire at the foundations of mathematics because they omitted the practical implementation. Some, such as Bourbaki, have even gone so far as to claim that "formalized mathematics cannot in practice be written down in full" and call such a project "absolutely unrealizable" [7, pp. 10–11].

While it is true that formal proofs may be too long to print, computers –

which do not have the same limitations as paper – have become the natural host of formal mathematics. In recent decades, logicians and computer scientists have reworked the foundations of mathematics, putting them in an efficient form designed for real use on real computers.

For the first time in history, it is possible to generate and verify every single logical inference of major mathematical theorems. This has now been done for many theorems, including the four-color theorem, the prime number theorem, the Jordan curve theorem, the Brouwer fixed point theorem, and the fundamental theorem of calculus. Freek Wiedijk reports that 87% of a list of one hundred famous theorems have now been checked formally [50]. The list of remaining theorems contains two particular challenges: the independence of the Continuum hypothesis and Fermat's Last theorem.

Some mathematicians remain skeptical of the process because computers have been used to generate and verify the logical inferences. Computers are notoriously imperfect, with flaws ranging from software bugs to defective chips. Even if a computer verifies the inferences, who verifies the verifier, or then verifies the verifier of the verifier? Indeed, it would be unscientific of us to place an unmerited trust in computers.

The choice comes down to two competing verification processes. The first is the traditional process of referees, which depends largely on the luck of the draw – some referees are meticulous, while others are careless. The second process is formal computer verification, which is less dependent on the whims of a particular referee. In my view, the choice between the conventional process by human referee and computer verification is as evident as the choice between a sundial and an atomic clock in science.

The standard of proof I have adopted is the highest scientific standard available by current technology. The introduction of steel in architecture is not a mere reinforcement of wood and stone; it changes the world of structural possibilities. There is no longer any reason to limit proofs to ten thousand pages when our technology supports a million pages.

The style of formal proofs is different from that of conventional ones. It is easier to formalize several short snappy proofs than a few intricate ones. Humans enjoy surprising new perspectives, but computers benefit from repetition and standardization. Despite these differences, I have sought proofs that might bring pleasure to the human reader while providing precise instructions for the implementation in silicon.

Conventions

To make formalization proceed more smoothly, long proofs have been broken into a sequence of smaller claims. Each claim starts a new paragraph and is set in italics. The second sentence of the paragraph begins with the word *indeed* when the proof of the claim is direct and with the word *otherwise* when the proof is indirect by contradiction.

Lemmas and theorems that are marked with an asterisk appear out of the natural logical sequence. Care should be taken to avoid logical gaps when they are cited.

The pronoun *we* is used inclusively for the author and reader as we work our way through the proofs in this book. The pronoun *I* refers to the author alone.

The asterisk $*$ is used as a wildcard symbol in patterns. It replaces a term in contexts where the name of the term is not relevant. It can also denote a bound variable. For example, the function $f(*, y)$ of a single variable is obtained from f by evaluating the second argument at a fixed value y.

The union of the family X of sets is written as $\bigcup X$ or as $\bigcup_{x \in X} x$ without any difference in meaning. The first form is preferred because of its economy. We also use both expressions $\bigcap X$ and $\bigcap_{x \in X} x$ for the intersection of a family of sets.

The documentation of the computer calculations for the Kepler conjecture has evolved over time. The 1998 preprint version of the proof of the Kepler conjecture contains long appendices that list hundreds of calculations that enter into the proof. These appendices were cut from the published version of the proof because it is more useful to store the computer part of the proof at a computer code repository that is permanent, versioned, and freely available. The computer code and documentation are housed at *Google Code project hosting*. Separate documentation, which is available at the project site, describes the computer calculations that appear in this book. When this book uses an external calculation, it is marked in italic font as a *computer calculation*[1] [21].

A Blueprint

The book is a blueprint for formal proofs because it gives the design of the formal proof to be constructed. The parts of this book that cover the text portions of the proof of the Kepler conjecture are being formally verified in the proof assistant HOL Light. I dream of a fully formally verified solution to the

[1] `[notation]` This explains notation.

proof that includes the computer portions of the proof as well. Details about and credits for this large team effort appear in Appendix A.

Decisions about what to include in this book have been shaped by the list of theorems already available in the library of the proof assistant *HOL Light*. For example, this book accepts basic point-set topology and measure theory because they have been formalized by Harrison [26].

The book is divided into three parts, the first of which describes the major ideas, methods, and organization of the proof.

The part on foundations provides background material about constructions in discrete geometry. The first of these chapters covers trigonometric identities and basic vector geometry. The second treats volume from an elementary point of view. The third chapter covers planar graph theory from a purely combinatorial perspective. The fourth chapter continues with planar graphs, now from a geometric perspective.

The final part of the book gives the solution to the packing problem. The first of these chapters gives a top-level overview of the major steps of the proof, describing how the problem can be reduced from a problem with infinitely many variables to one in finitely many variables. The remaining chapters in this part flesh out the proof.

The final section of the book views dense sphere packings from a larger perspective. It resolves another longstanding conjecture in discrete geometry: Bezdek's strong dodecahedral conjecture.

Simplifications

Many simplifications of the original proof have been found over the past several years. These simplifications are published here for the first time. Gonthier has reworked the proof of the four-color theorem to avoid the use of the Jordan curve theorem, using instead the much simpler notion of Möbius contour from the theory of hypermaps. I have followed Gonthier's lead.

The optimality of the face-centered cubic packing is an assertion about infinite space-filling packings. For computational purposes, it is useful to reduce the sphere packing problem to finite packings. A *correction term* is associated with each different reduction from infinite packings to finite packings. Ferguson and I worked together to produce the original proof of the Kepler conjecture. The two of us considered a large number of different correction terms, seeking one that would simplify the computations as much as possible. In a discussion of the solution of the packing problem, I wrote that "correction terms are extremely flexible and easy to construct, and soon Samuel Ferguson and I realized that every time we encountered difficulties in solving the minimization problem, we could adjust f [the correction term] to skirt the difficulty. . . . If I were to revise the proof to produce a simpler one, the first thing I would do would be to change the correction term once again. It is the key to a simpler proof" [19]. Marchal has recently found a simple correction term, giving a new way to reduce from infinite packings to finite packings [31]. This book implements his reduction step.

There are many other improvements of the proof that are not visible in the book because they are implemented in computer code, including a reduction of the number of lines of computer code from over 187,000 to about 10,000. Needless to say, the quickest way to be sure that a block of computer code will not execute a bug is to delete the code altogether.

Thomas C. Hales
Pittsburgh, PA