SOME CONDITIONS ON THE LINEAR COMPLEXITY PROFILES OF CERTAIN BINARY SEQUENCES

Glyn Carter

Racal Comsec Ltd.
Milford Industrial Estate
Tollgate Road
Salisbury
Wiltshire, SP1 2JG
ENGLAND

ABSTRACT

In this paper we consider the binary sequences whose bits satisfy any set of linear equations from a wide class of sets, of which the equations in the perfect profile characterization theorem are typical. We show that the linear complexity profile any such sequence will be restricted in the sense that it will have no jumps of a certain parity above a certain height.

1. INTRODUCTION

The *linear complexity* of a binary sequence is the length of the shortest linear feedback shift register (LFSR) on which the sequence can be generated. There are two forms of linear complexity; *global linear complexity*, which applies to infinite periodic binary sequences, and *local linear complexity*, which applies to binary sequences of finite length. In this paper we will be interested in the latter.

Consider an n-bit sequence $s_0 s_1 \ldots s_{n-1}$. The local linear complexity $L(n)$ of $s_0 s_1 \ldots s_{n-1}$ and the connection polynomial

J.J. Quisquater and J. Vandewalle (Eds.): Advances in Cryptology - EUROCRYPT '89, LNCS 434, pp. 691-695, 1990.

$C_n(x)$ of an L(n)-stage LFSR on which the sequence can be generated can be computed using the Berlekamp-Massey algorithm [3]. The algorithm also yields, in the course of computing L(n), the local linear complexities L(1), L(2), ..., L(n-1) of the subsequences s_0, $s_0 s_1$, ..., $s_0 s_1 \ldots s_{n-2}$ of $s_0 s_1 \ldots s_{n-1}$. We call the n-vector (L(1),L(2),...,L(n-1),L(n)) the *linear complexity profile* of $s_0 s_1 \ldots s_{n-1}$, and we say that the profile *jumps* with s_{k-1} if L(k)-L(k-1) > 0. L(k)-L(k-1) is known as the *height* of the jump. From the Berlekamp-Massey algorithm it can be seen that a profile can only jump with s_{k-1} if $2.L(k-1) \leqslant k-1$, and that if it does jump then L(k) must be equal to k-L(k-1).

A sequence is said to have the *perfect linear complexity profile* if all the jumps in its linear complexity profile have height 1. In 1984 Rueppel conjectured in his thesis [5] that the sequence 110100010000000100... (i.e. the binary sequence such that $s_i = 1$ if and only if $i = 2^r - 1$ for some integer $r \geqslant 0$) has the perfect linear complexity profile. This conjecture was later proved to be true by Dai [2]. In 1986 Wang and Massey extended this result by characterizing the set of binary sequences having the perfect linear complexity profile; in [6] they showed that an n-bit sequence $s_0 s_1 \ldots s_{n-1}$ has the perfect profile if and only if $s_0 = 1$ and $s_{2i} = s_{2i-1} + s_{i-1}$ for $1 \leqslant i \leqslant \frac{n-1}{2}$. We will refer to this result as the *perfect profile characterization theorem.*

In this paper we will consider the binary sequences whose bits satisfy any set of linear equations from a wide class of sets, of which the equations in the perfect profile characterization theorem are typical. We will show that the linear complexity profile any such sequence will be constrained in some way.

2. MAIN RESULTS

We now move on to the main results of this paper. In the sequences in the perfect profile characterization theorem, every other bit is the sum of the preceding bit and a bit approximately "half way back". The results in this section involve sequences in which, roughly speaking, every other bit is the sum of a number of the preceding few bits and a number of bits

approximately "half way back". We can show that the linear complexity profile of any sequence of this type is restricted in the sense that it can have no jumps of a certain parity above a certain height. The proofs of these results are rather long, and unfortunately there is no room to include them in this paper. The interested reader is referred to [1].

We deal with the sequences in two groups, according to whether their "fixed" bits (i.e. the ones which can be expressed as a sum of previous bits) are the ones with odd or even indices. The results in the two cases are very similar; we separate them for clarity only. We begin by considering the sequences whose fixed bits have odd indices :-

Theorem 2.1.

