Guang Gong
Tor Helleseth
Hong-Yeop Song
Kyeongcheol Yang (Eds.)

Sequences and Their Applications – SETA 2006

LNCS 4086

4th International Conference
Beijing, China, September 2006
Proceedings

Springer

Guang Gong Tor Helleseth
Hong-Yeop Song Kyeongcheol Yang (Eds.)

Sequences and Their Applications – SETA 2006

4th International Conference
Beijing, China, September 24-28, 2006
Proceedings

Springer

Volume Editors

Guang Gong
University of Waterloo
Department of Electrical and Computer Engineering
200 University Avenue West, Waterloo, ON, N2L 3G1, Canada
E-mail: ggong@calliope.uwaterloo.ca

Tor Helleseth
University of Bergen
Department of Informatics
Thormohlensgate 55, 5020 Bergen, Norway
E-mail: tor.helleseth@ii.uib.no

Hong-Yeop Song
Center for Information Technology of Yonsei University
School of Electrical and Electronics Engineering
Seoul,120-749, Korea
E-mail: hy.song@coding.yonsei.ac.kr

Kyeongcheol Yang
Pohang University of Science and Technology (POSTECH)
Dept. of Electronic and Electrical Engineering
Pohang, Gyungbuk 790-784, Korea
E-mail: kcyang@postech.ac.kr

Library of Congress Control Number: 2006932045

CR Subject Classification (1998): E.4, F.2, I.1, E.3, F.1, G.1

LNCS Sublibrary: SL 1 – Theoretical Computer Science and General Issues

ISSN 0302-9743
ISBN-10 3-540-44523-4 Springer Berlin Heidelberg New York
ISBN-13 978-3-540-44523-4 Springer Berlin Heidelberg New York

Typesetting: Camera-ready by author, data conversion by Scientific Publishing Services, Chennai, India
Printed on acid-free paper SPIN: 11863854 06/3142 5 4 3 2 1 0

Lecture Notes in Computer Science 4086

Commenced Publication in 1973
Founding and Former Series Editors:
Gerhard Goos, Juris Hartmanis, and Jan van Leeuwen

Editorial Board

Preface

This volume contains the refereed proceedings of the Fourth International Conference on Sequences and Their Applications (SETA 2006), held in Beijing, China during September 24–28, 2006. The previous three conferences SETA '98, SETA 2001, and SETA 2004 were held in Singapore, Bergen, and Seoul, respectively. The SETA conferences are motivated by the numerous applications of sequences in modern communication systems. These applications include pseudorandom sequences in spread spectrum, code-division-multiple-access, stream ciphers in cryptography, and several connections to coding theory and boolean functions.

The Technical Program Committee of SETA 2006 refereed 70 submitted papers. This represented more submissions than to any of the previous SETA conferences. The committee therefore had the challenging task of selecting 32 papers to be presented at the conference in addition to 4 invited papers.

The Co-chairs of the Technical Program Committee for SETA 2006, were Guang Gong (University of Waterloo) and Tor Helleseth (University of Bergen), with Hong-Yeop Song (Yonsei University, Korea) and Kyeongcheol Yang (Pohang University of Science and Technology, Korea) as the co-editors for these proceedings.

The editors wish to thank the other members of the Technical Program Committee: Anne Canteaut (INRIA, France), Claude Carlet (INRIA and University of Paris 8, France), Habong Chung, (Hongik University, Korea), Zongduo Dai (University of Science and Technology of China, Beijing, China), Cunsheng Ding (Hong Kong University of Science and Technology, Hong Kong), Pingzhi Fan (Southwest Jiaotong University, China), Dengguo Feng (Chinese Academy of Sciences, China), Solomon W. Golomb (University of Southern California, USA), Kyoki Imamura (Kyushu Institute of Technology, Japan), Jonathan Jedwab (Simon Fraser University, Canada), Thomas Johansson (University of Lund, Sweden), Andrew Klapper (University of Kentucky, USA), P. Vijay Kumar (University of Southern California, USA), Wai Ho Mow (Hong Kong University of Science and Technology, Hong Kong), Harald Niederreiter (National University of Singapore, Singapore), Jong-Seon No (Seoul National University, Korea), Matthew G. Parker (University of Bergen, Norway), Kenneth G. Paterson (Royal Holloway, University of London, UK), Alexander Pott (Otto-von-Guericke-University Magdeburg, Germany), Hans Schotten (Qualcomm Germany, Nuremberg, Germany), Parampalli Udaya (University of Melbourne, Australia), and Amr Youssef (Concordia University, Canada) for providing clear, insightful, and prompt reviews of the submitted papers.

