On The Quadratic Feedback Shift Registers

Ali Doğanaksoy and Elif Saygı

Department of Mathematics and Institute of Applied Mathematics,

Middle East Technical University

Outline

- Introduction and definitions
- Quadratic Maximum Length Sequences
- De Bruijn Sequences
- Quadratic Span Profile of Sequences
- Conclusion and Future Studies

Introduction and definitions

- In many fields, such as mathematics, computer science, communication, cryptography,networks etc., binary sequences are used extensively. A common way of producing such a sequence is employing a feedback shift register (FSR).
- It turns out to be an important problem to examine the properties of sequences produced by FSRs, and as a consequence, FSRs have been widely studied in the literature .

Introduction and definitions

- A FSR of length n consist of a pair (F; f) where f is a Boolean function defined on n variables and F is an n-tuple valued function also defined on n variables by setting

$F(x_1, x_2, ..., x_n) = (x_2,... , x_n; f(x_1, x_2, ..., x_n))$.

  - F, in fact describes how to obtain the new state from the previous states and thus, called the **next-state function**.

  - f is used to define the nth term of the new state and is called the **feedback function**.

Introduction and definitions

- Starting from an initial state $(s_1, s_2, \ldots, s_n)$, we obtain a sequence of states:

$F(s_1, s_2, \ldots, s_n) = (s_2, \ldots, s_n , s_{n+1})$,

$F(s_2, \ldots, s_{n+1}) = (s_3, \ldots, s_{n+1} , s_{n+2})$, ...

Then, by definition, the binary sequence produced by FSR is $s_1, s_2, \ldots, s_n , s_{n+1} \ldots$

Introduction and definitions

- **Span** of sequence s is the length of shortest FSR (not necessarily unique) which produces s.
- In many situations a FSR is not allowed to reach the all 0 state and in such a case the output sequence has period at most 2^{n-1} .

Introduction and definitions

- A binary sequence of span n is called a maximal length sequence (**m-sequence**) if its period (or length) is 2^{n-1}.
- If the feedback function f of a FSR is a linear (resp. quadratic) function we call the FSR a linear feedback shift register (**LFSR**) (resp. a quadratic feedback shift register (**QFSR**)).
- Length of shortest LFSR (resp. QFSR) that produces a sequence s is called the **linear span** (resp. **Quadratic span**) or the linear complexity of s.

Introduction and definitions

- If a sequence s has a linear span L, then only 2L terms are sufficient to determine the LFSR which produces s.
- The linear span of a sequence of length n can be determined by using Berlekamp-Massey algorithm in a running time $O(n^2)$.

Introduction and definitions

- Therefore for cryptographic applications only sequences having high linear spans are used.
- On the other hand, a sequence with a large linear span may be generated by a much shorter FSR .
- However, for a general nonlinear feedback function, efficiently determining the span and an associated feedback function is difficult because of the nonlinearities involved.

Introduction and definitions

- The feedback function of a QFSR can be represented as follows:

$$f(x_1, x_2, \ldots, x_n) = \sum_{1 \leq i \leq n} a_i x_i + \sum_{1 \leq i < j \leq n} a_{ij} x_i x_j.$$

Quadratic Maximum Length Sequences

- Here we mention some necessary conditions to generate quadratic m-sequences.

- For a FSR if the initial state is never repeated, the cycle of states generated is said to have **branch point**, that is, for some different states S_1 and S_2 , we have $F(S_1) = F(S_2)$.

Quadratic Maximum Length Sequences

- **Theorem 1** : A sequence have no branch point if and only if the next state function F is one to one.
- **Theorem 2** : A next state function F is one to one if and only if $\deg_f (x_1) = 1$.
- **Corollary 1** : Let f be a feedback function that generates a quadratic m-sequence then, $\deg_f (x_1) = 1$.

  Note that, $\deg_f (x_1) = 1$ means that f is of the form $f = x_1 + g$ where g is a Boolean function which does not depend on x_1.

Quadratic Maximum Length Sequences

- **Proposition 1**: Let $f = x_1 + g$ be a quadratic feedback function which generates an m- sequence. Then,
  - i. Number of linear terms in g and number of quadratic terms in g are not equal in modulo 2.
  - ii. There is at least one linear term in g.
  - iii. The function $f'(x_1, x_2, \ldots, x_n) = f(x_1, x_n, \ldots, x_2)$ also generates a quadratic m-sequence;

    namely the reverse of the sequence generated by f.

De Bruijn Sequences

- **Definition 1**: If the period of the output sequence of a FSR of length n is 2^n, then the output sequence is called a de Bruijn sequence.

It is well known that the number of all de Bruijn sequences generated by FSRs of span n is

$$2^{2^{n-1}-n}$$

De Bruijn Sequences

- A sequence generated by a FSR of span n can have period 2^{n-1} , therefore a trivial lower bound for the quadratic span of a de Bruijn sequence of span n is n + 1.

  It was conjectured that the quadratic span of a de Bruijn sequence of span n is at least n + 2 for n > 3.

De Bruijn Sequences

- The following theorems by Chan and Games gives an upper bound on the quadratic span of a de Bruijn sequence of span n and it is shown that this bound is attained by the class of de Bruijn sequences obtained from m- sequences.

De Bruijn Sequences

- **Theorem 3** : If s is a de Bruijn sequence of span n≥ 3, then the quadratic span of s is bounded above by $2^n - \binom{n}{2} - 1.$

- **Theorem 4**: Let s be a de Bruijn sequence of span n obtained from an m-sequence of span n by adding the zero n-tuple. Then the quadratic span of s is equal to $2^n - \binom{n}{2} - 1.$

Quadratic Span Profile of Sequences

- Youssef and Gong proved the following theorem that gives a partial answer to the changes in the quadratic span profile of a binary sequence.
- **Theorem 5** : Let $s = (s_1 , \ldots , s_m)$ be a binary sequence of length m and let the quadratic span of the sequence $s_k = (s_1, \ldots , s_k)$ be denoted by n_k, where $1 < k < m$. If $n_k > k / 2$, then $n_{k+1} = n_k$ that is the quadratic span remains unchanged.