Let $s_0 s_1 \ldots s_{n-1}$ be an n-bit sequence with

$$s_{2i+1-2w} = s_{2i+1-2x(1)} + s_{2i+1-2x(2)} + \ldots + s_{2i+1-2x(a)} + s_{2i-2y(1)} + s_{2i-2y(2)} + \ldots + s_{2i-2y(b)} + s_{i-z(1)} + s_{i-z(2)} + \ldots + s_{i-z(c)}$$

for $\min(w,z(1)) \leqslant i \leqslant \min(\frac{n}{2}+w-1, n+z(1)-1)$,

where $s_\ell := 0$ for $\ell < 0$

$(w < x(1) < x(2) < \ldots < x(a),\ w \leqslant y(1) < y(2) < \ldots < y(b),$
$z(1) < z(2) < \ldots < z(c),\ a \geqslant 0,\ b \geqslant 0,\ c > 0).$

Then the height j of any jump in the linear complexity profile of $s_0 s_1 \ldots s_{n-1}$ must satisfy either (i) or (ii) below :-

(i) j odd

(ii) $j \leqslant \max(2z(c)-2w, 2y(b)-2w+1, 2x(a)-2w)$

Proof

See [1].

□

We now deal with the sequences whose fixed bits have even indices :-

Theorem 2.2.

Let $s_0 s_1 \ldots s_{n-1}$ be an n-bit sequence with

$$s_{2i-2w} = s_{2i+1-2x(1)} + s_{2i+1-2x(2)} + \ldots + s_{2i+1-2x(a)} + s_{2i-2y(1)} + s_{2i-2y(2)} + \ldots + s_{2i-2y(b)} + s_{i-z(1)} + s_{i-z(2)} + \ldots + s_{i-z(c)}$$

$$\text{for } \min(w, z(1)) \leqslant i \leqslant \min(\tfrac{n-1}{2}+w, n+z(1)-1),$$

where $s_\ell := 0$ for $\ell < 0$

$$(w < x(1) < x(2) < \ldots < x(a),\ w < y(1) < y(2) < \ldots < y(b),$$
$$z(1) < z(2) < \ldots < z(c),\ a \geqslant 0,\ b \geqslant 0,\ c > 0).$$

Then the height j of any jump in the linear complexity profile of $s_0 s_1 \ldots s_{n-1}$ must satisfy either (i) or (ii) below :-

(i) j even

(ii) $j \leqslant \max(2z(c)-2w-1, 2y(b)-2w, 2x(a)-2w-1)$

Proof

See [1].

□

As an example of how these results can be applied to a sequence whose bits satisfy a particular set of linear equations, consider an n-bit sequence $s_0 s_1 \ldots s_{n-1}$ whose bits satisfy the following equations :-

$$s_1 = 0$$
$$s_3 = s_2 + s_1$$
$$s_{2i+1} = s_{2i} + s_{2i-2} + s_i + s_{i-1} \quad \text{for } 2 \leqslant i \leqslant \tfrac{n}{2}-1$$

By Theorem 2.1, the linear complexity profile of $s_0 s_1 \ldots s_{n-1}$ can have no jumps of even height greater than 2.

The above theory yields a large class of sequences in which non-randomness in the sequences is reflected in their linear complexity profiles. Empirical tests suggest that, in many cases, such non-randomness would not be identified by established statistical tests; it would in most cases, however, be identified by statistical tests based on linear complexity profiles (see [1] and [4]).

REFERENCES

[1] **Carter, G.D.**, *'Aspects of Local Linear Complexity'*, Ph.D. Thesis, University of London, (1988).

[2] **Dai, Z.D.**, 'Proof of Rueppel's linear complexity conjecture'. To appear.

[3] **Massey, J.L.**, 'Shift register synthesis and BCH decoding', *IEEE Transactions on Information Theory*, **IT-15**, (1969), pp 122-127.

[4] **Niederreiter, H.**, 'The probabilistic theory of linear complexity', *Advances in Cryptology: Proceedings of Eurocrypt 88*, Springer-Verlag, Berlin, (1988), pp 191-209.

[5] **Rueppel, R.A.**, *'New Approaches to Stream Ciphers'*, D.Sc. Dissertation, Swiss Federal Institute of Technology, Zurich, (1984).

[6] **Wang, M.Z. and Massey, J.L.**, 'The characterization of all binary sequences with perfect linear complexity profiles'. Presented at Eurocrypt 86.