

Cambridge University Press

978-1-107-07400-2 - Applied Algebra and Number Theory: Essays in Honor of
Harald Niederreiter on the occasion of his 70th birthday

Edited by Gerhard Larcher, Friedrich Pillichshammer, Arne Winterhof and Chaoping Xing

Table of Contents

[More information](#)

Contents

<i>Preface</i>	<i>page xi</i>
1 Some highlights of Harald Niederreiter's work	1
<i>Gerhard Larcher, Friedrich Pillichshammer, Arne Winterhof and Chaoping Xing</i>	
1.1 A short biography	1
1.2 Uniform distribution theory and number theory	4
1.3 Algebraic curves, function fields and applications	7
1.4 Polynomials over finite fields and applications	10
1.5 Quasi-Monte Carlo methods	13
References	18
2 Partially bent functions and their properties	22
<i>Ayça Çeşmelioglu, Wilfried Meidl and Alev Topuzoğlu</i>	
2.1 Introduction	22
2.2 Basic properties	24
2.3 Examples and constructions	28
2.4 Partially bent functions and difference sets	29
2.5 Partially bent functions and Hermitian matrices	35
2.6 Relative difference sets revisited: a construction of bent functions	36
References	38
3 Applications of geometric discrepancy in numerical analysis and statistics	39
<i>Josef Dick</i>	
3.1 Introduction	39
3.2 Numerical integration in the unit cube	40
3.3 Numerical integration over the unit sphere	44
3.4 Inverse transformation and test sets	47

Cambridge University Press

978-1-107-07400-2 - Applied Algebra and Number Theory: Essays in Honor of

Harald Niederreiter on the occasion of his 70th birthday

Edited by Gerhard Larcher, Friedrich Pillichshammer, Arne Winterhof and Chaoping Xing

Table of Contents

[More information](#)

vi	Contents	
	3.5	Acceptance-rejection sampler 48
	3.6	Markov chain Monte Carlo and completely uniformly distributed sequences 51
	3.7	Uniformly ergodic Markov chains and push-back discrepancy 53
		References 54
4		Discrepancy bounds for low-dimensional point sets 58
		<i>Henri Faure and Peter Kritzer</i>
	4.1	Introduction 58
	4.2	Upper discrepancy bounds for low-dimensional sequences 66
	4.3	Upper discrepancy bounds for low-dimensional nets 75
	4.4	Lower discrepancy bounds for low-dimensional point sets 81
	4.5	Conclusion 87
		References 88
5		On the linear complexity and lattice test of nonlinear pseudorandom number generators 91
		<i>Domingo Gómez-Pérez and Jaime Gutierrez</i>
	5.1	Introduction 91
	5.2	Lattice test and quasi-linear complexity 93
	5.3	Quasi-linear and linear complexity 94
	5.4	Applications of our results 97
	5.5	An open problem 99
		References 99
6		A heuristic formula estimating the keystream length for the general combination generator with respect to a correlation attack 102
		<i>Rainer Göttfert</i>
	6.1	The combination generator 102
	6.2	The model 102
	6.3	Preliminaries 103
	6.4	The correlation attack 103
	6.5	The formula 105
		References 108
7		Point sets of minimal energy 109
		<i>Peter J. Grabner</i>
	7.1	Introduction 109
	7.2	Generalized energy and uniform distribution on the sphere 111

Cambridge University Press

978-1-107-07400-2 - Applied Algebra and Number Theory: Essays in Honor of
Harald Niederreiter on the occasion of his 70th birthday

Edited by Gerhard Larcher, Friedrich Pillichshammer, Arne Winterhof and Chaoping Xing

Table of Contents

[More information](#)