The editors are also grateful to Serdar Boztas, Jin-Ho Chung, Deepak Kumar Dalai, Frédéric Didier, Gary Greenfield, Yun-Kyoung Han, Tom Høholdt, Alexander Kholosha, Margreta Kuijper, Gohar Kyureghyan, Cedric Lauradoux, Subhamoy Maitra, Joe Rushanan, Frank Ruskey, Igor Semaev, Jean-Pierre

Tillich, and Nam Yul Yu for their help and assistance in the reviewing of papers for SETA 2006. A special thanks goes to Sondre Rønjom for handling all the submissions and the web-review software during the review process.

In addition to the contributed papers, there are four invited papers. These papers provide a historical overview as well as new developments in important areas of the design and analysis of sequences. The invited contribution by Solomon Golomb presents a retro-perspective of some selected results on sequences. The invited paper by Harald Niederreiter includes an updated overview and some recent important results on the complexity of multisequences. Vijay Kumar provides an overview and new results on optical orthogonal codes. This topic is motivated by applying code division multiple access (CDMA) techniques in optical networks. Zongduo Dai presents an overview of multi-continued fraction algorithms and their applications to sequences.

We wish to thank Pingzhi Fan and Dengguo Feng for their support as General Co-chairs of SETA 2006, and Chuan-Kun Wu for local arrangements and updating the web site of SETA '06. We also thank Yi Qin for her support as secretary of SETA 2006, and Shi Zhang for her support as treasurer of SETA 2006. Last but not least, we thank all the authors of the papers for their help and collaboration in preparing this volume. Finally, we would like to thank the National Science Foundation of China (NSFC) and the Chinese Academy of Sciences (CAS) for their financial support.

September 2006

Guang Gong
Tor Helleseth
Hong-Yeop Song
Kyeongcheol Yang

Organization

SETA 2006

September 24-28, 2006, Beijing, China

General Co-chairs

Pingzhi Fan, Southwest Jiaotong University, China
Dengguo Feng, Chinese Academy of Sciences, China

Program Co-chairs

Guang Gong, University of Waterloo, Canada
Tor Helleseth, University of Bergen, Norway

Local Arrangements

Chuan-Kun Wu, Chinese Academy of Sciences, China

Secretary and Registration

Yi Qin, Chinese Academy of Sciences, China

Treasurer

Shi Zhang, Chinese Academy of Sciences, China

Proceedings Co-editors

Guang Gong, University of Waterloo, Canada
Tor Helleseth, University of Bergen, Norway
Hong-Yeop Song, Yonsei University, Korea
Kyeongcheol Yang, Pohang Univ. of Science and Technology, Korea

Technical Program Committee for SETA 2006

Program Co-chairs

Guang Gong ..... University of Waterloo, Canada
Tor Helleseth ..... University of Bergen, Norway

