On Interval Linear Complexity of Binary Sequences *

Vladimir B. Balakirsky
Member, IEEE

The author is currently with the
Fakultät für Mathematik, Universität Bielefeld,
Postfach 100131, D-33501 Bielefeld 1, Germany
on leave from the Data Security Association "Confident",
193060 St.-Petersburg, Russia
E-mail addresses :
vbal@mathematik.uni-bielefeld.de
vbal@vbal.spb.su

Abstract. Some properties of the 'm-interval linear complexity profile', which can be used as a criterion characterizing the level of randomness of a given binary sequence, are examined.

Key words :
Sequences, Polynomials, Linear complexity

*The work was supported in part by SFB-343, Universität Bielefeld, Germany

1 Introduction

A well-known measure of linear complexity of binary sequences, which is based on the linear descriptions of subsequences of a given sequence that have increasing lengths, was introduced by R.Rueppel [1]. This measure is called the linear complexity profile (LCP) of the sequence and it can be used to characterize the 'level of randomness' of that sequence. Nevertheless, there are cases when the criterions based on LCPs are not quite satisfactory [1]-[6]. In this correspondence, we develop the ideas of [7], [8] and examine the linear descriptions of the fragments of a given sequence having a fixed length m and introduce a measure of linear complexity which we call the m-interval linear complexity profile (m-LCP). We assume that a comparison of the parameters of the m-LCP constructed for a given sequence and for fair coin-tossing sequences gives more information characterizing the closeness of the sequence to that class than the use of the LCP.

Our analysis widely uses the relationships between binary sequences and irreducible ratios of polynomials over $GF(2)$. The notation is introduced in Section 2. Some well-known properties of the LCP and the observation concerning the connections between the lengths of the linear feedback shift registers (LFSRs) and the degrees of the feedback polynomials used in the description are given in Section 3. The observation directly leads to an explicit formula for the number of irreducible ratios of polynomials over $GF(2)$ when the denominator has a fixed degree. This result should be known, but we cannot give the exact reference. A short proof of that formula and some discussion are given in Section 4. In Section 5 we define the m-LCP and show that it has a very regular properties for any sequence and that the formula for the number of irreducible ratios determines the statistical characteristics of the m-LCP of the fair coin tossing sequences.

2 Relationships Between Binary Sequences and Irreducible Ratios

We will denote by

$$f(z) = f_0 + f_1 \cdot z + ... + f_L \cdot z^L$$