Contents		vii
7.3	Hyper-singular energies and uniform distribution	116
7.4	Discrepancy estimates	119
7.5	Some remarks on lattices	122
	References	123
8	The cross-correlation measure for families of binary sequences	126
	<i>Katalin Gyarmati, Christian Mauduit and András Sárközy</i>	
8.1	Introduction	126
8.2	The definition of the cross-correlation measure	129
8.3	The size of the cross-correlation measure	133
8.4	A family with small cross-correlation constructed using the Legendre symbol	135
8.5	Another construction	139
	References	141
9	On an important family of inequalities of Niederreiter involving exponential sums	144
	<i>Peter Hellekalek</i>	
9.1	Introduction	144
9.2	Concepts	148
9.3	A hybrid Erdős–Turán–Koksma inequality	157
	References	161
10	Controlling the shape of generating matrices in global function field constructions of digital sequences	164
	<i>Roswitha Hofer and Isabel Pirsic</i>	
10.1	Introduction	164
10.2	Global function fields	169
10.3	Constructions revisited	170
10.4	Designing morphological properties of the generating matrices	176
10.5	Computational results	182
10.6	Summary and outlook	185
	References	187
11	Periodic structure of the exponential pseudorandom number generator	190
	<i>Jonas Kaszian, Pieter Moree and Igor E. Shparlinski</i>	
11.1	Introduction	190
11.2	Preparations	194

Cambridge University Press

978-1-107-07400-2 - Applied Algebra and Number Theory: Essays in Honor of
Harald Niederreiter on the occasion of his 70th birthday

Edited by Gerhard Larcher, Friedrich Pillichshammer, Arne Winterhof and Chaoping Xing

Table of Contents

[More information](#)

viii	Contents	
	11.3 Main results	195
	11.4 Numerical results on cycles in the exponential map	199
	11.5 Comments	201
	References	202
12	Construction of a rank-1 lattice sequence based on primitive polynomials	204
	<i>Alexander Keller, Nikolaus Binder and Carsten Wächter</i>	
	12.1 Introduction	204
	12.2 Integro-approximation by rank-1 lattice sequences	205
	12.3 Construction	206
	12.4 Applications	211
	12.5 Conclusion	214
	References	214
13	A quasi-Monte Carlo method for the coagulation equation	216
	<i>Christian Lécot and Ali Tarhini</i>	
	13.1 Introduction	216
	13.2 The quasi-Monte Carlo algorithm	219
	13.3 Convergence analysis	222
	13.4 Numerical results	229
	13.5 Conclusion	229
	References	231
14	Asymptotic formulas for partitions with bounded multiplicity	235
	<i>Pierre Liardet and Alain Thomas</i>	
	14.1 Introduction	235
	14.2 Asymptotic expansion of $M_{U,q}$	239
	14.3 Proof of Theorem 14.2	246
	References	253
15	A trigonometric approach for Chebyshev polynomials over finite fields	255
	<i>Juliano B. Lima, Daniel Panario and Ricardo M. Campello de Souza</i>	
	15.1 Introduction	255
	15.2 Trigonometry in finite fields	257
	15.3 Chebyshev polynomials over finite fields	265
	15.4 Periodicity and symmetry properties of Chebyshev polynomials over finite fields	270

Cambridge University Press

978-1-107-07400-2 - Applied Algebra and Number Theory: Essays in Honor of
Harald Niederreiter on the occasion of his 70th birthday

Edited by Gerhard Larcher, Friedrich Pillichshammer, Arne Winterhof and Chaoping Xing

Table of Contents

[More information](#)

	Contents	ix
15.5	Permutation properties of Chebyshev polynomials over finite fields	273
15.6	Conclusions	278
	References	278
16	Index bounds for value sets of polynomials over finite fields	280
	<i>Gary L. Mullen, Daqing Wan and Qiang Wang</i>	
16.1	Introduction	280
16.2	Value sets of univariate polynomials	283
16.3	Permutation polynomial vectors	285
	References	294
17	Rational points of the curve $y^{q^n} - y = \gamma x^{q^h+1} - \alpha$ over \mathbb{F}_{q^m}	297
	<i>Ferruh Özbudak and Zülfükar Saygi</i>	
17.1	Introduction	297
17.2	Preliminaries	301
17.3	Proof of the main theorem	302
	References	306
18	On the linear complexity of multisequences, bijections between \mathbb{Z}ahlen and \mathbb{N}umber tuples, and partitions	307
	<i>Michael Vielhaber</i>	
18.1	Introduction and notation	307
18.2	Single sequences	309
18.3	Multilinear complexity	317
18.4	Partitions, bijections, conjectures	327
18.5	Open questions and further research	331
18.6	Conclusion	332
	References	332

The color plates are situated on page 337.