volume 187

lecture notes in pure and applied mathematics

complexity, logic, and recursion theory

edited by
Andrea Sorbi

CRC Press
Taylor & Francis Group

complexity, logic, and recursion theory

LECTURE NOTES IN PURE AND APPLIED MATHEMATICS

1. *N. Jacobson,* Exceptional Lie Algebras
2. *L.-Å. Lindahl and F. Poulsen,* Thin Sets in Harmonic Analysis
3. *I. Satake,* Classification Theory of Semi-Simple Algebraic Groups
4. *F. Hirzebruch, W. D. Newmann, and S. S. Koh, Differentiable Manifolds and Quadratic Forms*
5. *I. Chavel,* Riemannian Symmetric Spaces of Rank One
6. *R. B. Burckel,* Characterization of C(X) Among Its Subalgebras
7. *B. R. McDonald, A. R. Magid, and K. C. Smith,* Ring Theory: Proceedings of the Oklahoma Conference
8. *Y.-T. Siu,* Techniques of Extension on Analytic Objects
9. *S. R. Caradus, W. E. Pfaffenberger, and B. Yood,* Calkin Algebras and Algebras of Operators on Banach Spaces
10. *E. O. Roxin, P.-T. Liu, and R. L. Sternberg,* Differential Games and Control Theory
11. *M. Orzech and C. Small,* The Brauer Group of Commutative Rings
12. *S. Thomier,* Topology and Its Applications
13. *J. M. Lopez and K. A. Ross,* Sidon Sets
14. *W. W. Comfort and S. Negrepontis,* Continuous Pseudometrics
15. *K. McKennon and J. M. Robertson,* Locally Convex Spaces
16. *M. Carmeli and S. Malin,* Representations of the Rotation and Lorentz Groups: An Introduction
17. *G. B. Seligman,* Rational Methods in Lie Algebras
18. *D. G. de Figueiredo,* Functional Analysis: Proceedings of the Brazilian Mathematical Society Symposium
19. *L. Cesari, R. Kannan, and J. D. Schuur,* Nonlinear Functional Analysis and Differential Equations: Proceedings of the Michigan State University Conference
20. *J. J. Schäffer,* Geometry of Spheres in Normed Spaces
21. *K. Yano and M. Kon,* Anti-Invariant Submanifolds
22. *W. V. Vasconcelos,* The Rings of Dimension Two
23. *R. E. Chandler,* Hausdorff Compactifications
24. *S. P. Franklin and B. V. S. Thomas,* Topology: Proceedings of the Memphis State University Conference
25. *S. K. Jain,* Ring Theory: Proceedings of the Ohio University Conference
26. *B. R. McDonald and R. A. Morris,* Ring Theory II: Proceedings of the Second Oklahoma Conference
27. *R. B. Mura and A. Rhemtulla,* Orderable Groups
28. *J. R. Graef,* Stability of Dynamical Systems: Theory and Applications
29. *H.-C. Wang,* Homogeneous Branch Algebras
30. *E. O. Roxin, P.-T. Liu, and R. L. Sternberg,* Differential Games and Control Theory II
31. *R. D. Porter,* Introduction to Fibre Bundles
32. *M. Altman,* Contractors and Contractor Directions Theory and Applications
33. *J. S. Golan,* Decomposition and Dimension in Module Categories
34. *G. Fairweather,* Finite Element Galerkin Methods for Differential Equations
35. *J. D. Sally,* Numbers of Generators of Ideals in Local Rings
36. *S. S. Miller,* Complex Analysis: Proceedings of the S.U.N.Y. Brockport Conference
37. *R. Gordon,* Representation Theory of Algebras: Proceedings of the Philadelphia Conference
38. *M. Goto and F. D. Grosshans,* Semisimple Lie Algebras
39. *A. I. Arruda, N. C. A. da Costa, and R. Chuaqui,* Mathematical Logic: Proceedings of the First Brazilian Conference
40. *F. Van Oystaeyen,* Ring Theory: Proceedings of the 1977 Antwerp Conference
41. *F. Van Oystaeyen and A. Verschoren,* Reflectors and Localization: Application to Sheaf Theory
42. *M. Satyanarayana,* Positively Ordered Semigroups
43. *D. L Russell,* Mathematics of Finite-Dimensional Control Systems
44. *P.-T. Liu and E. Roxin,* Differential Games and Control Theory III: Proceedings of the Third Kingston Conference, Part A
45. *A. Geramita and J. Seberry,* Orthogonal Designs: Quadratic Forms and Hadamard Matrices
46. *J. Cigler, V. Losert, and P. Michor,* Banach Modules and Functors on Categories of Banach Spaces
47. *P.-T. Liu and J. G. Sutinen,* Control Theory in Mathematical Economics: Proceedings of the Third Kingston Conference, Part B
48. *C. Byrnes,* Partial Differential Equations and Geometry

49. *G. Klambauer,* Problems and Propositions in Analysis
50. *J. Knopfmacher,* Analytic Arithmetic of Algebraic Function Fields
51. *F. Van Oystaeyen,* Ring Theory: Proceedings of the 1978 Antwerp Conference
52. *B. Kadem,* Binary Time Series
53. *J. Barros-Neto and R. A. Artino,* Hypoelliptic Boundary-Value Problems
54. *R. L. Sternberg, A. J. Kalinowski, and J. S. Papadakis,* Nonlinear Partial Differential Equations in Engineering and Applied Science
55. *B. R. McDonald,* Ring Theory and Algebra III: Proceedngs of the Third Oklahoma Conference
56. *J. S. Golan,* Structure Sheaves Over a Noncommutative Ring
57. *T. V. Narayana, J. G. Williams, and R. M. Mathsen,* Combinatorics, Representation Theory and Statistical Methods in Groups: YOUNG DAY Proceedings
58. *T. A. Burton,* Modeling and Differential Equations in Biology
59. *K. H. Kim and F. W. Roush,* Introduction to Mathematical Consensus Theory
60. *J. Banas and K. Goebel,* Measures of Noncompactness in Banach Spaces
61. *O. A. Nielson,* Direct Integral Theory
62. *J. E. Smith, G. O. Kenny, and R. N. Ball,* Ordered Groups: Proceedings of the Boise State Conference
63. *J. Cronin,* Mathematics of Cell Electrophysiology
64. *J. W. Brewer,* Power Series Over Commutative Rings
65. *P. K. Kamthan and M. Gupta,* Sequence Spaces and Series
66. *T. G. McLaughlin,* Regressive Sets and the Theory of Isols
67. *T. L. Herdman, S. M. Rankin III, and H. W. Stech,* Integral and Functional Differential Equations
68. *R. Draper,* Commutative Algebra: Analytic Methods
69. *W. G. McKay and J. Patera,* Tables of Dimensions, Indices, and Branching Rules for Representations of Simple Lie Algebras
70. *R. L. Devaney and Z. H. Nitecki,* Classical Mechanics and Dynamical Systems
71. *J. Van Geel,* Places and Valuations in Noncommutative Ring Theory
72. *C. Faith,* Injective Modules and Injective Quotient Rings
73. *A. Fiacco,* Mathematical Programming with Data Perturbations I
74. *P. Schultz, C. Praeger, and R. Sullivan,* Algebraic Structures and Applications: Proceedings of the First Western Australian Conference on Algebra
75. *L Bican, T. Kepka, and P. Nemec,* Rings, Modules, and Preradicals
76. *D. C. Kay and M. Breen,* Convexity and Related Combinatorial Geometry: Proceedings of the Second University of Oklahoma Conference
77. *P. Fletcher and W. F. Lindgren,* Quasi-Uniform Spaces
78. *C.-C. Yang,* Factorization Theory of Meromorphic Functions
79. *O. Taussky,* Ternary Quadratic Forms and Norms
80. *S. P. Singh and J. H. Burry,* Nonlinear Analysis and Applications
81. *K. B. Hannsgen, T. L. Herdman, H. W. Stech, and R. L. Wheeler,* Volterra and Functional Differential Equations
82. *N. L. Johnson, M. J. Kallaher, and C. T. Long,* Finite Geometries: Proceedings of a Conference in Honor of T. G. Ostrom
83. *G. I. Zapata,* Functional Analysis, Holomorphy, and Approximation Theory
84. *S. Greco and G. Valla,* Commutative Algebra: Proceedings of the Trento Conference
85. *A. V. Fiacco,* Mathematical Programming with Data Perturbations II
86. *J.-B. Hiriart-Urruty, W. Oettli, and J. Stoer,* Optimization: Theory and Algorithms
87. *A. Figa Talamanca and M. A. Picardello,* Harmonic Analysis on Free Groups
88. *M. Harada,* Factor Categories with Applications to Direct Decomposition of Modules
89. *V. I. Istrăţescu,* Strict Convexity and Complex Strict Convexity
90. *V. Lakshmikantham,* Trends in Theory and Practice of Nonlinear Differential Equations
91. *H. L. Manocha and J. B. Srivastava,* Algebra and Its Applications
92. *D. V. Chudnovsky and G. V. Chudnovsky,* Classical and Quantum Models and Arithmetic Problems
93. *J. W. Longley,* Least Squares Computations Using Orthogonalization Methods
94. *L. P. de Alcantara,* Mathematical Logic and Formal Systems
95. *C. E. Aull,* Rings of Continuous Functions
96. *R. Chuaqui,* Analysis, Geometry, and Probability
97. *L. Fuchs and L. Salce,* Modules Over Valuation Domains
98. *P. Fischer and W. R. Smith,* Chaos, Fractals, and Dynamics
99. *W. B. Powell and C. Tsinakis,* Ordered Algebraic Structures
100. *G. M. Rassias and T. M. Rassias,* Differential Geometry, Calculus of Variations, and Their Applications

