Expansion in Finite Simple Groups of Lie Type
EDITORIAL COMMITTEE
Dan Abramovich
Daniel S. Freed
Rafe Mazzeo (Chair)
Gigliola Staffilani

2010 Mathematics Subject Classification. Primary 05C81, 11B30, 20C33, 20D06, 20G40.

For additional information and updates on this book, visit www.ams.org/bookpages/gsm-164

Library of Congress Cataloging-in-Publication Data
Tao, Terence, 1975
Expansion in finite simple groups of Lie type / Terence Tao.
   pages cm. – (Graduate studies in mathematics; volume 164)
   Includes bibliographical references and index.
   ISBN 978-1-4704-2196-0 (alk. paper)
   1. Finite simple groups. 2. Lie groups. I. Title.

QA387.T356 2015
512’.482–dc23 2014049154

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 select pages 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. Permissions to reuse portions of AMS publication content are handled by Copyright Clearance Center’s RightsLink® service. For more information, please visit: http://www.ams.org/rightslink.

Send requests for translation rights and licensed reprints to reprint-permission@ams.org.

Excluded from these provisions is material for which the author holds copyright. In such cases, requests for permission to reuse or reprint material should be addressed directly to the author(s). Copyright ownership is indicated on the copyright page, or on the lower right-hand corner of the first page of each article within proceedings volumes.

©2015 by Terence Tao. All rights reserved.
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  20 19 18 17 16 15
In memory of Garth Gaudry, who set me on the road
§4.2. The Bourgain-Gamburd expansion machine

Chapter 5. Product theorems, pivot arguments, and the Larsen-Pink nonconcentration inequality

§5.1. The sum-product theorem
§5.2. Finite subgroups of SL$_2$
§5.3. The product theorem in SL$_2$(k)
§5.4. The product theorem in SL$_d$(k)
§5.5. Proof of the Larsen-Pink inequality

Chapter 6. Nonconcentration in subgroups

§6.1. Expansion in thin subgroups
§6.2. Random generators expand

Chapter 7. Sieving and expanders

§7.1. Combinatorial sieving
§7.2. The strong approximation property
§7.3. Sieving in thin groups

Part 2. Related Articles

Chapter 8. Cayley graphs and the algebra of groups

§8.1. A Hall-Witt identity for 2-cocycles

Chapter 9. The Lang-Weil bound

§9.1. The Stepanov-Bombieri proof of the Hasse-Weil bound
§9.2. The proof of the Lang-Weil bound
§9.3. Lang-Weil with parameters

Chapter 10. The spectral theorem and its converses for unbounded self-adjoint operators

§10.1. Self-adjointness and resolvents
§10.2. Self-adjointness and spectral measure
§10.3. Self-adjointness and flows
§10.4. Essential self-adjointness of the Laplace-Beltrami operator

Chapter 11. Notes on Lie algebras

§11.1. Abelian representations
§11.2. Engel’s theorem and Lie’s theorem
§11.3. Characterising semisimplicity
§11.4. Cartan subalgebras
| §11.5. | $\mathfrak{sl}_2$ representations | 245 |
| §11.6. | Root spaces | 247 |
| §11.7. | Classification of root systems | 251 |
| §11.8. | Chevalley bases | 258 |
| §11.9. | Casimirs and complete reducibility | 263 |

Chapter 12. Notes on groups of Lie type

| §12.1. | Simple Lie groups over $\mathbb{C}$ | 268 |
| §12.2. | Chevalley groups | 278 |
| §12.3. | Finite simple groups of Lie type | 288 |

Bibliography | 293 |

Index | 301 |
Preface

Expander graphs are a remarkable type of graph (or more precisely, a family of graphs) on finite sets of vertices that manage to simultaneously be both sparse (low-degree) and “highly connected” at the same time. They enjoy very strong mixing properties: if one starts at a fixed vertex of an (two-sided) expander graph and randomly traverses its edges, then the distribution of one's location will converge exponentially fast to the uniform distribution. For this and many other reasons, expander graphs are useful in a wide variety of areas of both pure and applied mathematics.

There are now many ways to construct expander graphs, but one of the earliest constructions was based on the Cayley graphs of a finite group (or of a finitely generated group acting on a finite set). The expansion property for such graphs turns out to be related to a rich variety of topics in group theory and representation theory, including Kazhdan’s property (T), Gowers’ notion of a quasirandom group, the sum-product phenomenon in arithmetic combinatorics, and the Larsen-Pink classification of finite subgroups of a linear group. Expansion properties of Cayley graphs have also been applied in analytic number theory through what is now known as the affine sieve of Bourgain, Gamburd, and Sarnak, which can count almost prime points in thin groups.