Quadratic Span Profile of Sequences

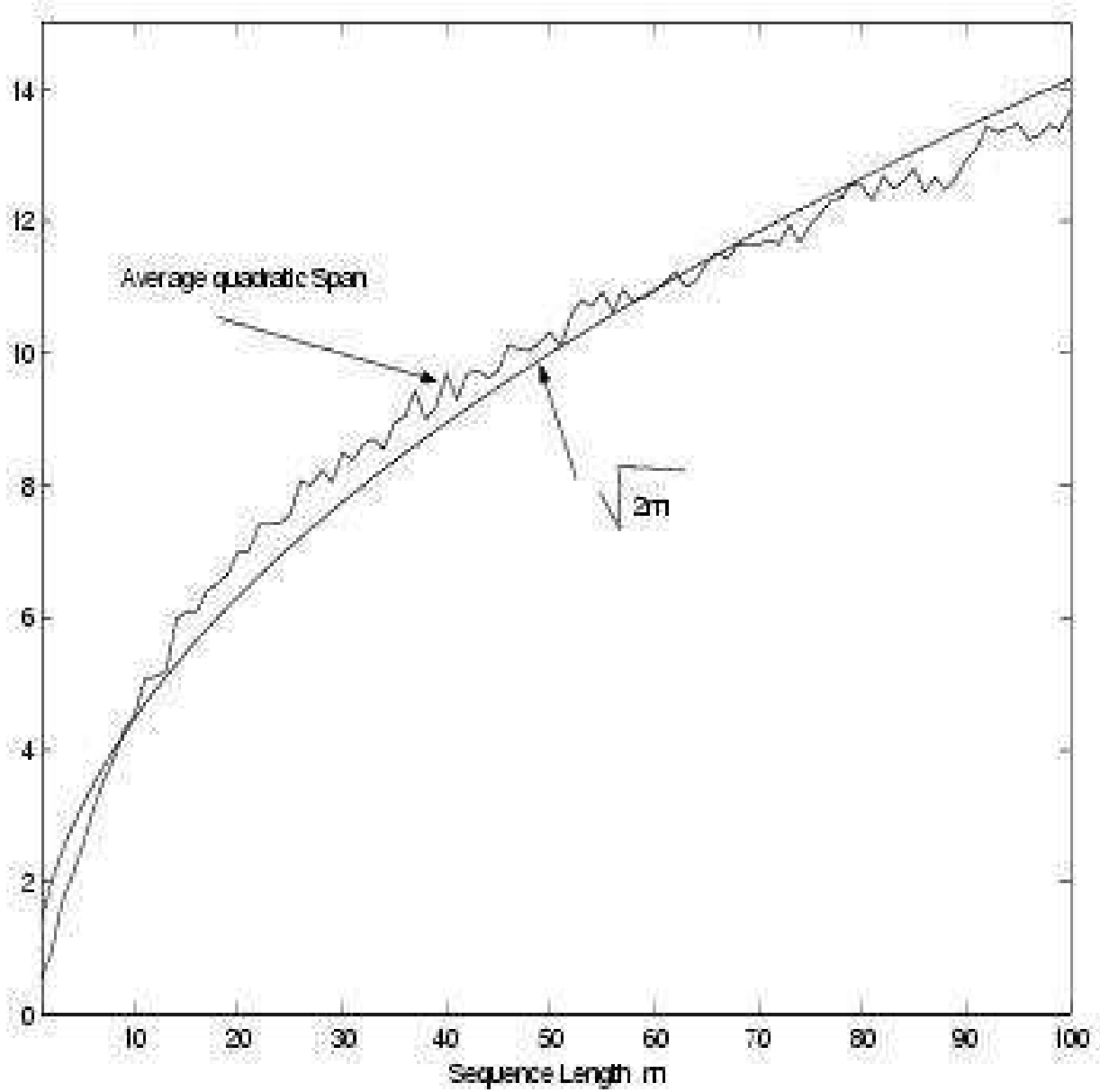
- Here given two conjectures which are supported by experimental results.
- **Conjecture 1** : Let $N_m(n)$ be the number of binary sequences of length m and quadratic span n > m / 2. Then $N_m(n)$ is a function of the difference (m-n) only, that is,

$$N_m(n) = N_{m+i}(n+i).$$

Quadratic Span Profile of Sequences

- Experimental average value of the quadratic span of randomly selected sequences of length $1 \leq m \leq 100$ is given in the following figure.

Quadratic Span Profile of Sequences



Quadratic Span Profile of Sequences

- **Conjecture 2**: For moderately large m, the expected value of the quadratic span of a random sequence of length m is given by

$$E(n_m) \approx \sqrt{2m}.$$

- Note that for moderately large m, the expected value of the linear span of a random sequence of length m is given by ≈ m / 2 and the expected value of the span is given by ≈ 2 $\log_2$ (m).

Conclusion and Future Studies

- In this paper, the properties of sequences that are generated from quadratic feedback shift registers are surveyed. Moreover some examples having large linear span but less quadratic span are given. Also some properties of the de Bruijn sequences are presented.

- For our future studies, we want to find new properties of quadratic m-sequences produced by FSRs. Furthermore, we want to investigate new methods to determine the quadratic span of a given sequence.

Thank you …

Questions?