Program Committee

Anne Canteaut ..... INRIA, France
Claude Carlet ..... INRIA and University of Paris 8, France
Habong Chung ..... Hongik University, Korea
Zongduo Dai ..... University of Science and Technology of China, China
Cunsheng Ding ..... Hong Kong University of Science and Technology, China
Pingzhi Fan ..... Southwest Jiaotong University, China
Dengguo Feng ..... Chinese Academy of Sciences, China
Solomon W. Golomb ..... University of Southern California, USA
Kyoki Imamura ..... Kyushu Institute of Technology, Japan
Jonathan Jedwab ..... Simon Fraser University, Canada
Thomas Johansson ..... University of Lund, Sweden
Andrew Klapper ..... University of Kentucky, USA
P. Vijay Kumar ..... University of Southern California, USA
Wai Ho Mow ..... Hong Kong University of Science and Technology, China
Harald Niederreiter ..... National University of Singapore, Singapore
Jong-Seon No ..... Seoul National University, Korea
Matthew G. Parker ..... University of Bergen, Norway
Kenneth G. Paterson ..... Royal Holloway, University of London, UK
Alexander Pott ..... Otto-von-Guericke University Magdeburg, Germany
Hans Schotten ..... Qualcomm Germany, Germany
Hong-Yeop Song ..... Yonsei University, Korea
Parampalli Udaya ..... University of Melbourne, Australia
Kyeongcheol Yang ..... Pohang University of Science and Technology, Korea
Amr Youssef ..... Concordia University, Canada

Lecture Notes in Computer Science

For information about Vols. 1–4085

please contact your bookseller or Springer

Vol. 4228: D.E. Lightfoot, C.A. Szyperski (Eds.), Modular Programming Languages. X, 415 pages. 2006.

Vol. 4208: M. Gerndt, D. Kranzlmüller (Eds.), High Performance Computing and Communications. XXII, 938 pages. 2006.

Vol. 4206: P. Dourish, A. Friday (Eds.), UbiComp 2006: Ubiquitous Computing. XIX, 526 pages. 2006.

Vol. 4193: T.P. Runarsson, H.-G. Beyer, E. Burke, J.J. Merelo-Guervós, L. D. Whitley, X. Yao (Eds.), Parallel Problem Solving from Nature - PPSN IX. XIX, 1061 pages. 2006.

Vol. 4192: B. Mohr, J.L. Träff, J. Worringen, J. Dongarra (Eds.), Recent Advances in Parallel Virtual Machine and Message Passing Interface. XVI, 414 pages. 2006.

Vol. 4188: P. Sojka, I. Kopeček, K. Pala (Eds.), Text, Speech and Dialogue. XIV, 721 pages. 2006. (Sublibrary LNAI).

Vol. 4187: J.J. Alferes, J. Bailey, W. May, U. Schwertel (Eds.), Principles and Practice of Semantic Web Reasoning. XI, 277 pages. 2006.

Vol. 4186: C. Jesshope, C. Egan (Eds.), Advances in Computer Systems Architecture. XIV, 605 pages. 2006.

Vol. 4185: R. Mizoguchi, Z. Shi, F. Giunchiglia (Eds.), The Semantic Web – ASWC 2006. XX, 778 pages. 2006.

Vol. 4184: M. Bravetti, M. Núñez, G. Zavattaro (Eds.), Web Services and Formal Methods. X, 289 pages. 2006.

Vol. 4183: J. Euzenat, J. Domingue (Eds.), Artificial Intelligence: Methodology, Systems, and Applications. XIII, 291 pages. 2006. (Sublibrary LNAI).

Vol. 4180: M. Kohlhase, OMDoc – An Open Markup Format for Mathematical Documents [version 1.2]. XIX, 428 pages. 2006. (Sublibrary LNAI).

Vol. 4178: A. Corradini, H. Ehrig, U. Montanari, L. Ribeiro, G. Rozenberg (Eds.), Graph Transformations. XII, 473 pages. 2006.

Vol. 4176: S.K. Katsikas, J. Lopez, M. Backes, S. Gritzalis, B. Preneel (Eds.), Information Security. XIV, 548 pages. 2006.

Vol. 4175: P. Bücher, B.M.E. Moret (Eds.), Algorithms in Bioinformatics. XII, 402 pages. 2006. (Sublibrary LNBI).

Vol. 4174: K. Franke, K.-R. Müller, B. Nickolay, R. Schäfer (Eds.), Pattern Recognition. XX, 773 pages. 2006.

Vol. 4169: H.L. Bodlaender, M.A. Langston (Eds.), Parameterized and Exact Computation. XI, 279 pages. 2006.

Vol. 4168: Y. Azar, T. Erlebach (Eds.), Algorithms – ESA 2006. XVIII, 843 pages. 2006.