This text is based on the lecture notes from a graduate course on these topics I gave at UCLA in the winter of 2012, as well as from some additional posts on my blog at terrytao.wordpress.com on further related topics. The first part of this text can thus serve as the basis for a one-quarter or one-semester advanced graduate course, depending on how much of the optional material one wishes to cover. While the material here is largely self-contained, some basic graduate real analysis (in particular, measure
theory, Hilbert space theory, and the theory of $L^p$ norms), graph theory, and linear algebra (e.g., the spectral theorem for unitary matrices) will be assumed. Some prior familiarity with the classical Lie groups (particularly the special linear group $\text{SL}_n$ and the unitary group $U_n$) and representation theory will be helpful but not absolutely necessary. To follow Section 3.3 (which is optional) some prior exposure to Riemannian geometry would also be useful.

The core of the text is Part 1. After discussing the general theory of expander graphs in the first section, we then specialise to the case of Cayley graphs, starting with the remarkable observation of Margulis linking Kazhdan’s property (T) with expansion, and then turning to the more recent observations of Sarnak, Xue, Gamburd, and Bourgain linking the property of finite groups now known as quasirandomness with expansion, which is also related to the famous “3/16 theorem” of Selberg. As we will present in this text, this sets up a general “machine” introduced by Bourgain and Gamburd for verifying expansion in a Cayley graph, which in addition to quasirandomness requires two additional ingredients, namely a product theorem and a nonconcentration estimate. These two ingredients are then the focus of the next two sections of this part. The former ingredient uses techniques from arithmetic combinatorics related to the sum-product theorem, as well as estimates of Larsen and Pink on controlling the interaction between finite subgroups of a linear group and various algebraic varieties (such as conjugacy classes or maximal tori). The latter ingredient is perhaps the most delicate aspect of the theory, and often requires a detailed knowledge of the algebraic (and geometric) structure of the ambient group. Finally, we present an application of these ideas to number theory by introducing the basics of sieve theory, and showing how expansion results may be inserted into standard sieves to give new bounds on almost primes in thin groups.

Part 2 contains a variety of additional material that is related to one or more of the topics covered in Part 1, but which can be omitted for the purposes of teaching a graduate course on the subject.

Notation

For reasons of space, we will not be able to define every single mathematical term that we use in this book. If a term is italicised for reasons other than emphasis or for definition, then it denotes a standard mathematical object, result, or concept, which can be easily looked up in any number of references.

---

1This material in Section 2 is not absolutely required for subsequent sections of this part, although it does provide some helpful context for these later sections. Thus, this section may be abridged or even omitted altogether in a lecture course if desired.
Given a subset $E$ of a space $X$, the indicator function $1_E : X \to \mathbb{R}$ is defined by setting $1_E(x)$ equal to 1 for $x \in E$ and equal to 0 for $x \not\in E$.

The cardinality of a finite set $E$ will be denoted $|E|$. We will use\(^2\) the asymptotic notation $X = O(Y)$, $X \ll Y$, or $Y \gg X$ denote the estimate $|X| \leq CY$ for some absolute constant $C > 0$. In some cases we will need this constant $C$ to depend on a parameter (e.g., $d$), in which case we shall indicate this dependence by subscripts, e.g., $X = O_d(Y)$ or $X \ll_d Y$. We also sometimes use $X \sim Y$ as a synonym for $X \ll Y \ll X$. If $n$ is a parameter going to infinity, we let $o_{n \to \infty}(1)$ denote a quantity depending on $n$ and bounded in magnitude by $c(n)$ for some quantity $c(n)$ that goes to zero as $n \to \infty$. More generally, given an additional parameter such as $k$, we let $o_{n \to \infty; k}(1)$ denote a quantity that may depend on both $k$ and $n$, which is bounded by $c_k(n)$ for some quantity $c_k(n)$ that goes to zero as $n \to \infty$ for each fixed $k$.

