Difference Sets
Connecting Algebra, Combinatorics, and Geometry
Difference Sets
Connecting Algebra, Combinatorics, and Geometry

Emily H. Moore
Harriet S. Pollatsek
Difference sets: connecting algebra, combinatorics, and geometry / Emily H. Moore, Harriet S. Pollatsek.

QA166.25.M66 2013
511′.6—dc23 2013006295

© 2013 by the American Mathematical Society. All rights reserved.

Visit the AMS home page at http://www.ams.org/
To Jack, Edie, and Ian Broadmoore
and to the memory of
David Pollatsek and Robert Liebler
## Contents

Preface \hspace{1cm} xi

Chapter 1. Introduction \hspace{1cm} 1

Chapter 2. Designs \hspace{1cm} 11
- 2.1. Incidence structures \hspace{1cm} 11
- 2.2. $t$-Designs \hspace{1cm} 14
- 2.3. Affine planes \hspace{1cm} 20
- 2.4. Symmetric designs \hspace{1cm} 26
- 2.5. Projective geometry \hspace{1cm} 30

Chapter 3. Automorphisms of Designs \hspace{1cm} 37
- 3.1. Group actions \hspace{1cm} 37
- 3.2. Automorphisms of symmetric designs \hspace{1cm} 40

Chapter 4. Introducing Difference Sets \hspace{1cm} 45
- 4.1. Definition and examples \hspace{1cm} 46
- 4.2. Difference sets and designs \hspace{1cm} 54
- 4.3. Integral group ring \hspace{1cm} 59
- 4.4. Equivalence \hspace{1cm} 65
## Chapter 5. Bruck-Ryser-Chowla Theorem

5.1. The BRC Theorem 72
5.2. Proof of BRC for $v$ odd 76
5.3. Partial converse and extension of BRC 84

## Chapter 6. Multipliers

6.1. Definition and examples 87
6.2. Existence of numerical multipliers 91
6.3. Multipliers fix $sD$ 94
6.4. Using multipliers 96
6.5. Multipliers in non-cyclic groups 99

## Chapter 7. Necessary Group Conditions

7.1. Intersection numbers 103
7.2. Turyn’s exponent bound 112
7.3. Dillon’s dihedral trick 116

## Chapter 8. Difference Sets from Geometry

8.1. Singer difference sets 121
8.2. Turyn’s construction 125
8.3. McFarland difference sets 129

## Chapter 9. Families from Hadamard Matrices

9.1. Hadamard matrices 135
9.2. Paley-Hadamard family: $v = 4n - 1$ 141
9.3. Hadamard family: $v = 4n$ 155

## Chapter 10. Representation Theory

10.1. Definitions and examples 167
10.2. Equivalent representations 177
10.3. Maschke’s Theorem 179
10.4. Representations and difference sets 191

## Chapter 11. Group Characters

11.1. Definitions and examples 198
## Contents

11.2. The Fundamental Theorem 201
11.3. Proof of the Fundamental Theorem 209
11.4. Characters and difference sets 220
11.5. Character tables 228

Chapter 12. Using Algebraic Number Theory 233
12.1. Why algebraic number theory? 233
12.2. Definitions and basic facts 235
12.3. Seeking difference sets 240
12.4. Proving Turyn’s exponent bound 247

Chapter 13. Applications 253
13.1. Binary sequences 253
13.2. Imaging with coded masks 257
13.3. Error correcting codes 261
13.4. Quantum information and MUBs 263

Appendix A. Background 267
Appendix B. Notation 273
Appendix C. Hints and Solutions to Selected Exercises 277

Bibliography 287
Index 293
Index of Parameters 297
Preface

We are drawn to the study of difference sets because this topic “be- longs both to group theory and to combinatorics and . . . uses tools from these areas as well as from geometry, number theory, and rep- resentation theory” (quoting from the opening of Chapter 1). Each of us has supervised undergraduate research on difference sets. Our original goal in writing this book was to collect in one place the ma- terial beyond a one-semester abstract algebra course required to prepare our students for these research projects. However, the links to many parts of mathematics led to our current, broader aim: not only to serve prospective undergraduate researchers but also to provide a rich text for a senior seminar or capstone course in mathematics. With this expanded goal in mind, we highlight these mathematical interconnections.