Vol. 4165: W. Jonker, M. Petković (Eds.), Secure, Data Management. X, 185 pages. 2006.

Vol. 4163: H. Bersini, J. Carneiro (Eds.), Artificial Immune Systems. XII, 460 pages. 2006.

Vol. 4162: R. Královič, P. Urzyczyn (Eds.), Mathematical Foundations of Computer Science 2006. XV, 814 pages. 2006.

Vol. 4160: M. Fisher, W.v.d. Hoek, B. Konev, A. Lisitsa (Eds.), Logics in Artificial Intelligence. XII, 516 pages. 2006. (Sublibrary LNAI).

Vol. 4159: J. Ma, H. Jin, L.T. Yang, J.J.-P. Tsai (Eds.), Ubiquitous Intelligence and Computing. XXII, 1190 pages. 2006.

Vol. 4158: L.T. Yang, H. Jin, J. Ma, T. Ungerer (Eds.), Autonomic and Trusted Computing. XIV, 613 pages. 2006.

Vol. 4156: S. Amer-Yahia, Z. Bellahsène, E. Hunt, R. Unland, J.X. Yu (Eds.), Database and XML Technologies. IX, 123 pages. 2006.

Vol. 4155: O. Stock, M. Schaerf (Eds.), Reasoning, Action and Interaction in AI Theories and Systems. XVIII, 343 pages. 2006. (Sublibrary LNAI).

Vol. 4153: N. Zheng, X. Jiang, X. Lan (Eds.), Advances in Machine Vision, Image Processing, and Pattern Analysis. XIII, 506 pages. 2006.

Vol. 4152: Y. Manolopoulos, J. Pokorný, T. Sellis (Eds.), Advances in Databases and Information Systems. XV, 448 pages. 2006.

Vol. 4151: A. Iglesias, N. Takayama (Eds.), Mathematical Software - ICMS 2006. XVII, 452 pages. 2006.

Vol. 4150: M. Dorigo, L.M. Gambardella, M. Birattari, A. Martinoli, R. Poli, T. Stützle (Eds.), Ant Colony Optimization and Swarm Intelligence. XVI, 526 pages. 2006.

Vol. 4149: M. Klusch, M. Rovatsos, T.R. Payne (Eds.), Cooperative Information Agents X. XII, 477 pages. 2006. (Sublibrary LNAI).

Vol. 4148: J. Vounckx, N. Azemard, P. Maurine (Eds.), Integrated Circuit and System Design. XVI, 677 pages. 2006.

Vol. 4146: J.C. Rajapakse, L. Wong, R. Acharya (Eds.), Pattern Recognition in Bioinformatics. XIV, 186 pages. 2006. (Sublibrary LNBI).

Vol. 4144: T. Ball, R.B. Jones (Eds.), Computer Aided Verification. XV, 564 pages. 2006.

Vol. 4139: T. Salakoski, F. Ginter, S. Pyysalo, T. Pahikkala, Advances in Natural Language Processing. XVI, 771 pages. 2006. (Sublibrary LNAI).

Vol. 4138: X. Cheng, W. Li, T. Znati (Eds.), Wireless Algorithms, Systems, and Applications. XVI, 709 pages. 2006.

Vol. 4137: C. Baier, H. Hermanns (Eds.), CONCUR 2006 – Concurrency Theory. XIII, 525 pages. 2006.

Vol. 4136: R.A. Schmidt (Ed.), Relations and Kleene Algebra in Computer Science. XI, 433 pages. 2006.

Vol. 4135: C.S. Calude, M.J. Dinneen, G. Păun, G. Rozenberg, S. Stepney (Eds.), Unconventional Computation. X, 267 pages. 2006.

Vol. 4134: K. Yi (Ed.), Static Analysis. XIII, 443 pages. 2006.

Vol. 4133: J. Gratch, M. Young, R. Aylett, D. Ballin, P. Olivier (Eds.), Intelligent Virtual Agents. XIV, 472 pages. 2006. (Sublibrary LNAI).

