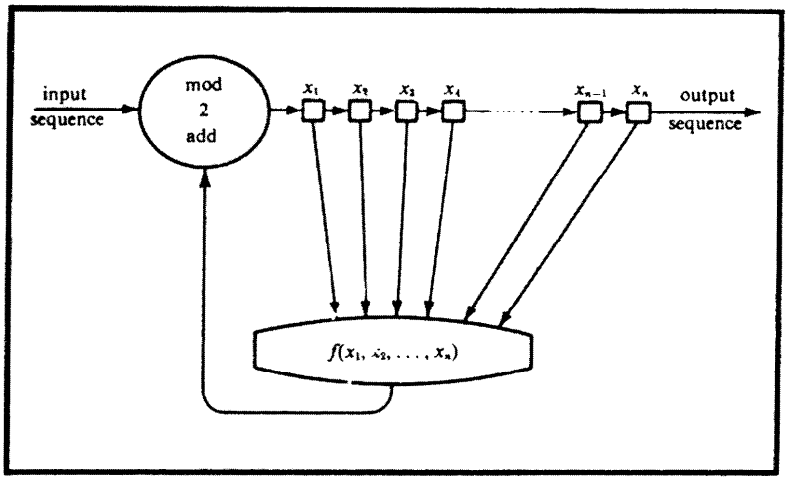
SHIFT REGISTER SEQUENCES

SECURE AND LIMITED-ACCESS CODE GENERATORS
EFFICIENCY CODE GENERATORS
PRESCRIBED PROPERTY GENERATORS
MATHEMATICAL MODELS



By SOLOMON W. GOLOMB

Aegean Park Press

SHIFT REGISTER SEQUENCES

Solomon W. Golomb
University of Southern California

With portions co-authored by

Lloyd R. Welch, Richard M. Goldstein,
and
Alfred W. Hales

ISBN: 0-89412-048-4

Aegean Park Press
P.O. Box 2120
Walnut Creek, California 94595
(800) 736-3587
(925) 947-2533
Fax (925) 947-2144
www.aegeanparkpress.com

Manufactured in the United States of America

PREFACE

The theory of shift register sequences has found major applications in a wide variety of technological situations, including secure, reliable and efficient communications, digital ranging and tracking systems, deterministic simulation of random processes, and computer sequencing and timing schemes. Yet this theory has been presented previously only in disjointed and scattered form, in a variety of out-of-print or otherwise inaccessible company reports, and in scattered journal articles. The purpose of this book is to collect and present in a single volume a thorough treatment of both the linear and nonlinear theory, with a guide to the area of application, and a full bibliography of the related literature.

From an engineering viewpoint, the theory of shift register sequences is very well worked out and fully ready for use. However, from a mathematical standpoint, there are certainly many unresolved problems worthy of further study.

I was first introduced to the problem of shift register sequences in 1954, while on a summer job with the Glenn L. Martin Company in Baltimore; and that was the beginning of a long friendship. My initial reaction was that the mathematics involved was extremely beautiful and that unfortunately the application was probably just shortlived and insignificant. Little did I realize then how important shift register techniques were destined to become in our technology.

I returned to Harvard in the fall, and I took advantage of being in Cambridge to pay frequent visits to Neal Zierler and others at the Lincoln Laboratory of M. I. T. who were similarly interested in shift registers. Finally, in June, 1955, I submitted my paper "Sequences with Randomness Properties," as the final progress report on my consulting contract with the Martin Co.

In the summer of 1956, I took a position at the Jet Propulsion Laboratory, where there was already considerable interest in shift register sequences. At JPL I worked both individually and in collabo-

ration with Lloyd Welch on these problems for several years, and a number of important reports were produced. The transfer of the JPL contract, in 1958, from Army Ordnance to NASA, meant a major redirection in the type of *applications* we sought for shift register sequences, but, as it turned out, the theoretical foundation was already almost complete. One of the many major applications of this work has been to a remarkably precise interplanetary-distance ranging system, which has been adopted by the Deep Space Network, operated by JPL for the Office of Tracking and Data Acquisition of NASA.

It is hard to establish accurate priorities as to who did what first. For example, E. N. Gilbert of the Bell Telephone Laboratories derived much of the linear theory a year or so earlier than either Zierler, Welch, or myself, but his memorandum had very limited distribution. Many others have rederived the linear theory independently since that time, and doubtless others will continue to do so. Of course, the first investigation of linear recurrence relations modulo p goes back as far as Lagrange, in the eighteenth century, and an excellent modern treatment was given (as a purely mathematical exposition) by Marshall Hall in 1937.

In assembling this volume, the procedure which I followed was to take the most important reports and articles of which I was an author or co-author, and edit them into a systematic exposition, with a reasonable continuity of both style and subject matter.

To preserve the historical flavor and continuity of the material, I have indicated the original publications from which the various papers were extracted, and in those relatively rare cases where the original version contained errors of fact or flaws in reasoning, I have not hesitated to correct them.