We never intended our book to be a comprehensive survey of difference sets. However, we hope it will encourage students to explore the literature on difference sets and give them a solid foundation so they can do so successfully.

We assume student readers have taken an abstract algebra course.\(^1\) We show them concrete examples of some algebraic ideas they studied there, and we apply and extend these concrete instances in a variety

---

\(^1\)Appendix A includes the background we need from prior courses, and specific results are cited using the notation A.x.
of settings. Some of our exposition, especially in earlier chapters, is very thorough, with reasoning fully explained. The proofs of some theorems are explicitly left for the exercises, and some of these exercises offer the student considerable guidance. For other theorems we may give rather terse proofs, more like what a student would encounter in a journal article. Normally we expect the reader to fill in any omitted arguments, so we don’t write “see the exercises” for each instance. In a few cases we quote theorems without proof, but always with a reference, and often with a comment on the accessibility of the proof given in the cited source.

Almost every section of the book ends with exercises. Some exercises aim to check the reader’s understanding of a definition or a proof. Some ask for proofs (with or without guidance). Some are puzzles to be solved. Some invite the student to explore ideas and examples, sometimes with the aid of a computer (and so indicated). All of these kinds of exercises vary from straightforward to challenging. Appendix C includes hints for exercises marked $\textcircled{H}$ and solutions to selected exercises marked $\textcircled{S}$.\(^2\) Every chapter except the first and the last ends with a brief Coda\(^3\) highlighting the main ideas and emphasizing mathematical connections.

Examples and exercises are numbered consecutively within chapters with, for example, Exercise 5 within a chapter and Exercise 7.5 for a reference to Exercise 5 in Chapter 7 made in a different chapter. Theorems are also numbered consecutively within chapters and are always referred to with both a chapter label and a theorem label, as, for example, Theorem 7.5 both within and outside of Chapter 7.

After the Introduction, Chapters 2–4 comprise the core of the book. We then see two kinds of selective paths through the rest. One would focus on representation theory and its applications. It would include Section 7.1 on intersection numbers, the constructions of difference sets in Chapters 8–9, Chapters 10–12, and Section 13.4. Another path would focus on the existence question for difference sets. It would include Chapters 5–9. Even if Chapters 10–12 are not

\(^2\)Complete solutions are available electronically for instructors; please send email to textbooks@ams.org for more information. Some helpful computer programs are available at http://www.ams.org/publications/authors/books/stml-67.

\(^3\)We borrow the term “coda” in this context from Jennifer Quinn.
covered, Sections 10.4 and 11.4 give a taste of the use of representation theory and characters in the study of difference sets. The applications in Sections 13.1–13.3 are suitable for readers following either path.

Acknowledgements.

We wish to thank the senior seminar and research students at Grinnell College and the REU students at Mount Holyoke College. Their enthusiasm inspired us, and their questions and reactions helped us shape this text. Mark Krusemeyer allowed us to borrow ideas and exercises from his Spring 2004 course on representation theory at Carleton College; we appreciate his generosity. We thank Robert McFarland for his sympathetic interest. John Polhill read several chapters and James A. Davis used parts of an early draft with an independent student; we thank them both for their encouragement. We owe a particular debt to Ken W. Smith, who read and commented on drafts of several chapters. We thank an anonymous reviewer for valuable advice on our treatment of the integral group ring. We are responsible for any errors or infelicities that remain. We are grateful for our support from the AMS: especially to Barbara Beeton for her unstinting technical assistance, to Thomas Costa for his careful and thoughtful copy-editing, and to Ina Mette for her interest and encouragement from the early days of our writing project. Finally, we thank Tom and Sandy for their love, support and many delicious dinners.