**Acknowledgments**

I am greatly indebted to my students of the course on which this text was based, as well as many further commenters on my blog, including Ian Agol, Abhishek Bhowmick, Nick Cook, Sean Eberhard, Alireza Golsefidy, Joerg Grande, Ben Green, Dick Gross, Harald Helfgott, Arie Israel, David Joyner, Matthew Kahle, Emmanuel Kowalski, Wolfgang Moens, Vipul Niak, William Orrick, Mikhail Ostrovskii, David Roberts, Misha Rudnev, Alexander Shaposhnikov, Lior Silberman, Vit Tucek, Yilong Yang, and Wei Zhou. These comments can be viewed online at:

<http://terrytao.wordpress.com/category/teaching/254b-expansion-in-groups/>

The author was supported by the NSF grant DMS-0649473, the James and Carol Collins Chair, the Mathematical Analysis & Application Research Fund Endowment, and the Simons Foundation.

---

\(^2\)Once we deploy the machinery of nonstandard analysis in Section I, we will use a closely related, but slightly different, asymptotic notation.
Bibliography


Index

(B, N)-pair, 283
abelianisation, 230
adjacency matrix, 5
adjoint, 208
adjoint form, 271
adjoint representation, 231
affine algebraic variety, 187
almost prime, 144
approximate group, 86
asymptotic notation, xiii
autocorrelation function, 50

Balog-Szemerédi theorem, 91
Balog-Szemerédi-Gowers lemma
approximate group form, 93
product set form, 92
Bertini’s theorem, 198
beta sieve, 151
bipartite graph, 88
Bochner’s theorem, 49
Bonferroni inequalities, 19
Borel subgroup, 281
bounded functional calculus, 214
Bourgain-Gamburd expansion machine, 87
Bruhat decomposition, 283
Brun’s theorem, 155