Vol. 4132: S. Kollias, A. Stafylopatis, W. Duch, E. Oja (Eds.), Artificial Neural Networks – ICANN 2006, Part II. XXXIV, 1028 pages. 2006.

Vol. 4131: S. Kollias, A. Stafylopatis, W. Duch, E. Oja (Eds.), Artificial Neural Networks – ICANN 2006, Part I. XXXIV, 1008 pages. 2006.

Vol. 4130: U. Furbach, N. Shankar (Eds.), Automated Reasoning. XV, 680 pages. 2006. (Sublibrary LNAI).

Vol. 4129: D. McGookin, S. Brewster (Eds.), Haptic and Audio Interaction Design. XII, 167 pages. 2006.

Vol. 4128: W.E. Nagel, W.V. Walter, W. Lehner (Eds.), Euro-Par 2006 Parallel Processing. XXXIII, 1221 pages. 2006.

Vol. 4127: E. Damiani, P. Liu (Eds.), Data and Applications Security XX. X, 319 pages. 2006.

Vol. 4126: P. Barahona, F. Bry, E. Franconi, N. Henze, U. Sattler, Reasoning Web. X, 269 pages. 2006.

Vol. 4124: H. de Meer, J.P. G. Sterbenz (Eds.), Self-Organizing Systems. XIV, 261 pages. 2006.

Vol. 4121: A. Biere, C.P. Gomes (Eds.), Theory and Applications of Satisfiability Testing - SAT 2006. XII, 438 pages. 2006.

Vol. 4119: C. Dony, J.L. Knudsen, A. Romanovsky, A. Tripathi (Eds.), Advanced Topics in Exception Handling Components. X, 302 pages. 2006.

Vol. 4117: C. Dwork (Ed.), Advances in Cryptology - CRYPTO 2006. XIII, 621 pages. 2006.

Vol. 4116: R. De Prisco, M. Yung (Eds.), Security and Cryptography for Networks. XI, 366 pages. 2006.

Vol. 4115: D.-S. Huang, K. Li, G.W. Irwin (Eds.), Computational Intelligence and Bioinformatics, Part III. XXI, 803 pages. 2006. (Sublibrary LNBI).

Vol. 4114: D.-S. Huang, K. Li, G.W. Irwin (Eds.), Computational Intelligence, Part II. XXVII, 1337 pages. 2006. (Sublibrary LNAI).

Vol. 4113: D.-S. Huang, K. Li, G.W. Irwin (Eds.), Intelligent Computing, Part I. XXVII, 1331 pages. 2006.

Vol. 4112: D.Z. Chen, D. T. Lee (Eds.), Computing and Combinatorics. XIV, 528 pages. 2006.

Vol. 4111: F.S. de Boer, M.M. Bonsangue, S. Graf, W.-P. de Roever (Eds.), Formal Methods for Components and Objects. VIII, 447 pages. 2006.

Vol. 4110: J. Díaz, K. Jansen, J.D.P. Rolim, U. Zwick (Eds.), Approximation, Randomization, and Combinatorial Optimization. XII, 522 pages. 2006.

Vol. 4109: D.-Y. Yeung, J.T. Kwok, A. Fred, F. Roli, D. de Ridder (Eds.), Structural, Syntactic, and Statistical Pattern Recognition. XXI, 939 pages. 2006.

Vol. 4108: J.M. Borwein, W.M. Farmer (Eds.), Mathematical Knowledge Management. VIII, 295 pages. 2006. (Sublibrary LNAI).

Vol. 4106: T.R. Roth-Berghofer, M.H. Göker, H. A. Güvenir (Eds.), Advances in Case-Based Reasoning. XIV, 566 pages. 2006. (Sublibrary LNAI).

Vol. 4105: B. Gunsel, A.K. Jain, A. M. Tekalp, B. Sankur (Eds.), Multimedia, Content Representation, Classification and Security. XIX, 804 pages. 2006.

Vol. 4104: T. Kunz, S.S. Ravi (Eds.), Ad-Hoc, Mobile, and Wireless Networks. XII, 474 pages. 2006.