101. *R.-E. Hoffmann and K. H. Hofmann,* Continuous Lattices and Their Applications
102. *J. H. Lightbourne III and S. M. Rankin III,* Physical Mathematics and Nonlinear Partial Differential Equations
103. *C. A. Baker and L. M. Batten,* Finite Geometrics
104. *J. W. Brewer, J. W. Bunce, and F. S. Van Vleck,* Linear Systems Over Commutative Rings
105. *C. McCrory and T. Shifrin,* Geometry and Topology: Manifolds, Varieties, and Knots
106. *D. W. Kueker, E. G. K. Lopez-Escobar, and C. H. Smith,* Mathematical Logic and Theoretical Computer Science
107. *B.-L. Lin and S. Simons,* Nonlinear and Convex Analysis: Proceedings in Honor of Ky Fan
108. *S. J. Lee,* Operator Methods for Optimal Control Problems
109. *V. Lakshmikantham,* Nonlinear Analysis and Applications
110. *S. F. McCormick,* Multigrid Methods: Theory, Applications, and Supercomputing
111. *M. C. Tangora,* Computers in Algebra
112. *D. V. Chudnovsky and G. V. Chudnovsky,* Search Theory: Some Recent Developments
113. *D. V. Chudnovsky and R. D. Jenks,* Computer Algebra
114. *M. C. Tangora,* Computers in Geometry and Topology
115. *P. Nelson, V. Faber, T. A. Manteuffel, D. L. Seth, and A. B. White, Jr.,* Transport Theory, Invariant Imbedding, and Integral Equations: Proceedings in Honor of G. M. Wing's 65th Birthday
116. *P. Clément, S. Invernizzi, E. Mitidieri, and I. I. Vrabie,* Semigroup Theory and Applications
117. *J. Vinuesa,* Orthogonal Polynomials and Their Applications: Proceedings of the International Congress
118. *C. M. Dafermos, G. Ladas, and G. Papanicolaou,* Differential Equations: Proceedings of the EQUADIFF Conference
119. *E. O. Roxin,* Modern Optimal Control: A Conference in Honor of Solomon Lefschetz and Joseph P. Lasalle
120. *J. C. Díaz,* Mathematics for Large Scale Computing
121. *P. S. Milojevič,* Nonlinear Functional Analysis
122. *C. Sadosky,* Analysis and Partial Differential Equations: A Collection of Papers Dedicated to Mischa Cotlar
123. *R. M. Shortt,* General Topology and Applications: Proceedings of the 1988 Northeast Conference
124. *R. Wong,* Asymptotic and Computational Analysis: Conference in Honor of Frank W. J. Olver's 65th Birthday
125. *D. V. Chudnovsky and R. D. Jenks,* Computers in Mathematics
126. *W. D. Wallis, H. Shen, W. Wei, and L. Zhu,* Combinatorial Designs and Applications
127. *S. Elaydi,* Differential Equations: Stability and Control
128. *G. Chen, E. B. Lee, W. Littman, and L. Markus,* Distributed Parameter Control Systems: New Trends and Applications
129. *W. N. Everitt,* Inequalities: Fifty Years On from Hardy, Littlewood and Pólya
130. *H. G. Kaper and M. Garbey,* Asymptotic Analysis and the Numerical Solution of Partial Differential Equations
131. *O. Arino, D. E. Axelrod, and M. Kimmel,* Mathematical Population Dynamics: Proceedings of the Second International Conference
132. *S. Coen,* Geometry and Complex Variables
133. *J. A. Goldstein, F. Kappel, and W. Schappacher,* Differential Equations with Applications in Biology, Physics, and Engineering
134. *S. J. Andima, R. Kopperman, P. R. Misra, J. Z. Reichman, and A. R. Todd,* General Topology and Applications
135. *P Clément, E. Mitidieri, B. de Pagter,* Semigroup Theory and Evolution Equations: The Second International Conference
136. *K. Jarosz,* Function Spaces
137. *J. M. Bayod, N. De Grande-De Kimpe, and J. Martínez-Maurica,* *p*-adic Functional Analysis
138. *G. A. Anastassiou,* Approximation Theory: Proceedings of the Sixth Southeastern Approximation Theorists Annual Conference
139. *R. S. Rees,* Graphs, Matrices, and Designs: Festschrift in Honor of Norman J. Pullman
140. *G. Abrams, J. Haefner, and K. M. Rangaswamy,* Methods in Module Theory
141. *G. L. Mullen and P. J.-S. Shiue,* Finite Fields, Coding Theory, and Advances in Communications and Computing
142. *M. C. Joshi and A. V. Balakrishnan,* Mathematical Theory of Control: Proceedings of the International Conference

143. *G. Komatsu and Y. Sakane*, Complex Geometry: Proceedings of the Osaka International Conference
144. *I. J. Bakelman*, Geometric Analysis and Nonlinear Partial Differential Equations
145. *T. Mabuchi and S. Mukai*, Einstein Metrics and Yang–Mills Connections: Proceedings of the 27th Taniguchi International Symposium
146. *L. Fuchs and R. Göbel*, Abelian Groups: Proceedings of the 1991 Curaçao Conference
147. *A. D. Pollington and W. Moran*, Number Theory with an Emphasis on the Markoff Spectrum
148. *G. Dore, A. Favini, E. Obrecht, and A. Venni*, Differential Equations in Banach Spaces
149. *T. West*, Continuum Theory and Dynamical Systems
150. *K. D. Bierstedt, A. Pietsch, W. Ruess, and D. Vogt*, Functional Analysis
151. *K. G. Fischer, P. Loustaunau, J. Shapiro, E. L. Green, and D. Farkas*, Computational Algebra
152. *K. D. Elworthy, W. N. Everitt, and E. B. Lee*, Differential Equations, Dynamical Systems, and Control Science
153. *P.-J. Cahen, D. L. Costa, M. Fontana, and S.-E. Kabbaj*, Commutative Ring Theory
154. *S. C. Cooper and W. J. Thron*, Continued Fractions and Orthogonal Functions: Theory and Applications
155. *P. Clément and G. Lumer*, Evolution Equations, Control Theory, and Biomathematics
156. *M. Gyllenberg and L. Persson*, Analysis, Algebra, and Computers in Mathematical Research: Proceedings of the Twenty-First Nordic Congress of Mathematicians
157. *W. O. Bray, P. S. Milojevič and Č. V. Stanojevič*, Fourier Analysis: Analytic and Geometric Aspects
158. *J. Bergen and S. Montgomery*, Advances in Hopf Algebras
159. *A. R. Magid*, Rings, Extensions, and Cohomology
160. *N. H. Pavel*, Optimal Control of Differential Equations
161. *M. Ikawa*, Spectral and Scattering Theory: Proceedings of the Taniguchi International Workshop
162. *X. Liu and D. Siegel*, Comparison Methods and Stability Theory
163. *J.-P. Zolésio*, Boundary Control and Variation
164. *M. Křížek, P. Neittaanmäki, and R. Stenberg*, Finite Element Methods: Fifty Years of the Courant Element
165. *G. Da Prato and L. Tubaro*, Control of Partial Differential Equations
166. *E. Ballico*, Projective Geometry with Applications
167. *M. Costabel, M. Dauge, and S. Nicaise*, Boundary Value Problems and Integral Equations in Nonsmooth Domains
168. *G. Ferreyra, G. R. Goldstein, and F. Neubrander*, Evolution Equations
169. *S. Huggett*, Twistor Theory
170. *H. Cook, W. T. Ingram, K. T. Kuperberg, A. Lelek, and P. Minc*, Continua: With the Houston Problem Book
171. *D. F. Anderson and D. E. Dobbs*, Zero-Dimensional Commutative Rings
172. *K. Jarosz*, Function Spaces: The Second Conference
173. *V. Ancona, E. Ballico, and A. Silva*, Complex Analysis and Geometry
174. *E. Casas*, Control of Partial Differential Equations and Applications
175. *N. Kalton, E. Saab, and S. Montgomery-Smith*, Interaction Between Functional Analysis, Harmonic Analysis, and Probability
176. *Z. Deng, Z. Liang, G. Lu, and S. Ruan*, Differential Equations and Control Theory
177. *P. Marcellini, G. Talenti, and E. Vesentini*, Partial Differential Equations and Applications: Collected Papers in Honor of Carlo Pucci
178. *A. Kartsatos*, Theory and Applications of Nonlinear Operators of Accretive and Monotone Type
179. *M. Maruyama*, Moduli of Vector Bundles
180. *A. Ursini and P. Aglianò*, Logic and Algebra
181. *X. H. Cao, S. X. Liu, K. P. Shum, and C. C. Yang*, Rings, Groups, and Algebras
182. *D. Arnold and R. M. Rangaswamy*, Abelian Groups and Modules
183. *S. R. Chakravarthy and A. S. Alfa*, Matrix-Analytic Methods in Stochastic Models
184. *J. E. Andersen, J. Dupont, H. Pedersen, and A. Swann*, Geometry and Physics
185. *P.-J. Cahen, M. Fontana, E. Houston, and S.-E. Kabbaj*, Commutative Ring Theory: Proceedings of the II International Conference
186. *J. A. Goldstein, N. E. Gretsky, and J. J. Uhl, Jr.*, Stochastic Processes and Functional Analysis
187. *A. Sorbi*, Complexity, Logic, and Recursion Theory
188. *G. Da Prato and J.-P. Zolésio*, Partial Differential Equation Methods in Control and Shape Analysis

Additional Volumes in Preparation

complexity, logic, and recursion theory

edited by

Andrea Sorbi
University of Siena
Siena, Italy

CRC Press
Taylor & Francis Group
Boca Raton London New York

CRC Press is an imprint of the
Taylor & Francis Group, an **informa** business

CRC Press
Taylor & Francis Group
6000 Broken Sound Parkway NW, Suite 300
Boca Raton, FL 33487-2742

First issued in hardback 2019

ISBN-13: 978-0-8247-0026-3 (pbk)
ISBN-13: 978-1-138-40410-6 (hbk)

Visit the Taylor & Francis Web site at
http://www.taylorandfrancis.com

and the CRC Press Web site at
http://www.crcpress.com

Library of Congress Cataloging-in-Publication Data

Complexity, logic, and recursion theory / edited by Andrea Sorbi.
p. cm. — (Lecture notes in pure and applied mathematics ; v. 187)
ISBN 0-8247-0026-0 (alk. paper)
1. Computational complexity. 2. Recursion theory. I. Sorbi, Andrea. II. Series.
QA267.7.C664 1997
511.3—dc21

96-52019
CIP

Preface

This book is a collection of refereed papers representing the research undertaken in the network *Complexity, Logic and Recursion Theory COLORET* (Contract No. ERBCHRXCT930415) of the Human Capital and Mobility European project. The activity of the network commenced on January 1, 1994, lasting three years and including three workshops (Amsterdam, Siena, and Barcelona). Scientists from Amsterdam, Barcelona, Heidelberg, Leeds, Siena, and Turin participated. The network was subsequently joined by researchers from Prague, Kazan, and Novosibirsk in the PECO project, supplementary agreement No. CIPDCT940615 to the COLORET contract.

The project brought together the two classical approaches to computability: the recursion theoretic approach, based on classifying the objects of the noncomputable universe according to their degree of noncomputability, and the complexity theoretic approach, based on classifying computable objects according to their degree of difficulty of computation.

The project stimulated collaboration between the participants, with many research visits within the network. It also promoted the training of young scientists from the various centres of COLORET.

The contents of the book are significant examples of the kind of work pursued in the project. Almost all are either authored or coauthored by scientists from the network or scientists who have for some time participated in the network, with the exceptions of Downey and Gasarch, whose contributions, reflecting areas of research relevant to the network, were presented at the Siena and Barcelona COLORET workshops respectively.

We wish to thank all the contributors to the book. We thank also Paolo Aglianò and Richard Coles for their help in preparing the volume

Andrea Sorbi

Contents

Contributors

Klaus Ambos-Spies Universität Heidelberg, Heidelberg, Germany

Marat Arslanov Kazan State University, Kazan, Russia

José L. Balcázar Universitat Politècnica de Catalunya, Barcelona, Spain

S. Barry Cooper University of Leeds, Leeds, England

Robert A. Di Paola Queens College of the City University of New York, New York, New York

Rodney G. Downey Victoria University, Wellington, New Zealand

Sophie Fischer IBM, Uithoorn, The Netherlands

William Gasarch University of Maryland, College Park, Maryland

Ricard Gavaldà Universitat Politècnica de Catalunya, Barcelona, Spain

Lane Hemaspaandra University of Rochester, Rochester, New York

Montserrat Hermo Universidad del País Vasco, San Sebastián, Spain

Elvira Mayordomo Universidad de Zaragoza, Zaragoza, Spain

Franco Montagna Università di Siena, Siena, Italy

André Nies University of Chicago, Chicago, Illinois

Piergiorgio Odifreddi Università di Torino, Torino, Italy

Carl H. Smith University of Maryland, College Park, Maryland

Andrea Sorbi Università di Siena, Siena, Italy

Leen Torenvliet University of Amsterdam, Amsterdam, The Netherlands

Peter van Emde Boas University of Amsterdam, Amsterdam, The Netherlands

complexity, logic, and recursion theory

Resource-Bounded Measure and Randomness

Klaus Ambos-Spies Universität Heidelberg, Heidelberg, Germany

Elvira Mayordomo Universidad de Zaragoza, Zaragoza, Spain

Abstract

We survey recent results on resource-bounded measure and randomness in structural complexity theory. In particular, we discuss applications of these concepts to the exponential time complexity classes $\mathbf{E}$ and $\mathbf{E}_2$. Moreover, we treat time-bounded genericity and stochasticity concepts which are weaker than time-bounded randomness but which suffice for many of the applications in complexity theory.