Cartan decomposition, 247
Cartan matrix, 261
Cartan semisimplicity criterion, 232
Cartan solvability criterion, 240
Cartan subalgebra, 242
Cartan’s theorem, 270
Casimir operator, 264
Cayley graph, 23, 167
Cayley transform, 69
centre of a Lie algebra, 231
characteristic subalgebra, 239
Cheeger constant, 10
Chevalley basis, 263
Chevalley group, 281
Chevalley normalisation, 262
chromatic number, 14
class equation, 117
classical Lie algebra, 260
closure of an operator, 207
coboundary, 183
cocycle, 35, 179
combinatorial sieve, 150
compact form, 272
complemented subspace, 241
complete graph, 4, 8
complexity of an algebraic variety, 187
composition factors, 157
composition series, 157
concentration of measure, 15
concrete Lie algebra, 228
conjugacy class, 114
conjugacy of Cartans, 241
Connectivity of an expander graph, 14
correspondence to Balog-Szemerédi-Gowers, 85
convolution, 62
coroot, 249
coweight lattice, 276
<table>
<thead>
<tr>
<th>Term</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Coxeter diagram</td>
<td>253</td>
</tr>
<tr>
<td>cusp</td>
<td>70</td>
</tr>
<tr>
<td>cyclic vector</td>
<td>217</td>
</tr>
<tr>
<td>depolarisation</td>
<td>214</td>
</tr>
<tr>
<td>derivation</td>
<td>229</td>
</tr>
<tr>
<td>derived algebra</td>
<td>230</td>
</tr>
<tr>
<td>derived series</td>
<td>230</td>
</tr>
<tr>
<td>diagram</td>
<td>169</td>
</tr>
<tr>
<td>Diameter of an expander graph</td>
<td>14</td>
</tr>
<tr>
<td>dimension</td>
<td>126</td>
</tr>
<tr>
<td>dimension of an algebraic variety</td>
<td>187</td>
</tr>
<tr>
<td>direct product</td>
<td>229</td>
</tr>
<tr>
<td>direct sum</td>
<td>229</td>
</tr>
<tr>
<td>direct sum of representations</td>
<td>29</td>
</tr>
<tr>
<td>discrete Cheeger inequality</td>
<td>13</td>
</tr>
<tr>
<td>discrete Cheeger inequality, weak</td>
<td>10</td>
</tr>
<tr>
<td>Dynkin diagram</td>
<td>255</td>
</tr>
<tr>
<td>edge expansion</td>
<td>9</td>
</tr>
<tr>
<td>Engel's theorem</td>
<td>236</td>
</tr>
<tr>
<td>escape from subspaces</td>
<td>121</td>
</tr>
<tr>
<td>essentially self-adjoint operator</td>
<td>209</td>
</tr>
<tr>
<td>exceptional Lie algebra</td>
<td>260</td>
</tr>
<tr>
<td>expander family</td>
<td>6</td>
</tr>
<tr>
<td>expander mixing lemma</td>
<td>13</td>
</tr>
<tr>
<td>extended Dynkin diagram</td>
<td>257</td>
</tr>
<tr>
<td>flattening lemma</td>
<td>83, 98</td>
</tr>
<tr>
<td>Fokker-Planck equation</td>
<td>81</td>
</tr>
<tr>
<td>Frobenius endomorphism</td>
<td>190</td>
</tr>
<tr>
<td>Frobenius lemma</td>
<td>59</td>
</tr>
<tr>
<td>functional calculus</td>
<td>203</td>
</tr>
<tr>
<td>fundamental domain</td>
<td>70</td>
</tr>
<tr>
<td>generalised eigenspace</td>
<td>233</td>
</tr>
<tr>
<td>girth</td>
<td>12</td>
</tr>
<tr>
<td>Goursat's lemma</td>
<td>159</td>
</tr>
<tr>
<td>graph</td>
<td>4</td>
</tr>
<tr>
<td>graph Laplacian</td>
<td>6</td>
</tr>
<tr>
<td>graph metric</td>
<td>13</td>
</tr>
<tr>
<td>Hardy's inequality</td>
<td>73</td>
</tr>
<tr>
<td>Hasse-Weil bound</td>
<td>190</td>
</tr>
<tr>
<td>heat flow</td>
<td>218</td>
</tr>
<tr>
<td>Hellinger-Toeplitz theorem</td>
<td>209</td>
</tr>
<tr>
<td>Herglotz representation theorem</td>
<td>213</td>
</tr>
<tr>
<td>horocycle flow</td>
<td>54</td>
</tr>
<tr>
<td>hyperbolic plane</td>
<td>68</td>
</tr>
<tr>
<td>indecomposable representation</td>
<td>241</td>
</tr>
<tr>
<td>independent set</td>
<td>14</td>
</tr>
<tr>
<td>indicator function</td>
<td>xiii</td>
</tr>
<tr>
<td>induced representation</td>
<td>39</td>
</tr>
<tr>
<td>invariant subspace</td>
<td>217</td>
</tr>
<tr>
<td>invariant vector</td>
<td>30</td>
</tr>
<tr>
<td>involved torus</td>
<td>124</td>
</tr>
<tr>
<td>irreducible representation</td>
<td>57</td>
</tr>
<tr>
<td>irreducible representation</td>
<td>241</td>
</tr>
<tr>
<td>irreducible root system</td>
<td>250</td>
</tr>
<tr>
<td>isogeny</td>
<td>286</td>
</tr>
<tr>
<td>Jacobi identity</td>
<td>227</td>
</tr>
<tr>
<td>Jacobi operator</td>
<td>212</td>
</tr>
<tr>
<td>Jordan's theorem</td>
<td>67</td>
</tr>
<tr>
<td>Jordan-Chevalley decomposition</td>
<td>234</td>
</tr>
<tr>
<td>Jordan-Holder theorem</td>
<td>157</td>
</tr>
<tr>
<td>Katz-Tao lemma</td>
<td>107</td>
</tr>
<tr>
<td>Kazhdan constant</td>
<td>30</td>
</tr>
<tr>
<td>Killing form</td>
<td>281</td>
</tr>
<tr>
<td>Landau conjectures</td>
<td>143, 155</td>
</tr>
<tr>
<td>Lang-Weil bound</td>
<td>189</td>
</tr>
<tr>
<td>Lang-Weil with parameters</td>
<td>192</td>
</tr>
<tr>
<td>large sieve</td>
<td>156</td>
</tr>
<tr>
<td>Larsen-Pink inequality</td>
<td>113, 115, 122</td>
</tr>
<tr>
<td>Lefschetz principle</td>
<td>140</td>
</tr>
<tr>
<td>Legendre identity</td>
<td>148</td>
</tr>
<tr>
<td>Legendre sieve</td>
<td>148</td>
</tr>
<tr>
<td>Leibniz rule</td>
<td>229</td>
</tr>
<tr>
<td>Levi decomposition</td>
<td>282</td>
</tr>
<tr>
<td>Lie algebra</td>
<td>227</td>
</tr>
<tr>
<td>Lie algebra ideal</td>
<td>229</td>
</tr>
<tr>
<td>Lie's second theorem</td>
<td>269</td>
</tr>
<tr>
<td>Lie's theorem</td>
<td>237</td>
</tr>
<tr>
<td>Lie's third theorem</td>
<td>269</td>
</tr>
<tr>
<td>linear</td>
<td>45</td>
</tr>
<tr>
<td>Littlewood-Paley projection</td>
<td>223</td>
</tr>
<tr>
<td>lower central series</td>
<td>230</td>
</tr>
<tr>
<td>Lubotzky's 1-2-3 problem</td>
<td>136</td>
</tr>
<tr>
<td>Möbius function</td>
<td>148</td>
</tr>
<tr>
<td>Mautner phenomenon</td>
<td>58</td>
</tr>
<tr>
<td>maximal torus</td>
<td>111, 281</td>
</tr>
<tr>
<td>Mersenne prime</td>
<td>143</td>
</tr>
<tr>
<td>mixing inequality</td>
<td>63</td>
</tr>
<tr>
<td>modular curve</td>
<td>193</td>
</tr>
<tr>
<td>Moore ergodic theorem</td>
<td>54</td>
</tr>
<tr>
<td>multiplicative energy</td>
<td>92</td>
</tr>
<tr>
<td>nilpotent Lie algebra</td>
<td>230</td>
</tr>
<tr>
<td>nilpotent operator</td>
<td>234</td>
</tr>
<tr>
<td>nonconcentration estimate</td>
<td>87</td>
</tr>
<tr>
<td>normaliser</td>
<td>242</td>
</tr>
<tr>
<td>notation</td>
<td>xiii</td>
</tr>
</tbody>
</table>
Index

