1. Record Nr. UNINA9910790471703321

Autore	Goresky Mark <1950->
Titolo	Algebraic shift register sequences / / Mark Goresky, Andrew Klapper [[electronic resource]]
Pubbl/distr/stampa	Cambridge : , : Cambridge University Press, , 2012
ISBN	1-107-23004-7 1-280-87767-7 1-139-22298-8 9786613718983 1-139-21818-2 1-139-22470-0 1-139-21509-4 1-139-22127-2 1-139-05744-8
Descrizione fisica	1 online resource (xv, 498 pages) : digital, PDF file(s)
Disciplina	621.397
Soggetti	Shift registers - Mathematics Sequences (Mathematics)
Lingua di pubblicazione	Inglese
Formato	Materiale a stampa
Livello bibliografico	Monografia
Note generali	Title from publisher's bibliographic system (viewed on 05 Oct 2015).
Nota di bibliografia	Includes bibliographical references (p. 481-490) and index.
Nota di contenuto	Cover; ALGEBRAIC SHIFT REGISTER SEQUENCES; Title; Copyright; Dedication; Contents; Figures; Tables; Acknowledgements; 1: Introduction; 1.1 Pseudo-random sequences; 1.2 LFSR sequences; 1.3 FCSR sequences; 1.4 Register synthesis; 1.5 Applications of pseudo-random sequences; 1.5.1 Frequency hopping spread spectrum; 1.5.2 Code division multiple access; 1.5.3 Optical CDMA; 1.5.4 Synchronization and radar; 1.5.5 Stream ciphers; 1.5.6 Pseudo-random arrays; 1.5.7 Monte Carlo; 1.5.8 Built in self test; 1.5.9 Wear leveling; Part I: Algebraically defined sequences; 2: Sequences; 2.1 Sequences and period 2.2 Fibonacci numbers2.3 Distinct sequences; 2.4 Sequence generators and models; 2.5 Exercises; 3: Linear feedback shift registers and linear recurrences; 3.1 Definitions; 3.2 Matrix description; 3.2.1 Companion matrix; 3.2.2 The period; 3.3 Initial loading; 3.4 Power series; 3.4.1

Definitions; 3.4.2 Recurrent sequences and the ring R0(x) of fractions; 3.4.3 Eventually periodic sequences and the ring E; 3.4.4 When R is a field; 3.4.5 R[[x]] as an inverse limit; 3.4.6 Reciprocal Laurent series; 3.5 Generating functions; 3.6 When the connection polynomial factors 3.7 Algebraic models and the ring R[x]/(q)3.7.1 Abstract representation; 3.7.2 Trace representation; 3.8 Families of recurring sequences and ideals; 3.8.1 Families of recurring sequences over a finite field; 3.8.2 Families of linearly recurring sequences over a ring; 3.9 Examples; 3.9.1 Shift registers over a field; 3.9.2 Fibonacci numbers; 3.10 Exercises; 4: Feedback with carry shift registers and multiply with carry sequences; 4.1 Definitions; 4.2 N-adic numbers; 4.2.1 Basic facts; 4.2.2 The ring QN; 4.2.3 The ring ZN,0; 4.2.4 ZN as an inverse limit; 4.2.5 Structure of ZN
4.3 Analysis of FCSRs4.4 Initial loading; 4.5 Representation of FCSR sequences; 4.6 Example: q=37; 4.7 Memory requirements; 4.8 Random number generation using MWC; 4.8.1 MWC generators; 4.8.2 Periodic states; 4.8.3 Memory requirements; 4.8.4 Finding good multipliers; 4.9 Exercises; 5: Algebraic feedback shift registers; 5.1 Definitions; 5.2 - adic numbers; 5.2.1 Construction of R; 5.2.2 Divisibility in R; 5.2.3 The example of d = N; 5.3 Properties of AFSRs; 5.4 Memory requirements; 5.4.1 AFSRs over number fields; 5.4.2 AFSRs over rational function fields
6.5 Elementary description of d-FCSR sequences

Sommario/riassunto

Pseudo-random sequences are essential ingredients of every modern digital communication system including cellular telephones, GPS, secure internet transactions and satellite imagery. Each application requires pseudo-random sequences with specific statistical properties. This book describes the design, mathematical analysis and implementation of pseudo-random sequences, particularly those generated by shift registers and related architectures such as feedback-with-carry shift registers. The earlier chapters may be used as a textbook in an advanced undergraduate mathematics course or a graduate electrical engineering course; the more advanced chapters provide a reference work for researchers in the field. Background material from algebra, beginning with elementary group theory, is provided in an appendix.