1 Introduction

The first attempt for defining the concept of a random sequence goes back to von Mises [vM19] in 1919. He proposed that an infinite 0-1-sequence S should be considered to be random if, in the limit, the number of the occurrences of the 0s and 1s in S is the same (i.e. the sequence S satisfies the law of large numbers) and if this stability property is inherited by every infinite subsequence of S obtained by an admissible selection rule. A fuzzyness in this concept, due to the lack of a formal definition of admissibility was later eliminated by Church [Ch40] in 1940, who proposed that a selection rule should be admissible if it is given by a recursive, i.e. in a formal sense computable, function, thereby introducing the first concept of algorithmic randomness. As observed by Ville [Vi39] in 1939 already, the von Mises-Church approach to randomness is not satisfying from the point of view of probability theory, however, since random sequences in this sense may fail to satisfy some of the fundamental statistical laws. In particular, Ville constructed such a random sequence which failed to show the typical speed of convergence in the ratio of the 0s and 1s as it is expressed by the law of the iterated logarithm.

The search for more satisfying randomness notions was completed by Martin-Löf [ML66] in 1966 who defined random sequences satisfying all recursive (in fact recursively enumerable) statistical tests. The robustness of this concept was demonstrated by alternative characterizations in terms of the descriptional (Kolmogorov) complexity of the

Supported by the Human Capital and Mobility Program of the European Community under grant ERB-CHRX-CT93-0415 (COLORET).

finite initial segments of a random sequence (see Li and Vitányi [LV93] for details) and in terms of betting strategies, called martingales (Schnorr [Sch71a], [Sch71b]).

Schnorr also used the martingale characterization of Martin-Löfs randomness concept to point out that, being a notion of recursively enumerable randomness, this concept is too restrictive and he proposed two notions of recursive randomness which he considered to be more adequate. Though it seems that his criticism was not widely accepted, his martingale approach led in a very natural way to resource-bounded measure and randomness concepts in complexity theory. Unfortunately, his notions of time-bounded randomness did not find the attention in complexity theory they deserved, and only recent attempts of Lutz ([Lu90], [Lu92]) for defining measures on the fundamental complexity classes like exponential time led to the rediscovery of Schnorr's concept. Though Lutz's and Schnorr's approach have somewhat different motivations they are equivalent in the sense that each one can be defined in terms of the other one. Lutz's goal was to define a measure on complexity classes sharing the fundamental properties of the classical Lebesgue measure thereby producing a powerful tool for analyzing quantitative, structural aspects of these complexity classes. Since complexity classes are countable and any countable class has measure 0 in the classical sense, this approach had to be based on resource-bounded measure concepts, which are also the basis for the definition of resource-bounded randomness concepts.

In this survey we present the fundamental results of Lutz's resource-bounded measure theory and Schnorr's resource-bounded randomness and their applications in structural complexity theory. We restrict ourselves to the case of deterministic-time complexity, which has been mainly treated in the literature so far. Most of the results are given with complete proofs. We emphasize the relations between Lutz's and Schnorr's approach by focusing on randomness and by proving numerous measure results via randomness. Moreover, we emphasize some concepts, strictly weaker than resource-bounded randomness but sufficient for many applications in complexity theory: the resource-bounded genericity concept of Ambos-Spies, Fleischhack and Huwig [AFH88] and resource-bounded stochasticity, which is the resource-bounded variant of the von Mises-Church-randomness concept recently introduced in [AMWZ96].

The outline of the paper is as follows. In Section 2 we introduce the fragment of Lebesgue measure theory needed in the following and we describe this theory in terms of martingales. Resource-bounded martingales and resource-bounded measure and randomness based on this concept are introduced in Section 3, where also some of the fundamental results on these notions are proven. In Section 4 the aspects of resource-bounded randomness captured by the weaker genericity concept of [AFH88] are discussed and a series of applications in structural complexity is given. Resource-bounded stochasticity and some of its applications are presented in Section 5. In Sections 6 and 7 Lutz's measure on the exponential time classes $\mathbf{E}$ and $\mathbf{E}_2$ is discussed in some detail. In Section 8 the limitations of resource-bounded genericity and stochasticity compared with randomness are discussed and some applications of resource-bounded randomness in complexity theory which seem to require the full strength of this concept are given. In Section 9 we investigate the internal structure of the class $\mathbf{NP}$ under some measure hypothesis and other strong hypotheses. In Section 10 we shortly summarize further work related to this survey.

The basic objects of structural complexity theory are sets of binary strings, whereas the basic objects of measure theory are infinite 0-1-sequences. By identifying sets with their characteristic sequence, however, we can bridge this gap. Since there are $2^n - 1$ binary strings of length less than n, the length of initial segment $A\restriction x$ of the characteristic sequence of a set A will be exponential in the length of x. Since martingales will have initial segments of sets as their inputs and since the complexity of a set or function is measured in the input length, this will imply that $t(n)$-randomness based on martingales computable in time $t(n)$ will be randomness for the deterministic time class $\mathbf{DTIME}(t(2^n - 1))$, not for $\mathbf{DTIME}(t(n))$. This fact is also responsible for problems in defining randomness for subexponential complexity classes. Here we will not discuss this problem, which has not been completely solved yet. For partial solutions we refer the reader to Allender and Strauss ([AS94], [AS95]) and Mayordomo [Ma94c].

We conclude this section by introducing some basic notation.

Let $\Sigma^* = \{0,1\}^*$ denote the set of finite binary strings. For a string x, $x(m)$ denotes the $(m+1)$th bit in x, i.e., $x = x(0)...x(n-1)$, where $n = |x|$ is the length of x. λ is the empty string. $x \sqsubseteq y$ denotes that the string x is extended by y and $x \sqsubset y$ denotes that this extension is proper. We identify strings with numbers, by letting n be the $(n+1)$th string under the canonical length-lexicographical ordering. Since there are 2^m strings of length m, $|n| \approx \log(n)$. N, Q, R denote the sets of natural, rational, and real numbers, respectively. $[0,1]$ is the unit interval in R. Lower case letters $..., x, y, z$ from the end of the alphabet will be used to denote strings, while the other letters denote numbers, with the exception of d, f, g, h and s, t which also denote functions. Lower case Greek letters denote reals.

A set of strings is called a *problem* or shortly a *set*, while sets of sets are called *classes*. Capital letters denote sets, boldface capital letters classes.
$||A||$ is the cardinality of the set A. We let $A^{\leq n} = \{x \in A : |x| \leq n\}$ and $A^{=n} = \{x \in A : |x| = n\}$. A set A is called *sparse* if there is a polynomial p such that $\| A^{\leq n} \| \leq p(n)$ for each n, and A is *exponentially dense* if there is a real number $\alpha > 0$ such that $\| A^{\leq n} \| > 2^{n^\alpha}$ almost everywhere. For sets A and B, $A \oplus B = \{0x : x \in A\} \cup \{1x : x \in B\}$ is the join (effective disjoint union) and $A \Delta B = (A - B) \cup (B - A)$ is the symmetric difference of A and B.

We identify a set with its infinite characteristic sequence, i.e., $x \in A$ iff $A(x) = 1$ and $x \notin A$ iff $A(x) = 0$, so that $2^\omega = \{0,1\}^\infty$, the set of infinite binary sequences, is identified with the power class $\mathcal{P}(\{0,1\}^*)$ of $\{0,1\}^*$. We let $A\restriction n$ denote the initial segment $A(0)...A(n-1) \in \{0,1\}^*$ of A of length n. We write $x \sqsubset A$ and say that A *extends* x if x is a finite initial segment of A. The class of all sets extending a string x is denoted by $\mathbf{B}_x = \{A : x \sqsubset A\}$.

We will use strings in two different meanings: as elements of sets and as finite initial segments of sets. In an attempt to avoid confusion, usually we will use the notation $X\restriction x$ for strings intended to denote initial segments. Then $X\restriction x$ denotes a string of length x and, for $y < x$, $X(y)$ or $(X\restriction x)(y)$ will denote the $(y+1)$th bit of $X\restriction x$.

For the following it will be important to note the difference in the length of an initial segment $A\restriction x$ and the length of its bound x, namely

$$(1.1) \quad 2^{|x|} - 1 \leq |A\restriction x| \leq 2^{|x|+1} - 1,$$

whence, for any number $k \geq 1$, $|A\restriction x|^k \approx 2^{k \cdot |x|}$. (These inequalities will be responsible for the fact that the $\mathbf{DTIME}(t(n))$-measure will be a measure for $\mathbf{DTIME}(t(2^n))$.)

Our complexity theoretic notation is mainly standard. For the fundamental complexity theoretic concepts used but not explained in this paper we refer the reader to [HU79] and [BDG95]. In particular we assume the reader to be familiar with the basic concepts and results of structural complexity theory. We will consider the deterministic time classes

$$\begin{aligned}\mathbf{P} &= \mathbf{DTIME}(poly) = \textstyle\bigcup_{k\geq 1}\mathbf{DTIME}\left(n^k\right),\\ \mathbf{E} &= \mathbf{DTIME}\left(2^{lin}\right) = \textstyle\bigcup_{k\geq 1}\mathbf{DTIME}\left(2^{kn}\right), and\\ \mathbf{E}_2 &= \mathbf{DTIME}\left(2^{poly}\right) = \textstyle\bigcup_{k\geq 1}\mathbf{DTIME}\left(2^{n^k}\right).\end{aligned}$$

Moreover, in our notation we will not distinguish between complexity classes for sets and functions. For any reducibility r (like 1 (= one-one), m (= many-one), $btt(k)$ (= k-query truth-table), btt (= bounded truth-table), tt (= truth-table) and T (= Turing)), we let $\mathbf{P}_r^{\leq}(A)$ or shortly $\mathbf{P}_r(A)$ be the class $\{B : B \leq_r^p A\}$ of sets which can be reduced to A by an r-reduction in polynomial time. (For the definition of these reducibilities, see [LLS75].) Note that $\mathbf{P}_T(A) = \mathbf{P}(A)$. Also note that $\mathbf{E}_2$ is the downward closure of $\mathbf{E}$ under any of the polynomial reducibilities, whence a set A is $\mathbf{P}$-r-complete for $\mathbf{E}$ iff $A \in \mathbf{E}$ and A is $\mathbf{P}$-r-complete for $\mathbf{E}_2$.

Throughout this article, we assume that all time bounds $t(n)$ are nondecreasing, time-constructible functions satisfying $t(n) \geq n$ for all n and $\mathbf{DTIME}(t(n)) = \mathbf{DTIME}(O(t(n)))$.

2 Measure and Martingales

In the first part of this section we introduce the fragment of the Lebesgue measure concept needed in the following. Then we give a characterization of the measure-0 classes due to Ville [Vi39] which is based on certain betting strategies, called martingales. By giving some examples, we will illustrate this concept, which will be the basis for the randomness concepts discussed in this paper.

For a more complete treatment of Lebesgue measure we refer the reader to Halmos [Ha50] or Oxtoby [Ox80].

The Lebesgue measure μ on the Cantor space is the product measure induced by the equiprobable measure μ_0 on $\{0, 1\}$ which assigns to both 0 and 1 the probability $\frac{1}{2}$. A model for this measure is the (independent) tossing of a fair coin. In particular, for the basic open class $\mathbf{B}_x = \{A : x \sqsubseteq A\}$, $\mu(\mathbf{B}_x) = 2^{-|x|}$ is the probability that a randomly chosen sequence of coin tosses begins with the $|x|$ events $x(0), \ldots, x(|x| - 1)$. For our goals it will not be necessary to define the Lebesgue measure μ completely but it suffices to define the "small" and "large" classes with respect to this measure, namely the measure-0 and measure-1 classes.

Definition 2.1. An infinite sequence $\mathcal{B} = \{\mathbf{B}_{x_n} : n \geq 0\}$ of basic open sets is an *α-cover* of a class $\mathbf{C}$ if

(i) $\mathbf{C} \subseteq \bigcup_{n\geq 0} \mathbf{B}_{x_n}$ and (ii) $\sum_{n\geq 0} \mu(\mathbf{B}_{x_n}) \leq \alpha$.

Example 2.2. For any set A, the sequence $\mathcal{B}_A = \{\mathbf{B}_{A\upharpoonright n} : n > k\}$ is a 2^{-k}-cover of $\{A\}$.