one-sided expander, 6
parabolic subgroup, 284
perfect group, 59
perfect Lie algebra, 230
pivot argument, 106
Poincaré disk, 69
Poincaré half-plane, 68
Poincaré inequality, 9
polar decomposition, 272
polarisation identity, 51
polycyclic Lie algebra, 231
primorial, 148
principal congruence subgroup, 74
principal modular curve, 70
principal series representation, 60
product theorem, 87, 101, 120
quasirandom group, 57
quasiregular representation, 29
quasisimple group, 271
radical of a Lie algebra, 232
Ramanujan graph, 7
rank of a Lie algebra, 244
Rayleigh quotient, 72
Ree groups, 290
regular element, 277
regular element of a Lie algebra, 242
regular graph, 4
regular representation, 29
regular semisimple element, 111
regular unipotent element, 111
representation (of a Lie algebra), 228
resolvent, 210
Resolvent identity, 210
root system, 250
root vector, 245
Ruzsa covering lemma, 93, 107
Ruzsa triangle inequality, 93, 107
Schrödinger propagator, 220
Schreier graph, 24
Schwarz-Zippel type bound, 138
Selberg sieve, 156
Selberg’s 3/16 theorem, 75
Selberg’s conjecture, 74
Selberg’s expander construction, 68
self-adjoint operator, 209
semidirect product, 229
semisimple Jordan decomposition, 241
semisimple Lie algebra, 232
semisimple operator, 234
short exact sequence, 228
simple Lie algebra, 231
simple Lie group, 271
solvable Lie algebra, 230
spectral gap, 71
split extension, 220
Steinberg group, 290
Steinberg representation, 60
Stone’s theorem, 220
strong approximation property, 169
subrepresentation, 30
sum-product theorem, 105
sumset estimates, 107
Suzuki groups, 290
Tits alternative, 138
transitivity of induction, 10
trivial representation, 28
twin prime, 148
twisted group of Lie type, 291
two-sided expander, 6
unipotent group, 111
unitary representation, 28
universal cover, 269
variety, 120
virtually quasirandom group, 66
wedding cake decomposition, 12
weight vector, 235
weighted Balog-Szemerédi-Gowers lemma, 86
weighted Balog-Szemerédi-Gowers theorem, 91
Weyl alcove, 224
Weyl chamber, 228
Weyl group, 257
Weyl’s complete reducibility theorem, 232, 263
Whitehead’s lemma, 264
Expander graphs are an important tool in theoretical computer science, geometric group theory, probability, and number theory. Furthermore, the techniques used to rigorously establish the expansion property of a graph draw from such diverse areas of mathematics as representation theory, algebraic geometry, and arithmetic combinatorics. This text focuses on the latter topic in the important case of Cayley graphs on finite groups of Lie type, developing tools such as Kazhdan’s property (T), quasirandomness, product estimates, escape from subvarieties, and the Balog–Szemerédi–Gowers lemma. Applications to the affine sieve of Bourgain, Gamburd, and Sarnak are also given. The material is largely self-contained, with additional sections on the general theory of expanders, spectral theory, Lie theory, and the Lang–Weil bound, as well as numerous exercises and other optional material.