Emily Moore
Grinnell College

Harriet Pollatsek
Mount Holyoke College
Bibliography


affine plane, 20
  coordinatized, 23
  order, 21
automorphism
design, 40
bases
  mutually unbiased, 263
binary sequence
  autocorrelation, 255
  correlation, 254
  pseudorandom, 256
binary sequence of period \( v \), 253
block
  repeated, 12
block design, 15
  balanced incomplete, 15
Bruck-Ryser-Chowla Theorem, 72
Burnside’s Lemma, 40
centralizer, 40, 269
class function, 202
degree, 198
difference list, 108
difference set, 46
difference of, 202
complement, 15
complete, 15
game, 38
isomorphic, 67
irreducible, 198
irreducible, 198
orthogonality relations, 224
parameters, 16, 26
symmetric, 26
t-design, 14
complement, 60
cyclotomic, 144
development, 54
equivalent, 65
character, 198
code
  linear, 261
  commutator, 269
  commutator subgroup, 220, 269
  complete graph, 15
  conjugacy class, 269
  conjugation, 38
comment, 263
coordinatized projective plane, 32
cyclotomic classes, 149
  order, 149
cyclotomic field, 235
cyclotomic integers, 235
design
  automorphism, 40, 94
  block, 15
  complement, 17
  complete, 15
  isomorphic, 67
  parameters, 16, 26
  symmetric, 26
  \( t \)-design, 14
difference of, 202
difference of, 202
difference set, 46
centralizer, 40, 269
difference of, 202
complement, 15
isomorphic, 67
parameters, 16, 26
symmetric, 26
\( t \)-design, 14
difference of, 202
difference of, 202
centralizer, 40, 269
difference of, 202
complement, 15
isomorphic, 67
parameters, 16, 26
symmetric, 26
\( t \)-design, 14
<table>
<thead>
<tr>
<th>Term</th>
<th>Page(s)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Hadamard</td>
<td>112, 138, 155</td>
</tr>
<tr>
<td>Hall family</td>
<td>148, 150</td>
</tr>
<tr>
<td>McFarland</td>
<td>129</td>
</tr>
<tr>
<td>Menon</td>
<td>138, 159</td>
</tr>
<tr>
<td>normalized</td>
<td>53</td>
</tr>
<tr>
<td>offset</td>
<td>49</td>
</tr>
<tr>
<td>order</td>
<td>47</td>
</tr>
<tr>
<td>Paley</td>
<td>49, 144</td>
</tr>
<tr>
<td>Paley-Hadamard</td>
<td>138, 141</td>
</tr>
<tr>
<td>parameters</td>
<td>47</td>
</tr>
<tr>
<td>partial</td>
<td>144</td>
</tr>
<tr>
<td>relative</td>
<td>265</td>
</tr>
<tr>
<td>residue</td>
<td>144</td>
</tr>
<tr>
<td>reversible</td>
<td>92</td>
</tr>
<tr>
<td>semi-regular relative</td>
<td>265</td>
</tr>
<tr>
<td>shift</td>
<td>49</td>
</tr>
<tr>
<td>Singer</td>
<td>121, 145</td>
</tr>
<tr>
<td>translate</td>
<td>49</td>
</tr>
<tr>
<td>trivial</td>
<td>47</td>
</tr>
<tr>
<td>twin prime powers</td>
<td>51, 145</td>
</tr>
<tr>
<td>dihedral group</td>
<td>48</td>
</tr>
<tr>
<td>Dillon’s dihedral trick</td>
<td>116</td>
</tr>
<tr>
<td>diophantine equation</td>
<td>72</td>
</tr>
<tr>
<td>elementary abelian 2-group</td>
<td>89</td>
</tr>
<tr>
<td>Euler phi function</td>
<td>238</td>
</tr>
<tr>
<td>evaluation map</td>
<td>107</td>
</tr>
<tr>
<td>exponent bound</td>
<td>112, 162, 247</td>
</tr>
<tr>
<td>exponent of a group</td>
<td>269</td>
</tr>
<tr>
<td>Fano plane</td>
<td>5, 41</td>