Definition 2.3. A class $\mathbf{C}$ has *measure* 0 ($\mu(\mathbf{C}) = 0$) if, for all $n \geq 0$, there is a 2^{-n}-cover of $\mathbf{C}$. A class $\mathbf{C}$ has *measure* 1 ($\mu(\mathbf{C}) = 1$) if the complement $\overline{\mathbf{C}}$ of $\mathbf{C}$ has measure 0.

We write $\mu(\mathbf{C}) \neq i$ ($i = 0, 1$) to abbreviate that $\mathbf{C}$ does not have measure i. Note that, for any cover $\mathcal{B} = \{\mathbf{B}_{x_n} : n \geq 0\}$ of the power class of $\{0,1\}^*$, $\sum_{n\geq 0} \mu(\mathbf{B}_{x_n}) \geq 1$. Hence, there is no class $\mathbf{C}$ such that $\mu(\mathbf{C}) = 0$ and $\mu(\mathbf{C}) = 1$. This consistency property can be also expressed by

Proposition 2.4. For any measure-0 class $\mathbf{C}$, $\mu(\mathbf{C}) \neq 1$.

In the next lemma we summarize the fundamental closure properties of the family of measure-0 classes.

Lemma 2.5.

(i) For every set A, $\mu(\{A\}) = 0$.

(ii) If $\mathbf{C} \subseteq \mathbf{D}$ and $\mu(\mathbf{D}) = 0$ then $\mu(\mathbf{C}) = 0$.

(iii) Let $\mathbf{C} = \bigcup_{n\geq 0} \mathbf{C}_n$ be the union of the measure-0 classes $\mathbf{C}_n$, $n \geq 0$. Then $\mu(\mathbf{C}) = 0$.

Proof. (i) follows from Example 2.2 while (ii) is immediate by definition. For a proof of (iii), fix $m \geq 0$. To show that $\mathbf{C}$ possesses a 2^{-m}-cover, by assumption choose $2^{-(m+k+1)}$-covers $\mathcal{B}_k = \{\mathbf{B}_{x_{k,n}} : n \geq 0\}$ of $\mathbf{C}_k$. Then, for $\hat{x}_{\langle k,n\rangle} = x_{k,n}$, $\mathcal{B} = \{\mathbf{B}_{\hat{x}_e} : e \geq 0\}$ is a 2^{-m}-cover of $\mathbf{C}$. □

Corollary 2.6. For any countable class $\mathbf{C}$, $\mu(\mathbf{C}) = 0$. □

(Examples of uncountable measure-0 classes can be found below.) By duality, we obtain the following closure properties of measure-1 classes.

Corollary 2.7.

(i) For any class $\mathbf{C}$ with countable complement, $\mu(\mathbf{C}) = 1$.

(ii) If $\mathbf{C} \subseteq \mathbf{D}$ and $\mu(\mathbf{C}) = 1$ then $\mu(\mathbf{D}) = 1$.

(iii) Let $\mathbf{C} = \bigcap_{n\geq 0} \mathbf{C}_n$ be the intersection of the measure-1 classes $\mathbf{C}_n$, $n \geq 0$. Then $\mu(\mathbf{C}) = 1$. □

We next give a characterization of the measure-0 classes in terms of certain betting strategies, called martingales.

Definition 2.8.

(a) A *martingale* is a function $d : \{0,1\}^* \to [0, \infty)$ such that $d(\lambda) > 0$ and, for every $x \in \{0,1\}^*$, the following equality holds:

$$(2.1) \qquad \frac{d(x0)+d(x1)}{2} = d(x)$$

$d(\lambda)$ is called the *norm* of d. d is *normed* if $d(\lambda) = 1$.

(b) A martingale d *succeeds* on a set A if

$$\limsup_{n \geq 0} d(A \upharpoonright n) = \infty.$$

$S^\infty[d]$ denotes the class of sets on which the martingale d succeeds.

A martingale d *succeeds* on a class $\mathbf{C}$ if $\mathbf{C} \subseteq S^\infty[d]$.

The definitions of martingale and success can be interpreted in relation with a fair betting game on the successive bits of a hidden sequence in $\{0,1\}^\infty$. The gambler starts with capital $d(\lambda)$ and in every round, depending on the previous outcomes x, he bets a certain fraction $\alpha \cdot d(x)$ ($\alpha \in [0,1]$) of his current capital $d(x)$ on the event 0, and he bets the remaining capital $(1-\alpha)d(x)$ on the event 1. The amount put on the correct guess of the event will be doubled while the amount put on the wrong guess will be lost. So for the outcomes 0 and 1 his capital in the next round will be $d(x0) = 2\alpha d(x)$ and $d(x1) = 2(1-\alpha)d(x)$, respectively. (This corresponds to the martingale property (2.1).)

We call the function, which determines the fraction of the capital put onto the 0 event in every round, the strategy underlying the martingale d.

Definition 2.9. A *(betting) strategy* s is a function $s : \{0,1\}^* \to [0,1]$. The *strategy* s_d *underlying the martingale* d is the function

$$(2.2) \qquad s_d(x) = \begin{cases} \frac{d(x0)}{2d(x)} & \text{if } d(x) \neq 0 \\ 0 & \text{otherwise.} \end{cases}$$

Conversely, for every strategy s and every real $\alpha > 0$, the *martingale* $d[s,\alpha]$ with start capital α *induced* by s is defined by $d(\lambda) = \alpha$ and, for any string $X \upharpoonright (n+1)$ where $n \geq 0$,

$$(2.3) \qquad d(X \upharpoonright (n+1)) = \begin{cases} 2 \cdot s(X \upharpoonright n) \cdot d(X \upharpoonright n) & \text{if } X(n) = 0 \\ 2 \cdot (1 - s(X \upharpoonright n)) \cdot d(X \upharpoonright n) & \text{if } X(n) = 1. \end{cases}$$

We write $d[s]$ in place of $d[s,1]$ for the normed martingale induced by the strategy s. Note that the strategy s_d underlying a martingale d is uniquely determined by d, and the normed martingale $d[s]$ induced by a strategy s is uniquely determined by s. Moreover, $d[s] = d[s']$ if and only if the strategies s and s' differ only on strings x with $d[s](x) = d[s'](x) = 0$.

Example 2.10.

1. For any set A, consider the strategy s defined by

   $$s(X \upharpoonright n) = 1 - A(n).$$

   (I.e., given any string $X \upharpoonright n$, the strategy s bets the whole capital on the guess $i = A(n)$ for the next bit i.) Then, for the normed martingale $d[s]$ induced by s, $S^\infty[d[s]] = \{A\}$. Namely, for every n, $d[s](A \upharpoonright (n+1)) = 2 \cdot d[s](A \upharpoonright n)$, whence $\lim_{n \geq 0} d[s](A \upharpoonright n) = \infty$, whereas for $B \neq A$, say $B(n_0) \neq A(n_0)$, $d[s](B \upharpoonright n) = 0$ for all $n > n_0$.

2. For any infinite set A, let s be the strategy defined by

$$s(X\restriction n) = \begin{cases} 0 & \text{if } A(n) = 1 \\ \frac{1}{2} & \text{otherwise.} \end{cases}$$

Then $d[s]$ succeeds on the supersets of A: $S^\infty[d[s]] = \{B : A \subseteq B\}$.

3. Recall that a set A is sparse if there is a polynomial p such that $\| A^{\leq n} \| \leq p(n)$ for all n. The strategy s with $s(X\restriction x) = \frac{3}{4}$, which always gives a $3:1$ preference to the outcome 0, succeeds on all sparse sets. Namely, for A and p as above and for $e(n) = \| (\Sigma^*)^{\leq n} \| = 2^{n+1} - 1$,

$$d[s](A\restriction 0^{n+1}) = \left(\frac{3}{2}\right)^{\|(\Sigma^* - A)^{\leq n}\|} \cdot \left(\frac{1}{2}\right)^{\|A^{\leq n}\|} = \frac{3^{e(n)-p(n)}}{2^{e(n)}}$$

Hence $\lim_{n\to\infty} d[s](A\restriction 0^n) = \infty$.

4. A set A has *exponential gaps* if $A^{=n} = \emptyset$ for infinitely many n. A martingale that succeeds on all sets with exponential gaps can be defined as follows. For any string $X\restriction x$ such that $X(y) = 0$ for all $y < x$ with $|y| = |x|$, the strategy s gives a $3:1$ preference to the outcome 0 and it is unbiased otherwise (i.e. $s((X\restriction 0^n)0^m) = \frac{3}{4}$ for n, m with $m \leq 2^n$ and $s(X\restriction x) = \frac{1}{2}$ otherwise). Then, for any set A and any number n, $d[s](A\restriction 0^{n+1}) \geq \frac{1}{2} d[s](A\restriction 0^n)$ whence $d[s](A\restriction 0^n) \geq (\frac{1}{2})^n$. Moreover, if $A^{=n} = \emptyset$ then $d[s](A\restriction 0^{n+1}) = (\frac{3}{2})^{2^n} \cdot d[s](A\restriction 0^n)$, whence $d[s](A\restriction 0^{n+1}) \geq (\frac{3}{2})^{2^n} \cdot (\frac{1}{2})^n \geq (\frac{3}{2})^{2n} \cdot (\frac{1}{2})^n = (\frac{9}{8})^n$. Since $\lim_{n\to\infty} (\frac{9}{8})^n = \infty$ this implies the claim.

To show that a class $\mathbf{C}$ has measure 0 iff there is a martingale d which succeeds on $\mathbf{C}$, we first describe covers in terms of martingales. We say that a martingale d *covers* a set X if

$$\text{(2.4)} \quad \liminf_{n\geq 0} d(X\restriction n) \geq 1$$

and d *covers* a class $\mathbf{C}$ if d covers every set $X \in \mathbf{C}$.

Lemma 2.11. Let $\mathcal{B} = \{\mathbf{B}_{x_n} : n \geq 0\}$ be an α-cover of $\mathbf{C}$. There is a martingale d such that $d(\lambda) \leq \alpha$ and d covers $\mathbf{C}$.

Proof. For any string x, the martingale d_x defined by

$$d_x(y) = \begin{cases} 2^{|y|-|x|} & \text{if } y \sqsubseteq x \\ 1 & \text{if } y \sqsupseteq x \\ 0 & \text{otherwise} \end{cases}$$

covers $\mathbf{B}_x$ and $d_x(\lambda) = 2^{-|x|} = \mu(\mathbf{B}_x)$. Since $\mathcal{B}$ is an α-cover of $\mathbf{C}$, it follows that d defined by

$$d(y) = \Sigma_{n\geq 0}\ d_{x_n}(y)$$

is a martingale with $d(\lambda) \leq \alpha$ and d covers $\mathbf{C}$. □

Lemma 2.12. Let $\mathbf{C}$ be a measure-0 class. There is a martingale d which succeeds on $\mathbf{C}$.

Proof. By Definition 2.3 and Lemma 2.11, for each $n \geq 0$ there is a martingale d_n such that $d_n(\lambda) \leq 2^{-n}$ and d_n covers $\mathbf{C}$. So, for d defined by $d(y) = \Sigma_{n \geq 0}\, d_n(y)$, d is a martingale which succeeds on $\mathbf{C}$. □

Lemma 2.13. Let d be a martingale and let $\mathbf{C} = \{X : \exists n(d(X\restriction n) \geq 1)\}$. There is a $d(\lambda)$-cover of $\mathbf{C}$.

