Golomb, Solomon W.

Shift register sequences. With portions co-authored by Lloyd R. Welch, Richard M. Goldstein and Alfred W. Hales. (English) Zbl 0267.94022

Holden-Day Series in Information Systems. San Francisco etc.: Holden-Day, Inc. xiv, 224 p. $ 12.00 (1967).

This is the first book devoted entirely to shift register sequences, which have found major applications in a wide variety of technological situations. The merit of the author is to collect results presented previously in inaccessible company reports, and in scattered Journal articles.

Chapter 1 gives the indication of the place of shift register theory and applications in current technology. Chapter 2 outlines the broader framework (namely, mathematical machines theory) in which shift registers are an important special case. Chapters 3, 4 and 5 deal with the linear theory. The analysis of linear shift register behaviour reduces to the study of their characteristic equations, which are polynomials with coefficients in the field of two elements. In the discussion of the linear theory the following subjects are given in detail: sequences with random properties, structural properties of maximum length, linear recurring sequences modulo, factorization of trinomials over GF(2).

Chapters 6, 7 and 8 deal with the nonlinear theory. The nonlinear case is, of course, the general case. The author's material on the nonlinear theory involves mathematical treatment of experimental results, tabulation on experimental results, tabulation on experimental data on nonlinear shift register sequences, also the cycle structure of nonlinear shift register sequences and the classification of Boolean functions are discussed in detail. The nonlinear theory leaves many important questions yet unanswered. The latter fact will stimulate some mathematicians to study shift register sequences.

Anyone who wishes to learn about the explosive new theory of shift register sequences is encouraged by the reviewer to start with this book as background.

Reviewer: József Dénes (Budapest)

MSC:

94A55	Shift register sequences and sequences over finite alphabets in information and communication theory
94-02	Research exposition (monographs, survey articles) pertaining to information and communication theory
94D10	Boolean functions
11T71	Algebraic coding theory; cryptography (number-theoretic aspects)

Keywords:

shift register sequences; linear shift register; sequences with random properties; structural properties of maximum length; linear recurring sequences modulo; factorization of trinomials over Galois Field; nonlinear shift register sequences; cycle structure; classification of Boolean functions