</tr>
<tr>
<td>Fermat’s Last Theorem</td>
<td>235</td>
</tr>
<tr>
<td>field</td>
<td></td>
</tr>
<tr>
<td>construction</td>
<td>270</td>
</tr>
<tr>
<td>cyclotomic</td>
<td>235</td>
</tr>
<tr>
<td>four squares theorem</td>
<td></td>
</tr>
<tr>
<td>Gaussian integers</td>
<td>194</td>
</tr>
<tr>
<td>generalized dihedral extension</td>
<td>116</td>
</tr>
<tr>
<td>Gram-Schmidt</td>
<td>185</td>
</tr>
<tr>
<td>group</td>
<td></td>
</tr>
<tr>
<td>dihedral</td>
<td>48</td>
</tr>
<tr>
<td>quaternion</td>
<td>228</td>
</tr>
<tr>
<td>group action</td>
<td>37</td>
</tr>
<tr>
<td>regular</td>
<td>39, 55</td>
</tr>
<tr>
<td>transitive</td>
<td>39</td>
</tr>
<tr>
<td>group of units</td>
<td>270</td>
</tr>
<tr>
<td>group presentation</td>
<td>48</td>
</tr>
<tr>
<td>group ring</td>
<td>60</td>
</tr>
<tr>
<td>integral</td>
<td>59</td>
</tr>
<tr>
<td>Hadamard matrix</td>
<td>135, 141</td>
</tr>
<tr>
<td>equivalent</td>
<td>136</td>
</tr>
<tr>
<td>normalized</td>
<td>136</td>
</tr>
<tr>
<td>order</td>
<td>135</td>
</tr>
<tr>
<td>regular</td>
<td>138, 155</td>
</tr>
<tr>
<td>Hall polynomial</td>
<td>63</td>
</tr>
<tr>
<td>hyperplane</td>
<td>33, 268</td>
</tr>
<tr>
<td>ideal</td>
<td></td>
</tr>
<tr>
<td>prime</td>
<td>237</td>
</tr>
<tr>
<td>principal</td>
<td>237</td>
</tr>
<tr>
<td>unique factorization</td>
<td>237</td>
</tr>
<tr>
<td>incidence matrix</td>
<td>12</td>
</tr>
<tr>
<td>incidence structure</td>
<td>11</td>
</tr>
<tr>
<td>isomorphic</td>
<td>13</td>
</tr>
<tr>
<td>simple</td>
<td>12</td>
</tr>
<tr>
<td>inclusion-exclusion</td>
<td>271</td>
</tr>
<tr>
<td>inner product</td>
<td></td>
</tr>
<tr>
<td>class functions</td>
<td>202</td>
</tr>
<tr>
<td>complex</td>
<td>184</td>
</tr>
<tr>
<td>standard</td>
<td>183</td>
</tr>
<tr>
<td>integral group ring</td>
<td>59</td>
</tr>
<tr>
<td>intersection numbers</td>
<td>105</td>
</tr>
<tr>
<td>intertwining transformation</td>
<td>210</td>
</tr>
<tr>
<td>invariant subspace</td>
<td>170</td>
</tr>
<tr>
<td>inversion formula</td>
<td>225</td>
</tr>
<tr>
<td>Klein-four group</td>
<td>179, 191</td>
</tr>
<tr>
<td>Kronecker delta</td>
<td>229</td>
</tr>
<tr>
<td>Kronecker product</td>
<td>137</td>
</tr>
<tr>
<td>Lagrange’s Theorem</td>
<td>77</td>
</tr>
<tr>
<td>Legendre’s Theorem</td>
<td>73</td>
</tr>
<tr>
<td>Lehmer’s Lemma</td>
<td>151</td>
</tr>
<tr>
<td>Maschke’s Theorem</td>
<td>182, 188</td>
</tr>
<tr>
<td>matrix</td>
<td></td>
</tr>
<tr>
<td>equivalent</td>
<td>78</td>
</tr>
<tr>
<td>trace</td>
<td>42</td>
</tr>
<tr>
<td>unitary</td>
<td>185</td>
</tr>
<tr>
<td>McFarland difference sets</td>
<td>129</td>
</tr>
<tr>
<td>Menon construction</td>
<td>159</td>
</tr>
<tr>
<td>Mersenne primes</td>
<td>145</td>
</tr>
<tr>
<td>multiplier</td>
<td>88</td>
</tr>
<tr>
<td>left</td>
<td>88</td>
</tr>
<tr>
<td>numerical</td>
<td>89</td>
</tr>
<tr>
<td>orbit</td>
<td>97</td>
</tr>
</tbody>
</table>
Multiplier conjecture, 91
Multiplier Theorem
   First, 91
   Second, 91
multiset, 2, 46