Proof. We only sketch the proof. Let C_d be the set of minimal strings covered by d, i.e., $C_d = \{x : d(x) \geq 1 \text{ and } \forall y \sqsubset x(d(y) < 1)\}$. Then $\mathbf{C} = \bigcup_{x \in C_d} \mathbf{B}_x$. Moreover, C_d is prefix free, i.e., for $x, y \in C_d$, $x \sqsubseteq y$ implies that $x = y$. By the latter property of C_d it easily follows from the martingale property (2.1) that

$$\Sigma_{x \in C_d}\, d(x) \cdot 2^{-|x|} \leq d(\lambda).$$

Since $d(x) \geq 1$ for $x \in C_d$ it follows that

$$\Sigma_{x \in C_d}\, \mu(\mathbf{B}_x) = \Sigma_{x \in C_d}\, 2^{-|x|} \leq d(\lambda),$$

whence $\mathcal{B} = \{\mathbf{B}_x : x \in C_d\}$ is a $d(\lambda)$-cover of $\mathbf{C}$. □

Lemma 2.14. Let $\mathbf{C}$ be a class and let d be a martingale which succeeds on $\mathbf{C}$. Then $\mu(\mathbf{C}) = 0$.

Proof. Given $m \geq 0$, it suffices to show that there is a 2^{-m}-cover of $\mathbf{C}$. For the constant $c = 2^{-m} \cdot d(\lambda)^{-1}$, let $d'(y) = c \cdot d(y)$. Then $d'(\lambda) = 2^{-m}$, d' is a martingale and $\mathbf{C} \subseteq \{X : \exists n(d'(X\restriction n) \geq 1)\}$. So the required cover exists by Lemma 2.13. □

Theorem 2.15. Let $\mathbf{C}$ be a class. Then $\mu(\mathbf{C}) = 0$ iff there is a martingale which succeeds on $\mathbf{C}$.

Proof. By Lemmas 2.12 and 2.14. □

3 Resource-Bounded Martingales and Randomness

We next introduce Schnorr's resource-bounded randomness concept ([Sch71a], [Sch71b]) and Lutz's resource-bounded measure ([Lu92]). Both concepts, which are closely related to each other, are based on Ville's martingale characterization of the measure-0 classes.

Note that for any countable sequence $D = \{d_n : n \geq 0\}$ of martingales, the class $\mathbf{S} = \bigcup_{n \geq 0} S^\infty[d_n]$ has measure 0 (by Theorem 2.15 and Lemma 2.5). So, for every set X in the measure-1 class $\overline{\mathbf{S}}$, no martingale in D succeeds on X. Hence we may call such a set X *random* for D. Schnorr proposed that a set X should be called *recursively random* if no recursive martingale succeeds on X, i.e. if X is random for the class D of recursive martingales. Moreover, by additionally imposing resource bounds, Schnorr introduced resource-bounded randomness concepts. Later Lutz extended these concepts by considering notions of resource-bounded measure. Here we introduce these concepts for the deterministic time complexity classes. By admitting only rational valued strategies and martingales, the time complexity of these functions can be defined in the usual way. To be more precise, we represent nonnegative rational numbers by triples $\langle p, q, r\rangle$ where p, q, r are (binary strings representing) nonnegative integers and $\langle p, q, r\rangle$ denotes the rational number $\frac{p}{q} \cdot 2^{-r}$. With this codification the sum of two rational numbers of length n can be done in time $O(n)$, whereas multiplication and division can be both done in time $O(n(log\, n)^2)$, using the best known integer multiplication algorithms.

Definition 3.1. Let $t : N \to N$ be a nondecreasing recursive function.

1. A $t(n)$-*strategy* is a function $s : \{0,1\}^* \to [0,1] \cap \mathrm{Q}$ such that $s \in \mathbf{DTIME}(t(n))$.
2. A $t(n)$-*martingale* is a martingale $d = d[s, \alpha]$ induced by a $t(n)$-strategy s and a rational number $\alpha > 0$.

Schnorr [Sch71b] and Ambos-Spies, Terwijn and Zheng [ATZ94] call a martingale d a $t(n)$-martingale if $d \in \mathbf{DTIME}(t(n))$, while our definition follows [AMWZ96] (It is chosen in order to simplify the comparison of $t(n)$-randomness with $t(n)$-genericity and $t(n)$-stochasticity in the next two sections). Lutz [Lu92] introduced still another notion of $t(n)$-martingale based on $\mathbf{DTIME}(t(n))$-approximations of real valued martingales. As shown in part by the following proposition, all these concepts are more or less equivalent though the correspondence does not preserve the exact time bounds.

Proposition 3.2. 1. For any $t(n)$-martingale d, $d \in \mathbf{DTIME}(n \cdot t(n) \cdot log(t(n))^2)$.
2. Any martingale $d \in \mathbf{DTIME}(t(n))$ is a $(t(n) \cdot log(t(n))^2)$-martingale.

Proof. By the above mentioned time bounds on multiplication and division of rationals, this follows from (2.3) and (2.2), respectively. □

Example 3.3. The complexity of the martingales in Example 2.10 is as follows:

1. and 2. If $A \in \mathbf{DTIME}(t(2^n - 1))$, then $d[s]$ is a $t(n)$-martingale. Note that for any string x, $2^{|x|} - 1 \leq |X\restriction x| \leq 2^{|x|+1} - 1$. So $A(x)$, hence $s(X\restriction x)$, can be computed in $t(2^{|x|} - 1) \leq t(|X\restriction x|)$ steps.
3. and 4. $d[s]$ is an $O(1)$-martingale and an n^2-martingale, respectively.

Definition 3.4 (Schnorr [Sch71b], Lutz [Lu92]).

1. A class $\mathbf{C}$ has $t(n)$-*measure* 0 ($\mu_t(\mathbf{C}) = 0$) if there is a $t(n)$-martingale d that succeeds on $\mathbf{C}$.
2. A class $\mathbf{C}$ has $t(n)$-*measure* 1 ($\mu_t(\mathbf{C}) = 1$) if $\overline{\mathbf{C}}$ has $t(n)$-measure 0.
3. A set A is $t(n)$-*random* if no $t(n)$-martingale succeeds on it.
   Let $\mathbf{RAND}(t(n))$ denote the class of $t(n)$-random sets.

Note that the $t(n)$-measure μ_t is consistent with the classical measure μ, but due to the presence of resource-bounds, certain classes which in the classical sense are small (large) cannot be classified here. Examples are the singletons $\{A\}$, where A is $t(n)$-random.

Proposition 3.5. Let t, t' be recursive functions such that $t(n) \leq t'(n)$ a.e.

(i) For any class $\mathbf{C}$ and $i \in \{0,1\}$, $\mu_t(\mathbf{C}) = i \Rightarrow \mu_{t'}(\mathbf{C}) = i \Rightarrow \mu(\mathbf{C}) = i$.

(ii) $\mathbf{RAND}(t(n)) \supseteq \mathbf{RAND}(t'(n))$. □

Proposition 3.6. For any set A, the following are equivalent.

(i) A is $t(n)$-random.

(ii) $\mu_t(\{A\}) \neq 0$.

(iii) For every $t(n)$-measure-1 class $\mathbf{C}$, $A \in \mathbf{C}$. □

Another simple but useful observation is that the closure of the deterministic time classes under complement caries over to $t(n)$-measure and $t(n)$-randomness as follows.

Proposition 3.7. Let $\mathbf{C}$ be a class with $\mu_t(\mathbf{C}) = i$ $(i \in \{0,1\})$. Then, for co-$\mathbf{C} = \{\overline{A} : A \in \mathbf{C}\}$, $\mu_t(\text{co-}\mathbf{C}) = i$ too. In particular, for any $t(n)$-random set A, $\overline{A}$ is $t(n)$-random too.

Proof. This follows from the fact that a $t(n)$-martingale d succeeds on a set A iff the $t(n)$-martingale $\overline{d}$ succeeds on $\overline{A}$, where: $\overline{d}(X{\restriction}n) = d(\overline{X}{\restriction}n)$ for all strings $X{\restriction}n$, where $\overline{X}{\restriction}n$ is defined by $\overline{X}(m) = 1 - X(m)$ for $m < n$. □

By Proposition 3.6, Lemma 2.5 does not hold for the resource-bounded-measure, since the first part fails for any $t(n)$-random set A. The second part obviously holds in this setting too.

Proposition 3.8. If $\mathbf{C} \subseteq \mathbf{D}$ and $\mu_t(\mathbf{D}) = 0$ then $\mu_t(\mathbf{C}) = 0$. □

The closure under countable unions, however, fails too. The countable union of classes of $t(n)$-measure 0 has $t'(n)$-measure 0, however, if $t'(n)$ is chosen big enough so that in particular $\mathbf{DTIME}(t'(n))$ contains a universal function for $\mathbf{DTIME}(t(n))$. This observation also yields a $t(n)$-random set of almost minimum complexity. Similar union lemmas can be found in [Sch71b], [Lu92], [Ma94b], [ATZ94].

Lemma 3.9. Let $t'(n) \geq n^3 \cdot t(n) \cdot \log(t(n))^4$ a.e.. There is a $t'(n)$-martingale d which succeeds on all $t(n)$-measure-0 classes, i.e. $\mu_{t'}(\bigcup\{\mathbf{C} : \mu_t(\mathbf{C}) = 0\}) = 0$. Moreover, there is a $t(n)$-random set $A \in \mathbf{DTIME}(2^n \cdot t'(2^{n+1}))$.

Proof. Let $\{s_k : k \geq 0\}$ be a recursive enumeration of the $t(n)$-strategies. By the standard construction of a universal machine, we may assume that, for $|x| = n > k$, $s_k(x)$ can be uniformly computed in $O(t(n) \cdot log(t(n)))$ steps. For each k define a martingale d_k by $d_k(X{\restriction}n) = 2^{-k}$ for $n \leq k$ and by (2.3) with d_k in place of d otherwise and combine the martingales d_k to a "universal" martingale d by letting

$$d(X{\restriction}n) = \sum_{k=0}^{\infty} d_k(X{\restriction}n) = \sum_{k=0}^{n} d_k(X{\restriction}n) + \sum_{k=n+1}^{\infty} 2^{-k}.$$

Note that $S^\infty[d[s_k]] = S^\infty[d_k] \subseteq S^\infty[d]$ whence d succeeds on all $t(n)$-measure-0 classes. So it suffices to show that d is a $t'(n)$-martingale. By (2.3), d_k can be inductively defined from s_k in $O(n \cdot t(n) \cdot log(t(n))^3)$ steps whence $d \in \mathbf{DTIME}(n^2 \cdot t(n) \cdot log(t(n))^3)$. So, by Proposition 3.2.2, d is an $(n^3 \cdot t(n) \cdot log(t(n))^4)$-martingale. For a proof of the second part of the lemma, inductively define A by letting $A(n) = 0$ if $d((A\restriction n)0) \leq d((A\restriction n)1)$ and $A(n) = 1$ otherwise. Then, by (2.1), $d(A\restriction n) \leq d(\lambda)$ for all n whence d does not succeed on A. So A is $t(n)$-random. Moreover, by $d \in \mathbf{DTIME}(t'(n))$ and by (1.1), $A \in \mathbf{DTIME}(2^{n+1} \cdot t'(2^{n+1}))$. □

By combining Proposition 3.6 and Lemma 3.9, we obtain the following relations between resource-bounded measure and randomness.

Corollary 3.10. Let t, t' be recursive functions such that $t'(n) \geq n^3 \cdot t(n) \cdot \log(t(n))^4$ and let $\mathbf{C}$ be any class.

(i) $\mu_t(\mathbf{C}) = \mathbf{0} \Rightarrow \mathbf{RAND}(t(n)) \cap \mathbf{C} = \emptyset \ \Rightarrow \mu_{t'}(\mathbf{C}) = 0$

(ii) $\mu_t(\mathbf{C}) = 1 \ \Rightarrow \mathbf{RAND}(t(n)) \subseteq \mathbf{C} \ \Rightarrow \mu_{t'}(\mathbf{C}) = 1$

Proof. By symmetry, it suffices to prove (i). The first implication is immediate by definition. For the second implication note that $\mathbf{RAND}(t(n)) \cap \mathbf{C} = \emptyset$ implies that $\mu_t(\{A\}) = 0$ for all $A \in \mathbf{C}$. So the claim follows from Lemma 3.9 □

Corollary 3.11. For any function t' such that $t'(n) \geq n^3 \cdot t(n) \cdot \log(t(n))^4$, $\mu_{t'}(\mathbf{RAND}(t(n))) = 1$. □

These close relations between measure and randomness allow the choice of which concept to work with. Due to the lack of closure properties of the $t(n)$-measure, the randomness approach sometimes is somewhat simpler, whence we will stress this concept here.