Vol. 4103: J. Eder, S. Dustdar (Eds.), Business Process Management Workshops. XI, 508 pages. 2006.

Vol. 4102: S. Dustdar, J.L. Fiadeiro, A. Sheth (Eds.), Business Process Management. XV, 486 pages. 2006.

Vol. 4099: Q. Yang, G. Webb (Eds.), PRICAI 2006: Trends in Artificial Intelligence. XXVIII, 1263 pages. 2006. (Sublibrary LNAI).

Vol. 4098: F. Pfenning (Ed.), Term Rewriting and Applications. XIII, 415 pages. 2006.

Vol. 4097: X. Zhou, O. Sokolsky, L. Yan, E.-S. Jung, Z. Shao, Y. Mu, D.C. Lee, D. Kim, Y.-S. Jeong, C.-Z. Xu (Eds.), Emerging Directions in Embedded and Ubiquitous Computing. XXVII, 1034 pages. 2006.

Vol. 4096: E. Sha, S.-K. Han, C.-Z. Xu, M.H. Kim, L.T. Yang, B. Xiao (Eds.), Embedded and Ubiquitous Computing. XXIV, 1170 pages. 2006.

Vol. 4095: S. Nolfi, G. Baldassarre, R. Calabretta, J.C. T. Hallam, D. Marocco, J.-A. Meyer, O. Miglino, D. Parisi (Eds.), From Animals to Animats 9. XV, 869 pages. 2006. (Sublibrary LNAI).

Vol. 4094: O. H. Ibarra, H.-C. Yen (Eds.), Implementation and Application of Automata. XIII, 291 pages. 2006.

Vol. 4093: X. Li, O.R. Zaïane, Z. Li (Eds.), Advanced Data Mining and Applications. XXI, 1110 pages. 2006. (Sublibrary LNAI).

Vol. 4092: J. Lang, F. Lin, J. Wang (Eds.), Knowledge Science, Engineering and Management. XV, 664 pages. 2006. (Sublibrary LNAI).

Vol. 4091: G.-Z. Yang, T. Jiang, D. Shen, L. Gu, J. Yang (Eds.), Medical Imaging and Augmented Reality. XIII, 399 pages. 2006.

Vol. 4090: S. Spaccapietra, K. Aberer, P. Cudré-Mauroux (Eds.), Journal on Data Semantics VI. XI, 211 pages. 2006.

Vol. 4089: W. Löwe, M. Südholt (Eds.), Software Composition. X, 339 pages. 2006.

Vol. 4088: Z.-Z. Shi, R. Sadananda (Eds.), Agent Computing and Multi-Agent Systems. XVII, 827 pages. 2006. (Sublibrary LNAI).

Vol. 4087: F. Schwenker, S. Marinai (Eds.), Artificial Neural Networks in Pattern Recognition. IX, 299 pages. 2006. (Sublibrary LNAI).

Vol. 4086: G. Gong, T. Helleseth, H.-Y. Song, K. Yang (Eds.), Sequences and Their Applications – SETA 2006. XII, 433 pages. 2006.

¥477.00元

Table of Contents

Invited Papers

Linear Complexity of Sequences

Correlation of Sequences

Stream Ciphers and Transforms

Topics in Complexities of Sequences

Linear/Nonlinear Feedback Shift Register Sequences

Multi-sequence Synthesis

Filtering Sequences and Pseudorandom Sequence Generators

Sequences and Combinatorics

FCSR Sequences

Aperiodic Correlation and Applications

Boolean Functions

Shift Register Sequences – A Retrospective Account

Solomon W. Golomb

University of Southern California
Viterbi School of Engineering
Los Angeles, CA 90089-2565
milly@usc.edu

Abstract. Binary feedback shift registers, with applications to reliable communications, stream cipher cryptography, radar signal design, pseudorandom number generation, digital wireless telephony, and many other areas, have been studied for more than half a century. The maximum-length binary linear feedback shift registers, called *m-sequences* or *PN sequences*, are the best-known and most thoroughly understood special case.

