ALGEBRAIC SHIFT REGISTER SEQUENCES

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.

MARK GORESKY is a Member of the School of Mathematics in the Institute for Advanced Study at Princeton.

ANDREW KLAPPER is a Professor in the Department of Computer Science at the University of Kentucky, Lexington.

ALGEBRAIC SHIFT REGISTER SEQUENCES

MARK GORESKY
Institute for Advanced Study, Princeton

ANDREW KLAPPER
University of Kentucky

CAMBRIDGE
UNIVERSITY PRESS

CAMBRIDGE UNIVERSITY PRESS
Cambridge, New York, Melbourne, Madrid, Cape Town,
Singapore, São Paulo, Delhi, Tokyo, Mexico City

Cambridge University Press
The Edinburgh Building, Cambridge CB2 8RU, UK

Published in the United States of America by Cambridge University Press, New York

www.cambridge.org
Information on this title: www.cambridge.org/9781107014992

First published 2012

Printed in the United Kingdom at the University Press, Cambridge

A catalogue record for this publication is available from the British Library

ISBN 978-1-107-01499-2 Hardback

To Bob and Judy for their patience and support

Contents

Figures

Tables

Acknowledgements

The authors would like to thank Sergei Gelfand, the referees, and editors for their many valuable suggestions that have improved this book. Mark Goresky is grateful to the Defense Advanced Research Projects Agency for its support under grants no. HR0011-04-1-0031 and no. HR0011-09-1-0010. He also wishes to thank the Institute for Advanced Study for its support through grants from the Association of Members of the IAS, the Bell Companies Fellowship, the Charles Simonyi Endowment, and the Ambrose Monell Foundation.

Andrew Klapper thanks The Fields Institute at the University of Toronto, Princeton University, and The Institute for Advanced Study, where he was a visitor during part of the writing of this book. His participation in the writing of this book was partially supported by NSF grants CCF-0514660 and CCF-0914828, and by DARPA grant no. HR0011-04-1-0031.