From the above examples we obtain the following properties of $t(n)$-random sets.

Lemma 3.12. Let A be $t(n)$-random where $t(n) \geq n^2$. Then A is not sparse and A does not have exponential gaps.

Proof. This follows from the third and fourth parts of Examples 2.10 and 3.3.

□

For strengthenings of Lemma 3.12 see Corollaries 5.7 and 8.5. Recall that a set A is $\mathbf{C}$-*immune* if A does not contain any infinite set $B \in \mathbf{C}$ as a subset, and A is $\mathbf{C}$-*bi-immune* if A and $\overline{A}$ are $\mathbf{C}$-immune. (In the following we will write p-(bi-)immune instead of $\mathbf{P}$-(bi-)immune.)

Lemma 3.13. Let A be $t(n)$-random. Then $A \notin \mathbf{DTIME}(t(2^n - 1))$. In fact, A is $\mathbf{DTIME}(t(2^n - 1))$-bi-immune.

Proof. By the first parts of Examples 2.10 and 3.3, no $t(n)$-random set can be in $\mathbf{DTIME}(t(2^n-1))$. Similarly, by the second parts of these examples, any $t(n)$-random set is $\mathbf{DTIME}(t(2^n - 1))$-immune, hence, by Proposition 3.7, $\mathbf{DTIME}(t(2^n - 1))$-bi-immune. □

Bi-immunity is a fundamental property in structural complexity theory. Note that a set A is $\mathbf{DTIME}(t(n))$-bi-immune iff, for every infinite set $B \in \mathbf{DTIME}(t(n))$,

$A \cap B \notin \mathbf{DTIME}(t(n))$, i.e., iff $t(n)$ is an almost everywhere lower time bound for A (see e.g. [GHS87] for more details). Many natural problems have easy parts, so that the second part of Lemma 3.13 is a quite powerful tool for showing that certain classes have $t(n)$-measure 0. For later use we give the characterization of bi-immunity in terms of complexity cores due to Balcazar and Schöning [BaS85]. Lynch [Ly75] defined that a set B is a $\mathbf{DTIME}(t(n))$-*complexity core* of a set A if, for every Turing machine M which is consistent with A (i.e. whenever $M(x)\downarrow$ then $M(x) = A(x)$), there are only finitely many $x \in B$ such that $M(x)$ is defined in less than $t(|x|)$ steps. (And B is a *p-complexity core* of A if B is a $\mathbf{DTIME}(n^k)$-complexity core of A for all $k \geq 1$.) Note that this is equivalent to saying that, for every infinite set $C \in \mathbf{DTIME}(t(n))$ with $C \subseteq B$, $A \cap C \neq \emptyset$ and $\overline{A} \cap C \neq \emptyset$. So A is $\mathbf{DTIME}(t(n))$-bi-immune iff $\{0,1\}^*$ is a $\mathbf{DTIME}(t(n))$-complexity core of A.

Corollary 3.14. Let A be $t(n)$-random. Then $\{0,1\}^*$ is a $\mathbf{DTIME}(t(2^n-1))$-complexity core of A. □

4 Genericity versus Randomness

In Section 3 we have seen that random sets have certain properties which are commonly ensured by diagonalization. So, intuitively speaking, a random set has built in certain diagonalizations. For analyzing which types of diagonalizations are subsumed by randomness, it is instructive to compare randomness with genericity. As the random sets are the typical sets with respect to measure, the generic sets are typical with respect to Baire category. Baire category is an alternative topological classification scheme for the Cantor space, in which the meager (comeager) classes correspond to the measure-0 (measure-1) classes. In contrast to measure, however, category is directly related to diagonalization, and various resource-bounded category concepts capturing the most fundamental types of diagonalization arguments in structural complexity have been recently introduced (see [Am96]).

Here we will not consider all of these concepts but we will restrict ourselves to the general $t(n)$-genericity concept of Ambos-Spies [Am96] and a special case of it, $t(n)$-genericity, due to Ambos-Spies, Fleischhack and Huwig [AFH88].

Corresponding to the classical case, where we can find comeager measure-0 classes, general $t(n)$-genericity and $t(n)$-randomness are incompatible too. In contrast, however, all $t(n)$-random sets are $t(n)$-generic, so that the diagonalizations formalized by this genericity notion are captured by $t(n)$-randomness.

We use this observation to establish further properties of the $t(n)$-random sets. Finally we discuss two aspects relative to which $t(n)$-randomness strengthens $t(n)$-genericity.

A *classical extension function* is a function $f : \{0,1\}^* \to \{0,1\}^*$. A set A *meets* the extension function f at n if $(A\restriction n)\, f(A\restriction n) \sqsubseteq A$. Intuitively, if we inductively define the set A by determining longer and longer initial segments of its characteristic sequence and if A meets f at n, then the finite initial segment $A\restriction n$ is extended as required by f. Extension functions correspond to the requirements in a diagonalization construction. E.g. if we want to diagonalize over an infinite countable class $\mathbf{C}$, then any set $C \in \mathbf{C}$ is associated with the extension function $f_c(X\restriction n) = 1 - C(n)$. Then, for any set A, $A \notin \mathbf{C}$

iff A meets all the extension functions associated with the members of **C**.

We say that a set A *avoids* the extension function f if there is no n such that A meets f at n. A class **C** is *nowhere dense* if there is an extension function avoided by all members of **C**. A countable union of nowhere dense classes is called *meager*, the complement of a meager class is *comeager*. Meager and comeager classes may be viewed as small and large, respectively, and if we replace measure-0 and measure-1 by meager and comeager, respectively, then the fundamental properties of the Lebesgue measure stated in Lemma 2.5 and Corollary 2.7 remain valid. Here we will not pursue these Baire category concepts in detail but we will only consider the typical objects of it. (For a more complete account of classical Baire category, we refer to Oxtoby [Ox80].)

For a countable class $F = \{f_n : n \geq 0\}$ of extension functions, there will be a comeager (hence nonempty) class of sets meeting all members of F. Such sets are called *generic for F*. Resource-bounded genericity concepts can be obtained by considering the class F of extension functions computable within a certain time bound. This approach has been taken by Lutz in [Lu90]. The genericity concept obtained in this way is rather weak, however, whence stronger notions have been introduced. The concept we study here is obtained by considering more flexible extension functions. The first amendment (due to Fenner [Fe91]) is to consider functions, which do not completely specify the extension. The second amendment (due to Ambos-Spies, Fleischhack, and Huwig [AFH84], [AFH87], [AFH88]) is to admit extension functions which are not total but defined infinitely often along the constructed sequence.

Definition 4.1.

(i) An *extension function* is a partial function $f : \{0,1\}^* \to (\{0,1\}^* \times \{0,1\})^*$, such that, for any string $X\restriction x$ on which f is defined,

$$f(X\restriction x) = (x_0, i_0), \ldots, (x_m, i_m) \qquad (4.1)$$

where $m \geq 0$, $x_0, \ldots x_m$ are strings such that $x \leq x_0 < x_1 < \ldots < x_m$ and $i_0, \ldots, i_m \in \{0,1\}$. A *$t(n)$-extension function* is an extension function $f \in$ **DTIME**$(t(n))$.

(ii) An extension function f is *dense along* a set A if $f(A\restriction x)$ is defined for infinitely many strings x.

(iii) A set A *meets* an extension function f *at* a string x if $f(A\restriction x)$ is defined, say $f(A\restriction x) = (x_0, i_0), \ldots, (x_m, i_m)$, and $A(x_l) = i_l$ for $0 \leq l \leq m$. *A meets f* if A meets f at some x, and A *avoids* f otherwise.

(iv) A is *general $t(n)$-generic* if A meets all $t(n)$-extension functions which are dense along A.

Classical Baire category can be defined in terms of this extension function concept too: A class **C** is nowhere dense if there is an extension function f which is dense along all members of **C** and avoided by all of them. So, for any recursive function $t(n)$, the class of the general $t(n)$-generic sets is comeager, hence nonempty.

We next give some examples to illustrate the above concepts. These should be compared with Example 2.10.

Examples 4.2.

1. For any set A, let f be the extension function defined by

$$f(X\upharpoonright x) = (x, 1 - A(x)).$$

Then f is dense along all sets and a set B meets f iff $B \neq A$. Moreover, for $A \in \mathbf{DTIME}(t(2^n - 1))$, f is a $t(n)$-extension function.

2. For any infinite set A, let f be the following extension function. For $x \in A$, $f(X\upharpoonright x) = (x, 0)$, and $f(X\upharpoonright x)$ is undefined otherwise. Then, by infinity of A, f is dense along all sets and a set B meets f iff $A \not\subseteq B$. Again, for $A \in \mathbf{DTIME}(t(2^n - 1))$, f is a $t(n)$-extension function.

3. For $m \geq 0$ define the n^2-extension function f_m by

$$f_m(X\upharpoonright 0^n) = (0^n, 0), \ldots, (1^n, 0)$$

if $m \leq n$ and $f_m(X\upharpoonright x)\uparrow$ otherwise. (Since there are 2^n strings x of length n and, for each such x, $|(x,0)| = O(n)$, $f_m(X\upharpoonright 0^n)$ can be computed in $O(n \cdot 2^n)$ steps, whence f_m is an n^2-martingale by (1.1).) Then f_m is dense along all sets and a set A meets f_m iff $A^{=n} = \emptyset$ for some $n \geq m$. So A has exponential gaps iff A meets f_m for all m.

By the first two examples, for any general $t(n)$-generic set G, $G \notin \mathbf{DTIME}$ $(t(2^n - 1))$, in fact G is $\mathbf{DTIME}(t(2^n - 1))$-bi-immune. So general $t(n)$-generic and $t(n)$-random sets share some interesting properties (cf. Lemma 3.13). By the third example and by Lemma 3.12, however, $t(n)$-randomness and general $t(n)$-genericity are incompatible.

Theorem 4.3 (Ambos-Spies [Am96]). For $t(n) \geq n^2$ there is no set which is general $t(n)$-generic and $t(n)$-random. Namely every general n^2-generic set has exponential gaps whereas no n^2-random set has exponential gaps. □

Theorem 4.3 is based on the observation that, in general, if a set A meets an extension function at some string x, this does not only determine the value of A on some single strings but on intervals of growing length (in $|x|$). By admitting only short extensions, in particular extensions which only determine the value of A on the next string, we obtain a genericity concept compatible with randomness.

Definition 4.4.

(i) An extension function f is *simple* if $f(X\upharpoonright x) \in \{(x,0),(x,1)\}$ whenever $f(X\upharpoonright x)$ is defined.

(ii) A set A is $t(n)$-*generic* if A meets every simple $t(n)$-extension function which is dense along A.

Note that the extension functions in Examples 4.2.1 and 4.2.2 are simple. To simplify notation, for a simple extension function f we write $f(X\upharpoonright x) = i$ instead of $f(X\upharpoonright x) = (x, i)$. Definition 4.4 is due to Ambos-Spies et al. [AFH88], though there $t(n)$-genericity is defined in terms of conditions, not extension functions. It can be easily shown, however, that $t(n)$-genericity as defined there coincides with $t(n+1)$-genericity as defined above (see [Am96] or [AMWZ96]).

Obviously every general $t(n)$-generic set is $t(n)$-generic but the converse in general fails: In contrast to Theorem 4.3, $t(n)$-genericity is compatible with $t(n)$-randomness.

Theorem 4.5 ([ANT94],[ATZ94]). Every $t(n)$-random set is $t(n)$-generic.