octic residues, 98
orbit, 38
orbit-stabilizer theorem, 39
order
   affine plane, 21
cyclotomic classes, 149
difference set, 47
Hadamard matrix, 135
projective plane, 31
symmetric design, 27
orthogonal complement, 185

parallel, 20
partial difference set, 144
projective plane, 30
   coordinatized, 32
duality, 31
   order, 31
projective space, 33
   coordinatized, 33
quadratic residues, 27, 28, 49
quartic residues, 50

representation
   degree, 168
direct sum, 181
   equivalent, 177, 205, 210
   faithful, 168
irreducible, 171
left regular, 175
linear, 168
natural, 168, 173
reducible, 171
regular, 175, 205
restriction, 182
right regular, 175
trivial, 169
residues
   $e$th power, 149
root of unity, 270
   primitive, 270
Schur’s Lemma, 211
self-conjugate, 114
set
   $s$-set, 14
square-free integer, 73
stabilizer, 38
Steiner system, 15
structure theorem, 268
subspace
   $G$-invariant, 170
   invariant, 170
   stable, 170
   trivial, 170
Sylow $p$-subgroup, 269
Sylow theorems, 269
symmetric design, 26
   complement, 28
   order, 27
   parameters, 26
   trivial, 27
t-design, 14
trace, 42, 267
transformation
   intertwining, 210
   unitary, 185
Turyn’s construction, 125
twin primes, 51, 53, 92, 145
unique factorization domain, 235
unitary matrix, 185
unitary transformation, 185
vector
   length, 184
   orthogonal, 184
vector space
   direct sum, 180, 181
Witt’s Cancellation Theorem, 80
Index of Parameters

( 4,1,0 ), 157
( 7,3,1 ), 41, 54, 67, 124
( 7,4,2 ), 51
( 11,5,2 ), 54, 61, 98
design, 27
Paley, 47
( 13,4,1 ), 53, 54, 88, 89, 124
( 15,7,3 ), 47, 93, 97, 98, 125
TPP, 53
( 16,6,2 ), 75, 157
abelian (2,2,2,2), 68, 89, 96
abelian (4,2,2), 68
abelian (4,4), 58, 65, 68, 194
abelian (8,2), 66
design, 27, 29
non-abelian, 118
( 19,9,4 ), 29, 93, 148
( 21,5,1 ), 52
abelian, 90, 91, 93, 98
non-abelian, 49, 65
( 22,7,2 ), 72
( 23,11,5 ), 93
( 25,9,3 ), 75, 109, 240
( 31,15,7 ), 152, 154
Paley, 67
Singer, 67
( 31,6,1 ), 93
( 31, k, λ ), 99
( 35,17,8 ), 98
TPP, 53
TPP+, 92
( 36,15,6 ), 158
abelian (6,6), 48
( 37,9,2 ), 29, 53, 91, 93, 98
( 39,19,9 ), 84, 111, 144
( 40,13,4 ), 111
( 43, 7,1 ), 74
( 43,15,5 ), 73
( 43,21,10 ), 99
( 49,16,5 ), 72
( 49, k, λ ), 99
( 51,25,12 ), 75
( 56,11,2 ), 29
( 57,8,1 ), 110
( 64,28,12 ), 115
( 66,26,10 ), 246
( 67,12,2 ), 75
( 67, k, λ ), 99
( 71,15,3 ), 29, 75
( 73,9,1 ), 98
( 79,13,2 ), 29, 97
( 93,24,6 ), 75
( 99,49,24 ), 100
( 100,45,20 ), 162, 234
( 111,11,1 ), 74, 112
( 154,18,2 ), 245
( 160,54,18 ), 115
( 175,30,5 ), 115
( 201,25,3 ), 112
( 324,153,72 ), 115
Index of Parameters

(343,19,1), 73
(575,k,\lambda ), 102
Difference sets belong both to group theory and to combinatorics. Studying them requires tools from geometry, number theory, and representation theory. This book lays a foundation for these topics, including a primer on representations and characters of finite groups. It makes the research literature on difference sets accessible to students who have studied linear algebra and abstract algebra, and it prepares them to do their own research.

This text is suitable for an undergraduate capstone course, since it illuminates the many links among topics that the students have already studied. To this end, almost every chapter ends with a coda highlighting the main ideas and emphasizing mathematical connections. This book can also be used for self-study by anyone interested in these connections and concrete examples.

An abundance of exercises, varying from straightforward to challenging, invites the reader to solve puzzles, construct proofs, and investigate problems—by hand or on a computer. Hints and solutions are provided for selected exercises, and there is an extensive bibliography. The last chapter introduces a number of applications to real-world problems and offers suggestions for further reading.

Both authors are experienced teachers who have successfully supervised undergraduate research on difference sets.