The m-sequences have several important *randomness properties*, and are known as *pseudo-random sequences*. They are characterized by the *cycle-and-add property*, whereby the term-by-term sum of two cyclic shifts is a third cyclic shift. Along with other families of binary sequences that correspond to *cyclic Hadamard difference sets*, they have the *two-level autocorrelation property*. The m-sequences share the *span-n property* (all subsequences of length n, except n zeroes, occur in each period of length $2^n - 1$) with a far larger class of nonlinear shift register sequences. No counterexample has been found to the conjecture that only the m-sequences have both the two-level autocorrelation and the span-n properties.

The class of m-sequences is too small, and has too many regularities, to provide useful cryptographic security as key sequences for stream ciphers. For this purpose, nonlinear shift register sequences which have large linear span and a sufficiently high degree of *correlation immunity* may be employed.

1 Linear Shift Register Sequences

Let $S_0 = \{a_1, a_2, \ldots, a_p\} = \{a_i\}$ be a binary sequence of period p, and $S_j = \{a_{1+j}, a_{2+j} \ldots, a_j\}$for all $0 \leq j \leq p-1$. Then S_0 is an m-sequence if and only if $S_i + S_j = S_k$ for all $0 \leq i < j \leq p-1$, where addition of sequences is term-by-term and modulo 2. Equivalently, if a p-component binary vector, together with all its cyclic shifts and the p-component zero vector, form a subspace of $GF(2^p)$, then $p = 2^n - 1$ for some n, and the binary sequence is an m-sequence; and conversely, every m-sequence has this property.

There are $\frac{\phi(p)}{n} = \frac{\phi(2^n-1)}{n}$ cyclically distinct m-sequences of degree n and period p, where ϕ is Euler's phi-function. Of the many additional properties

G. Gong et al. (Eds.): SETA 2006, LNCS 4086, pp. 1–4, 2006.

possessed by these sequences, two of the most important are the *span-n property* and the *two-level autocorrelation property.* The *span-n property* here refers to a binary sequence of period $p = 2^n - 1$ in which every possible n-bit subsequence except for n zeroes occurs exactly once in each period. These sequences are in direct one-to-one correspondence with the *de Bruijn sequences* of span n, which have period 2^n, and in which every possible n-bit subsequence appears exactly once in each period; and the exact number of cyclically distinct de Bruijn sequences is well known [1] to be $2^{2^{n-1}-n}$ for span n, for every positive integer n. The *two-level autocorrelation property* for m-sequences asserts that between S_i and S_j, for all $0 \leq i < j \leq p-1$, there are $\frac{p-1}{2} = 2^{n-1} - 1$ term-by-term agreements and $\frac{p+1}{2} = 2^{n-1}$ term-by-term disagreements. The cyclically distinct binary two-level autocorrelation sequences of period p are in one-to-one correspondence with *cyclic Hadamard difference sets* modulo p, which are the *perfect* (v, k, λ) *difference sets* having $(v, k, \lambda) = (p, \frac{p-1}{2}, \frac{p-3}{4}) = (2^n - 1, 2^{n-1} - 1, 2^{n-2} - 1)$.

All cyclic Hadamard difference sets with these parameters have been found by exhaustive computer searches for each degree n, $2 \leq n \leq 10$. All the examples thus found belong to *families* of cyclic Hadamard difference sets, for multiple values of p, which were all known before the complete search at $p = 2^{10} - 1 = 1023$ was undertaken. There is some optimism that all the constructions which yield cyclic Hadamard difference sets are now known (see [2]), but this has not been proved.

Every m-sequence of period $p = 2^n - 1$ is simultaneously a span-n sequence and a $(p, \frac{p-1}{2}, \frac{p-3}{4})$ cyclic Hadamard sequence. It has been conjectured that the converse is also true: that is, that if a binary sequence has both span-n and two-level autocorrelation, then it must be an m-sequence. While the truth of this conjecture has been verified for all $n \leq 10$, and for certain two-level autocorrelation sequences with $n > 10$, the general case of this conjecture remains open.

