

Combinatorics and Finite Geometry

This undergraduate textbook is suitable for introductory classes in combinatorics and related topics.

The book covers a wide range of both pure and applied combinatorics, beginning with the very basics of enumeration and then going on to Latin squares, graphs and designs. The latter topic is closely related to finite geometry, which is developed in parallel. Applications to probability theory, algebra, coding theory, cryptology and combinatorial game theory comprise the later chapters. Throughout the book, examples and exercises illustrate the material, and the interrelations between the various topics is emphasized.

Readers looking to take first steps toward the study of combinatorics, finite geometry, design theory, coding theory, or cryptology will find this book valuable. Essentially self-contained, there are very few prerequisites aside from some mathematical maturity, and the little algebra required is covered in the text. The book is also a valuable resource for anyone interested in discrete mathematics as it ties together a wide variety of topics.

ISBN 978-3-030-56394-3



1	Foundational Combinatorial Structures	1
1.1	Basic Counting	1
1.2	Multinomial Coefficients	12
1.3	Pigeonhole Principle	14
1.4	Permutations	16
1.4.1	Japanese Ladders	19
1.5	Generating Functions	27
1.5.1	Coin Counting	27
1.5.2	Fibonacci Sequence	31
2	Foundational Algebraic Structures	35
2.1	Modular Arithmetic	35
2.1.1	Euclidean Algorithm	36
2.1.2	Arithmetic Operations	38
2.1.3	Fermat's Little Theorem and Euler's Generalization	42
2.2	Finite Fields	49
2.3	Combinatorial Numbers	56
2.3.1	Geometric Numbers	56
2.3.2	Catalan Numbers	64
2.3.3	Stirling Numbers	69
2.3.4	Towers of Hanoi	72
3	Mutually Orthogonal Latin Squares	75
3.1	36 Officers and Latin Squares	75
3.2	Forming Latin Squares	87
3.3	Structure of Latin Squares	93
4	Affine and Projective Planes	97
4.1	Introduction	97
4.2	Definitions	99
4.3	Planes from Fields	107
4.4	Connection Between Affine Planes and MOLS	111
4.5	Fundamental Question	113

5	Graphs	117
5.1	Königsberg Bridge Problem	117
5.2	Simple Graphs	123
5.3	Colorings of Graphs	130
5.4	Directed Graphs and Relations	137
6	Higher Dimensional Finite Geometry	141
6.1	Linear Algebra	142
6.2	Affine Geometry	153
6.3	Projective Geometry	158
6.4	Desargues' Theorem	162
6.5	The Bruck–Ryser Theorem	164
6.6	Arcs and Ovals	167
6.7	Baer Subplanes	175
6.8	Translation Planes and Non-Desarguesian Planes	177
7	Designs	181
7.1	Designs	181
7.2	Biplanes	188
7.3	Symmetric Designs	190
7.4	Kirkman Schoolgirl Problem and Steiner Triple Systems	193
7.5	Nets and Transversal Designs	197
8	Combinatorial Objects	203
8.1	Introduction to Hadamard Matrices	203
8.2	Hadamard Designs	209
8.3	Generalized Hadamard Matrices	212
8.4	Latin Hypercubes	214
8.5	Partially Ordered Sets	216
8.6	Association Schemes	230
9	Discrete Probability—A Return to Counting	237
9.1	Definitions and Elementary Probability	237
9.2	Conditional Probability	242
10	Automorphism Groups	245
10.1	Groups	245
10.2	Automorphisms of a Design	253
10.3	Quasigroups	257
10.4	Difference Sets	259
11	Codes	263
11.1	Introduction	263
11.2	Basics of Coding Theory	265
11.3	Orthogonal Codes	268
11.4	Syndrome Decoding	272

11.5	The Binary Hamming Code and the Projective Plane of Order 2	275
11.6	Projective Geometry and Coding Theory	280
11.7	Sphere Packing Bound and Perfect Codes	281
11.8	MDS Codes	283
11.9	Weight Enumerators and the Assmus-Mattson Theorem	286
11.10	Codes of Planes	290
12	Cryptology	295
12.1	Substitution Ciphers	296
12.2	German Enigma Machine	306
12.3	Public-Key Cryptography	309
12.3.1	RSA Cryptosystem	313
12.3.2	El Gamal Cryptosystem	315
12.3.3	Diffie-Hellman Key Exchange	316
12.4	McEliece Cryptographic System	317
13	Games and Designs	321
13.1	The Game	322
13.2	Weight Functions	324
13.2.1	The Game on Planes	326
13.2.2	The Game on Biplanes	327
13.2.3	The Game on Symmetric Designs	328
13.2.4	The Game on Hadamard Designs	328
13.2.5	The Game on Nets	329
13.2.6	The Game on Steiner Triple Systems	330
14	Epilogue	333
	Solutions to Selected Odd Problems	335
	Glossary	357
	References	363
	Index	367