Proof. Let A be $t(n)$-random and let f be a simple $t(n)$-extension function which is dense along A. For a contradiction assume that A avoids f. Define a $t(n)$-strategy s by letting

$$s(X\upharpoonright x) = \begin{cases} f(X\upharpoonright x) & \text{if } f(X\upharpoonright x)\downarrow \\ \frac{1}{2} & \text{otherwise.} \end{cases}$$

Informally, given $X\upharpoonright x$, the strategy s makes a bet iff $f(X\upharpoonright x)\downarrow$, and if so then s bets the whole capital on the outcome $1 - f(X\upharpoonright x)$, i.e. the outcome that X avoids f at x. We will show that the normed $t(n)$-martingale $d[s]$ induced by s succeeds on A contrary to the assumption that A is $t(n)$-random. First observe that, by A avoiding f, $f(A\upharpoonright x) = 1 - A(x)$ for all x such that $f(A\upharpoonright x)\downarrow$, whence $d[s](A\upharpoonright x)$ is nondecreasing in x. Moreover, by density of f along A, $d[s]((A\upharpoonright x)A(x)) = 2 \cdot d[s](A\upharpoonright x)$ for infinitely many x, whence $A \in S^\infty[d[s]]$. □

Theorem 4.5 provides a new approach for establishing properties of $t(n)$-random sets, by showing these properties for the $t(n)$-generic sets. E.g., by the second part of Example 4.2, every $t(n)$-generic set is $\mathbf{DTIME}(t(2^n-1))$-bi-immune, which gives an alternative proof of Lemma 3.13.

Lemma 4.6 (Ambos-Spies, Neis and Terwijn [ANT94]). Let A be $t(n)$-generic. Then A is $\mathbf{DTIME}(t(2^n-1))$-bi-immune. □.

Similarly we can show that a $t(n)$-generic set, hence a $t(n)$-random set, is incompressible under $\mathbf{DTIME}(t(2^n-1))$ many-one reductions. Recall that a set A is $\mathbf{DTIME}(t(n))$-*m-incompressible* if, for any set B and for any function $g \in \mathbf{DTIME}(t(n))$ such that $A \leq_m B$ via g, g is almost one-to-one (i.e., for some string x, $g(y) \neq g(z)$ for all strings $x < y < z$). A set A is *p-m-incompressible* if A is $\mathbf{DTIME}(n^k)$-m-incompressible for all $k \geq 1$.

Lemma 4.7 (Ambos-Spies, Neis and Terwijn [ANT94]). Let A be $n \cdot t(n)$-generic. Then A is $\mathbf{DTIME}(t(2^n-1))$-m-incompressible.

Proof. Fix $g \in \mathbf{DTIME}(t(2^n-1))$ and B such that $A(x) = B(g(x))$ for all x. Then g is *consistent* with A, i.e.,

$$\forall\, x, y\ \ (g(x) = g(y)\ \Rightarrow\ A(x) = A(y)).$$

Define the simple $n \cdot t(n)$-extension function f by letting $f(X{\restriction}x) = 1 - X(y)$ for the least $y < x$ such that $g(y) = g(x)$ if such a y exists, and by letting $f(X{\restriction}x)\uparrow$ otherwise.

Then, for any set X which meets f, g is not consistent with X. So, by $n \cdot t(n)$-genericity of A, f is not dense along A. Since $f(A{\restriction}x)\downarrow$ if x witnesses a violation of the injectivity of g, it follows that g is almost one-to-one. □

Note that any $t(n)$-m-incompressible set is $t(n)$-bi-immune (Ko and Moore [KoM75]). Incompressibility is frequently used in the following form.

Proposition 4.8. Let A be p-m-incompressible and let $A \leq^p_m B$ via g. There is a number n_0 such that

$$\forall n \geq n_0 \, \exists x \, (|x| = n \ \& \ |g(x)| \geq n).$$

Moreover, for $G = \{x : |g(x)| \geq |x| - 1\}$, $\|G^{\leq n+1}\| \geq 2^n$ a.e.

Proof. There are 2^n strings of length n but only $2^n - 1$ strings of length less than n. □

For obtaining more properties of the $t(n)$-generic, hence the $t(n)$-random sets, it is useful to note that a $t(n)$-generic set does not only meet 1-bit extension functions but also those extension functions for which the extension is specified by a constant number of strings, and that it meets the extension functions not just once but infinitely often.

Proposition 4.9 (Ambos-Spies et al. [AFH87]). Let A be $t(n)$-generic and let f be a simple $t(n)$-extension function which is dense along A. Then A meets f at x for infinitely many strings x.

Proof. Given y, it suffices to show that A meets f at x for some $x \geq y$. Define the simple $t(n)$-extension function f_y by letting $f_y(X{\restriction}x) = f(X{\restriction}x)$ for strings $X{\restriction}x$ where $x \geq y$ and by letting $f_y(X{\restriction}x)$ be undefined otherwise. Then f_y is dense along A, whence A meets f_y. By definition of f_y this implies that A meets f for some $x \geq y$. □

Definition 4.10. A $t(n)$-extension function f is *k-bounded* ($k \geq 1$) if whenever $f(X{\restriction}x)$ is defined then $f(X{\restriction}x) = (x_0, i_0), \ldots, (x_l, i_l)$ for some $l < k$ (and for some $x_0, \ldots, x_l$, $i_0, \ldots, i_l$). If, moreover, $x_m = x + m$ for $m \leq l$ then f is *strongly k-bounded.*

Lemma 4.11. Let A be $n \cdot t(n)$-generic. Then A meets every k-bounded $t(n)$-extension function f which is dense along A at infinitely many strings x ($k \geq 1$).

Lemma 4.11 has been shown for strongly k-bounded extensions in [AFH87] and in its general form in [Am96].

Proof. Fix a k-bounded extension function f which is dense along A. W.l.o.g. we may assume that, for $X{\restriction}x$ in the domain of f, $f(X{\restriction}x)$ is of the form (4.1) with $m = k - 1$. Define simple $n \cdot t(n)$-extension functions f_l ($l < k$) as follows. If there is no string $x < y$ such that, for some $x_0, \ldots, x_{k-1}, i_0, \ldots, i_{k-1}$, $f(X{\restriction}x) = (x_0, i_0), \ldots, (x_{k-1}, i_{k-1})$, $y = x_l$, and $X(x_j) = i_j$ for $j < l$, then let $f_l(X{\restriction}y)$ be undefined. Otherwise choose the least such x and let $f(X{\restriction}y) = i_l$. Then, by induction on l, f_l is dense along A and (by Proposition 4.9) A meets f_l infinitely often. By definition, however, if A meets f_{k-1} infinitely often then A meets f infinitely often too. □

We now apply Lemma 4.11 to give some properties of the n^3-generic (hence n^3-random) sets related to the polynomial time reducibilities. We observe that the n^3-generic sets separate the standard bounded query reductions. Here we consider the 1 (one-one), m (many-one), $btt(k)$ (bounded truth-table of norm k), btt (bounded truth-table) and tt (truth-table) reducibilities. (For definitions and more details, see e.g. Ladner et al. [LLS75].) For any polynomial reducibility p-r from above we let

$$\begin{array}{lll} & \mathbf{P}_r(A) = \mathbf{P}_r^{\leq}(A) = \{B : B \leq_r^p A\} & (\textit{lower p-r-span} \text{ of } A) \\ (4.2) & \mathbf{P}_r^{-1}(A) = \mathbf{P}_r^{\geq}(A) = \{B : A \leq_r^p B\} & (\textit{upper p-r-span} \text{ of } A) \\ & \mathbf{P}_r^{=}(A) = \{B : A =_r^p B\} & (\textit{p-r-degree} \text{ of } A) \end{array}$$

Theorem 4.12 ([AFH87],[ANT94]). Let A be n^3-generic. Then, for any $k \geq 1$,

$$(4.3) \quad \mathbf{P}_1(A) \subset \mathbf{P}_m(A) \subset \mathbf{P}_{btt(k)}(A) \subset \mathbf{P}_{btt(k+1)}(A) \subset \mathbf{P}_{btt}(A) \subset \mathbf{P}_{tt}(A).$$

Proof. As one can easily check,

$$\begin{array}{lll} A \oplus A \leq_m^p A, & & \\ \overline{A} \leq_{btt(1)}^p A, & & \\ A_k \leq_{btt(k+1)}^p A, & \text{where} & A_k = \{x : \{x, \dots, x+k\} \cap A \neq \emptyset\} \\ A_\omega \leq_{tt}^p A, & \text{where} & A_\omega = \{0^k 1x : x \in A_k\} \end{array}$$

Hence it suffices to show that

$$(4.4) \quad A \oplus A \not\leq_1^p A$$

$$(4.5) \quad \overline{A} \not\leq_m^p A$$

$$(4.6) \quad A_k \not\leq_{btt(k)}^p A$$

$$(4.7) \quad A_\omega \not\leq_{btt}^p A$$

Now (4.7) is an easy consequence of (4.6). The other claims are proved by contradiction. For a fixed reduction refuting the claim, we define a simple or bounded n^2-extension function f such that f is dense along A but A does not meet f. By Lemma 4.11 this will contradict n^3-genericity of A. In the first two parts we use p-m-incompressibility of the n^2-generic sets to avoid case distinctions in the definition of the extension function.
1. Assume that $A \oplus A \leq_1^p A$ via the one-to-one function $g \in \mathbf{P}$. Then, for all strings x,

$$(4.8) \quad A(g(0x)) = A(g(1x)) \text{ and } g(0x) \neq g(1x).$$

Moreover, by injectivity of g, as in the proof of Proposition 4.8 we can argue that for all $n \geq 1$ there is a string x of length n such that $|g(0x)| \geq n$ and $|g(1x)| \geq n$. For each n let x_n be the least such string. Then f, defined by $f(X \restriction 0^n) = (g(0x_n), 0), (g(1x_n), 1)$ and $f(X \restriction x) \uparrow$ otherwise, is a 2-bounded n^2-extension function which is dense along all sets. By (4.8), however, A does not meet f.
2. Assume that $\overline{A} \leq_m^p A$ via $g \in \mathbf{P}$. Then, for all strings x,

$$(4.9) \quad A(x) \neq A(g(x))$$

and, by Lemma 4.7 and Proposition 4.8, we may fix n_0 such that, for $n \geq n_0$, $|g(x)| \geq n$ for some string x of length n. Let x_n be the first such string. Then f, defined by $f(X \upharpoonright 0^n) = (x_n, 0), (g(x_n), 0)$ and $f(X \upharpoonright x) \uparrow$ otherwise, is a 2-bounded n^2-extension function which is dense along all sets but, by (4.9), A does not meet f.
3. Assume that $A_k \leq^p_{btt(k)} A$ via $g_0, \ldots, g_{k-1}, h \in \mathbf{P}$ where $g_i : \{0,1\}^* \to \{0,1\}^*$ are selectors and $h : \{0,1\}^* \times \{0,1\}^k \to \{0,1\}$ is an evaluator so that

$$(4.10) \qquad A_k(x) = h(x, A(g_0(x)), \ldots, A(g_{k-1}(x)))$$

for all strings x. Moreover, w.l.o.g., $g_0(x) < g_1(x) < \ldots < g_{k-1}(x)$ for all x. Define a total $(2k+1)$-bounded n^2-extension function f as follows. Given $X \upharpoonright x$, let l be the least m such that $g_m(x) \geq x$ or $m = k$, let $i = h(x, X(g_0(x)), \ldots, X(g_{l-1}(x)), 0, \ldots, 0)$, and let $z_0, \ldots, z_n$ be the elements of

$$\{x, \ldots, x+k\} - \{g_0(x), \ldots, g_{k-1}(x)\}$$

in order. (Note that this difference is nonempty whence z_0 is defined.) Then

$$f(X \upharpoonright x) = (z_0, 1-i), (z_1, 0), \ldots, (z_n, 0), (g_l(x), 0), \ldots, (g_{k-1}(x), 0).$$

It remains to show that A does not meet f at x. Otherwise, $A(g_m(x)) = 0$ for $l \leq m < k$, whence $h(x, A(g_0(x)), \ldots, A(g_{k-1}(x))) = i$, while on the other side $A \cap \{x, \ldots x+k\} = A \cap \{z_0\}$ and $\| A \cap \{z_0\} \| = 1 - i$, whence $A_k(x) = 1 - i$. So (4.10) fails contrary to assumption. □

In the remainder of this section we will address some limitations of $t(n)$-genericity and the resulting differences between $t(n)$-genericity and $t(n)$-randomness. These limitations are illustrated by the following technical result, which we state without proof.