The two chapters which form Part One are chronologically the most recent. However, they are written from a tutorial standpoint, and thus serve to put the more technical material which follows into better perspective. Also, being more recently written, they give a more up-to-date indication of the place of shift register theory and applications in our current technology. Chapter II indicates the broader framework (namely, mathematical machine theory) within which shift registers are such an important special case.

Part Two deals with the linear theory. Although the term *linear* has been much overworked and abused, there is a reasonably consistent usage common to the terms *linear algebra, linear differential equations, linear operators, linear difference equations,* and *linear systems theory.* Moreover, there are a number of standard techniques for analyzing linear systems-matrix methods, operator methods, Laplace-Stieltjes transform methods, flow graph methods, impulse-response methods, etc.

All of these methods succeed in replacing a linear system by its "characteristic equation," and the behavior of the system is related to the factorization and the roots of the characteristic equation.

Linear shift registers are *linear* in this standardized sense. However, the underlying arithmetic is not that of the real or complex numbers, but of the field of two elements, 0 and 1, operating modulo 2. The analysis of linear shift register behavior, then, reduces to the study of their characteristic equations, which are polynomials with coefficients in the field of two elements.

In Chapter III, "Sequences with Randomness Properties," we start with certain desirable constraints on binary sequences, and are led to linear shift registers for the generation of such sequences. The analysis of linear shift registers uses the method recently popularized among electrical engineers under the name of the "Z-transform," and known to mathematicians since the late eighteenth century as the method of "generating functions." It would have been equally valid to use any of the other methods for analyzing linear systems, and there are articles by various authors which do so. In any case, the same theorems result, and the same correspondence between shift registers and polynomials occurs.

In Chapter IV, "Structural Properties of PN Sequences," we pay special attention to the correlation properties and spectra of shift register sequences. The correlation results provide a deeper insight into the behavior of the linear shift register sequences, and the spectral results are particularly important when the shift register sequence is used to modulate a radio signal.

Finally, in Chapter V, "Factorization of Trinomials over GF(2)," there is a detailed discussion of the theory of polynomial factorization over the field of two elements, with special emphasis on trinomials (i.e. three term polynomials), which correspond to the simplest shift registers to construct. Chapter V concludes with a factorization table for trinomials through degree 46.

Part Three deals with the nonlinear theory. The "nonlinear" case is, of course, the general case, in which almost anything can happen. Unlike the highly restricted "linear" case, where we developed the necessary analytical procedures to determine exact lengths of sequences, it is sufficiently ambitious in general to ask *qualitative* questions.

In Chapter VI, "Nonlinear Shift Register Sequences," we concern ourselves with such problems as when the state diagram has only "pure" cycles, without branches, and how often all the states lie on a single cycle. In the case of branchless cycles, a simple criterion is given for whether the total number of cycles is even or odd, and a number of important corollaries are deduced from this result.

In Chapter VII, "Cycles from Nonlinear Shift Registers," we develop a *statistical* model for the number of cycles, the expected lengths of the cycles, the probability that a given vector lies on the longest cycle, etc. Also, a construction is explained for obtaining cycles of any length from 1 to 2^n inclusive from a shift register of n stages.

A nonlinear shift register necessarily involves a Boolean function of n variables to compute the feedback term. We conclude the discussion of the nonlinear case with Chapter VIII, "On the Classification of Boolean Functions," which explains the reduction in the number of truly distinct cases which need to be considered, based on symmetry properties of the Boolean functions.

Not surprisingly, the nonlinear theory leaves many important questions as yet unanswered. However, the treatment presented here resolves most of the basic qualitative issues, and sets up procedural guidelines and methodology for further investigations.

PREFACE
TO THE REVISED EDITION

In the fifteen years since *Shift Register Sequences* was originally published in hard cover by Holden-Day, Inc., a great many developments have taken place. Far more is now known about both the theory and the applications of these sequences, and it would be a monumental undertaking to revise the book so as to reflect all of this. The present objective is more modest. There has been great demand for copies of the book since it went out of print, and even for the long-unobtainable Martin Co. and Jet Propulsion Laboratory reports which were reincarnated as some of its chapters. To fill this demand, the paperback edition faithfully reprints the original text, with two significant additions. One is a Comprehensive Bibliography with more than 400 entries, which gives the ambitious reader a head start on getting fully up to date in those areas in which he is most interested. The other is a new Chapter 9, titled *Selective Update*, which describes some of the most important recent developments involving topics which are already treated in the text. It is my hope to publish another volume, based on nine or ten of the most important papers which have appeared about shift register sequences since 1967, within the next two years.

I wish to express my gratitude to Wayne G. Barker, President of the Aegean Park Press, for his interest in publishing this edition, and for prodding me into doing the required work; and to Holden-Day, Inc., and its President, Fredrick H. Murphy, for the assignment of copyright from the original edition.

Solomon W. Golomb
Los Angeles, California
May 1, 1982