The m-sequences of period $p = 2^n - 1$ are in one-to-one correspondence with the irreducible polynomials of degree n over $GF(2)$ whose roots are primitive p^{th}-roots of unity. It is conjectured that there are infinitely many such polynomials with only three terms, $x^n + x^a + 1$, called *primitive trinomials* over $GF(2)$. It has even been conjectured that $x^n + x + 1$ is primitive for infinitely many values of n. By a theorem of Richard Swan, there are no primitive (or even irreducible) trinomials $x^n + x^a + 1$ where the degree n is a multiple of 8. By a theorem of Øystein Ore, if $f(x) = \sum_{i=0}^{n} a_i x^i$ is a primitive irreducible polynomial over $GF(2)$, then $F(x) = \sum_{i=0}^{n} a_i x^{2^i - 1}$ is irreducible (though not necessarily primitive). While primitive trinomials fail to exist for infinitely many degrees n, it is conjectured that primitive pentanomials (five-term polynomials) exist for every degree $n \geq 5$. However, it has not even been proved that there are infinitely many degrees n having a primitive polynomial with no more than t terms, for *any* specific positive integer t.

2 Nonlinear Shift Register Sequences

In contrast to *linear* binary feedback shift registers, which are well-understood mathematically, the much larger family of *nonlinear* feedback shift registers has far fewer regularities. The most general feedback function for an n-stage binary shift register is an arbitrary one of the 2^{2^n} boolean functions $f(x_1, x_2, \ldots, x_n)$ of n binary variables, where the variables are taken from the n stages of the shift register. The 2^n possible states of an n-stage shift register become the vertices of a directed graph ("digraph") whose directed edges go from each state to its successor state. For any particular shift register, this digraph is a subgraph of the *de Bruijn graph*, whose edges indicate all the possible shift register transitions from one state to the next. In the de Bruijn graph for the general n-stage shift register there are 2^n vertices and 2^{n+1} directed edges, showing the two possible predecessors and the two possible successors of each state of the shift register.

For any specific nonlinear shift register, its digraph will decompose entirely into one or more disjoint cycles (i.e. "cycles without branches") if and only if one can write the feedback function $f(x_1, x_2, \ldots, x_n)$ in the form $g(x_1, x_2, \ldots, x_{n-1}) + x_n$, where x_n comes from the "oldest" stage of the shift register, and is added modulo 2 to an arbitrary boolean function $g(x_1, x_2, \ldots, x_{n-1})$ of the other $n-1$ stages. In this case of "pure cycles without branches", the number of cycles has the same parity (even or odd) as the number of *ones* in the truth table of $g(x_1, x_2, \ldots, x_{n-1})$, for all $n > 2$. In particular, for $n > 2$, in order to get all 2^n possible states of the shift register to lie on a single cycle, the truth table for $g(x_1, x_2, \ldots, x_{n-1})$ must have an odd number of ones, which requires that all $n-1$ variables occur, and occur nonlinearly, in the computation of $g(x_1, x_2, \ldots, x_{n-1})$.

3 Applications

When a nonlinear shift register is used to generate a key stream for use in a stream cipher, cryptanalytic attacks which attempt to reconstruct, in whole or in part, the structure of the shift register being used, are usually based on multi-dimensional correlations of the key sequence. These correlation values correspond directly to the *invariants*, described in [1], of the boolean function $g(x_1, x_2, \ldots, x_{n-1})$, which can be obtained from the Walsh function expansion coefficients of the truth table of the function g.

Shift registers are also used for both the encoding and the decoding of both block codes and convolutional codes. They are used to generate the pseudo-random binary chip sequences needed for spectral spreading in "direct-sequence spread spectrum" secure communications and for mutual non-interference between callers in code division multiple access (CDMA) wireless telephony. The two-level correlation property makes m-sequences very well suited for use as modulation patterns in radar and sonar applications.

For a more detailed account of the properties of both linear and nonlinear shift register sequences, see [1]. For a description of the various constructions now known for $(2^n - 1, 2^{n-1} - 1, 2^{n-2} - 1)$ cyclic (Hadamard) difference sets, as well as a concluding chapter briefly mentioning various applications, see [2].