Theorem 4.13 (Ambos-Spies et al. [ANT94]). For any recursive function t, any recursive set B, and any recursive nondecreasing and unbounded function $s : N \to N$ there is a recursive $t(n)$-generic set G such that $\|(G \Delta B)^{=n}\| \leq s(n)$ for all n.

The first limitation of $t(n)$-genericity, which is typical for genericity in general, is that genericity alone does not suffice to control the frequency with which an extension function is met. By Proposition 4.9 we know that a $t(n)$-generic set G meets every simple $t(n)$-extension function which is dense along G infinitely often and, similarly, by symmetry, G avoids f at infinitely many strings. The relative frequency of these events, however, is not determined by G. E.g., for the extension function $f(X \upharpoonright x) = 0$ requiring the next bit to be a 0, balanced occurrences of the events of A meeting and avoiding f at some string x will result in a set A satisfying the *law of large numbers*:

$$(4.11) \qquad \lim_{n \to \infty} \frac{\| \{x < n : A(x) = 0\} \|}{\| \{x < n : A(x) = 1\} \|} = 1$$

In particular such a set is exponentially dense. There are $t(n)$-generic sets, however, which are sparse.

Corollary 4.14 ([AFH88], [ANT94]). There is a sparse $t(n)$-generic set G.

Proof. In Theorem 4.13 let $B = \emptyset$ and $s(n) = n$. Then $\| G^{\leq n} \| \leq n^2$. □

In [AMWZ96] the concept of balanced $t(n)$-genericity is introduced which overcomes this shortcoming.

Definition 4.15 (Ambos-Spies, Mayordomo, Wang, Zheng [AMWZ96]). A set A is *balancedly $t(n)$-generic* if A *balancedly* meets every simple $t(n)$-extension function f which is dense along A, i.e., if

$$\text{(4.12)} \quad \lim_{n\to\infty} \frac{\| \{x < n : \ A \text{ meets } f \text{ at } x\} \|}{\| \{x < n : \ f(A\restriction x)\downarrow\} \|} = \frac{1}{2}.$$

We will discuss this concept, which coincides with the resource-bounded version of the recursive randomness concept proposed by Church [Ch40], in the next section. There, in particular, we will show that any $t(n)$-random set is balancedly $t(n)$-generic.

Balancing $t(n)$-genericity, however, is not sufficient for completely subsuming $t(n)$-randomness. As shown in Lemma 4.11, $t(n)$-genericity does not only capture diagonalization steps of length 1 but also those of constant length. If the length of the diagonalization grows with the length of the string at which we (start to) diagonalize, however, then $t(n)$-genericity in general will fail. We will illustrate this phenomenon by considering necessary gaps in the $t(n)$-generic sets.

We say that a set A has *$s(n)$-gaps* ($s(n) \leq 2^n$) if, for infinitely many n, the first $s(n)$ strings of length n do not belong to A, i.e., if $A \cap \{0^n, 0^n + 1, \ldots, 0^n + s(n) - 1\} = \emptyset$. Note that A has 2^n-gaps iff A has exponential gaps in the sense of Example 2.10.4.

Lemma 4.16.

(a) For $t(n) \geq n^3$ and $k \geq 1$, every $t(n)$-generic set A has k-gaps.

(b) Let $l : N \to N$ be a recursive, nondecreasing, unbounded function. There is a recursive $t(n)$-generic set G without $l(n)$-gaps.

Proof. Part (a) follows from Lemma 4.11 by considering the k-bounded n^2-extension function $f(X\restriction 0^n) = (0^n, 0), \ldots, (0^n + k - 1, 0)$. For a proof of part (b) apply Theorem 4.13 to $B = \{0,1\}^*$ and $s(n) = l(n) \dot{-} 1$. □

Though this limitation of $t(n)$-genericity extends to balanced $t(n)$-genericity, $t(n)$-randomness captures certain diagonalizations of non-constant length. In Section 8 we will discuss this in more detail.

5 Stochasticity

The first notion of randomness was proposed by von Mises [vM19] in 1919. He called a sequence $A \in \{0,1\}^\infty$ random if the sequence satisfies the law of large numbers (4.11) and if this property is inherited by every infinite subsequence of A obtained by an "admissible selection rule". In 1940 Church [Ch40] formalized this concept by interpreting "admissible selection" by recursive selection functions thereby introducing the first algorithmic randomness concept. Following Kolmogorov (see [USS90]) we call randomness based on the uniform distribution of 0*s* and 1*s* *stochasticity*.

Ambos-Spies, Mayordomo, Wang, and Zheng [AMWZ96] recently introduced $t(n)$-stochasticity, a resource-bounded version of Church's stochasticity concept, and they analyzed the relations between $t(n)$-stochasticity, $t(n)$-genericity, and $t(n)$-randomness. By giving characterizations of $t(n)$-stochasticity in terms of prediction functions, which are just simple extension functions, and in terms of martingales, they showed that $t(n)$-stochasticity and balanced $t(n)$-genericity coincide and that the following implications hold:

(5.1) $t(n)$-random $\Rightarrow$ $t(n)$-stochastic $\Rightarrow$ $t(n)$-generic

Here we summarize these results and give a few properties of the $t(n)$-stochastic sets.

Definition 5.1 (Church [Ch40] , Ambos-Spies et al. [AMWZ96]). A *selection function* is a total recursive function $f: \{0,1\}^* \to \{0,1\}$. A *$t(n)$-selection function* is a selection function $f \in \mathbf{DTIME}(t(n))$. The selection function f is *dense along* a set A if $f(A\restriction x) = 1$ for infinitely many x. For f dense along A, the *subsequence* of A *selected* by f is the sequence

$$S[A, f] = i_0 i_1 i_2 \dots \quad (i_n \in \{0, 1, \lambda\})$$

where $i_n = A(n)$ if $f(A\restriction n) = 1$ and $i_n = \lambda$ otherwise. A set A is *$t(n)$-stochastic* if, for every $t(n)$-selection function f which is dense along A, the selected subsequence $S[A, f]$ satisfies the law of large numbers, i.e.,

$$(5.2) \quad \lim_{n\to\infty} \frac{\| \{x < n : f(A\restriction x) = 1 \;\&\; x \in A\} \|}{\| \{x < n : f(A\restriction x) = 1\} \|} = \frac{1}{2}.$$

Di Paola [Pa69] studied subrecursive versions of Church stochasticity corresponding to the Ritchie and Grzegorczyk hierarchies. Time-bounded stochasticity concepts, which are weaker than the one introduced above, were proposed by Wilber [Wi83] and Ko [Ko86]. For the relations among these resource-bounded stochasticity concepts see [AMWZ96].

To illustrate Definition 5.1, let $B \in \mathbf{DTIME}(t(2^n - 1))$. Then f defined by $f(X\restriction n) = B(n)$ is a $t(n)$-selection function which selects the places x which are elements of B. So, for infinite B, f is dense along all sets A, and $A \cap B \neq \emptyset$ iff the sequence $S[A, f]$ contains at least one 1. So, for $t(n)$-stochastic A, $A \cap B \neq \emptyset$. By symmetry, it follows that every $t(n)$-stochastic set is $\mathbf{DTIME}(t(2^n - 1))$-bi-immune.

By taking the n-selection function f selecting all places, i.e. $f(X\restriction x) = 1$ everywhere, $S[A, f] = A$, whence, by (5.2) every $t(n)$-stochastic set A satisfies the law of large numbers (4.11).

Proposition 5.2 ([AMWZ96]). Let A be $t(n)$-stochastic. Then A satisfies the law of large numbers, hence is exponentially dense.

Proof. By the above, it suffices to observe that (4.11) implies that $\|A^{\leq n}\| \geq 2^{n-1}$ for almost all n. □

For comparing $t(n)$-stochasticity with $t(n)$-genericity and $t(n)$-randomness it is convenient to characterize this concept in terms of *prediction* functions.

Definition 5.3 ([AMWZ96]). A *prediction function* f is a partial recursive function $f : \{0,1\}^* \to \{0,1\}$ with recursive domain. A *$t(n)$-prediction function* is a prediction function $f \in \mathbf{DTIME}(t(n))$. A prediction function f is *dense* along a set A if $f(A\restriction x)\downarrow$ for infinitely many x. f *predicts* A if f is dense along A and

$$(5.3) \qquad \limsup_{n\to\infty} \frac{\| \{x < n : f(A\restriction x)\downarrow = A(x)\} \|}{\| \{x < n : f(A\restriction x)\downarrow\} \|} > \frac{1}{2}.$$

A set A is *$t(n)$-predictable* if there is a $t(n)$-prediction function which predicts A, and A is *$t(n)$-unpredictable* otherwise.

Just like a martingale, a prediction function f can be interpreted as a strategy in a fair betting game on the successive bits of a hidden sequence $X \in \{0,1\}^\infty$. A player using this strategy who has seen the first n bits $X\restriction n$ of this sequence will predict that the next bit will be i if $f(X\restriction n) = i$ and he will not make any prediction for the next bit if $f(X\restriction n)\uparrow$. The player will win if he makes infinitely many predictions (i.e. if f is dense along X) and, for some $\epsilon > 0$, the ratio of the correct vs. the false predictions will be greater than or equal to $1+\epsilon$ infinitely often (i.e. f predicts X).

Note that making no prediction corresponds to splitting the capital in equal parts on the 0 and 1 outcomes in the martingale game. As we will see below, the martingale game is more flexible in allowing the player to express different degrees of confidence in the prediction, by allocating smaller or larger sums on the predicted bit. If we eliminate this option, however, both concepts are equivalent (see Theorem 5.6 below).

Note that a $t(n)$-prediction function is just a simple $t(n)$-extension function: Density along a set is defined in the same way for both concepts, and f correctly predicts a value $A(x)$ iff A meets f at x. So unpredictability and balanced genericity coincide. Moreover, selection and prediction functions can be expressed by each other whence we obtain the following equivalence.

Theorem 5.4 ([AMWZ96]). For any recursive function t and any set A, the following are equivalent.

(i) A is $t(n)$-stochastic

(ii) A is $t(n)$-unpredictable

(iii) A is balancedly $t(n)$-generic

Proof. We will prove the implications (i) $\Rightarrow$ (ii) $\Rightarrow$ (iii) $\Rightarrow$ (i).
(i) $\Rightarrow$ (ii). Let A be $t(n)$-stochastic and let f be a $t(n)$-prediction function which is dense along A. We have to show that (5.3) fails. For a contradiction assume (5.3). Then, for some $i \in \{0,1\}$, $f(A\restriction x) = i$ for infinitely many x and

$$\limsup_{n\to\infty} \frac{\| \{x < n : f(A\restriction x) = i = A(x)\} \|}{\| \{x < n : f(A\restriction x) = i\} \|} > \frac{1}{2}.$$

So, for the $t(n)$-selection function $\hat{f}$ defined by $\hat{f}(X\restriction x) = 1$ if $f(X\restriction x) = i$ and $\hat{f}(X\restriction x) = 0$ otherwise, $\hat{f}$ is dense along A and (5.2) fails for $\hat{f}$ (in place of f). So A is not $t(n)$-stochastic contrary to assumption.
(ii) $\Rightarrow$ (iii). Let A be $t(n)$-unpredictable and let f be a simple $t(n)$-extension function