Enumeration Results on the Linear Complexity of Sequences

Ramakanth Kavuluru

Department of Computer Science
University of Kentucky

Graduate Student Combinatorics Conference 2009
Outline

1 Preliminaries
- LFSRs and Linear Complexity
- $k$-Error Linear Complexity

2 Counting Functions for $k$-Error Linear Complexity
- $2^n$-Periodic Binary Sequences
- Notation and Auxiliary Results
- Counting Functions

3 Concluding Remarks
Definition of LFSRs

\[ g_i, a_j \in \mathbb{F}_q, \text{ field} \]

\[ s_r = g_1 s_{r-1} + \cdots + g_r s_0 \]

Output \( S = s_0, s_1, \cdots, s_{r-1}, s_r, s_{r+1}, \cdots \)

Analysis:

- generating function \( \sum_i s_i x^i \)
- connection polynomial \( g(x) = -1 + g_1 x + g_2 x^2 + \cdots + g_r x^r \)
Properties of LFSRs

LFSR sequences are eventually periodic.

The generating function of LFSR sequences is rational

\[ \sum_{i=0}^{\infty} s_i x^i = \frac{u(x)}{g(x)}, \quad u(x), g(x) \in \mathbb{F}_q[x] \]

- S periodic iff \( \deg(u(x)) < \deg(g(x)) \)

- If \( \gcd(u(x), g(x)) = 1 \) period is the smallest \( T \) such that \( g(x) | x^T - 1 \).

- m-sequence: If \( g(x) \) primitive, period = \( q^r - 1 \)

- m-sequences: uniform – each nonzero \( r \)-tuple occurs once
Linear Complexity

**Definition**

The linear complexity $L(S)$ of a sequence $S = (s_0, s_1, \cdots)$ over $\mathbb{F}_q$ is the length of smallest LFSR that can generate $S$.

The generating function

$$
\sum_{i=0}^{\infty} s_i x^i = \frac{u(x)}{g(x)}, \quad \gcd(u(x), g(x)) = 1.
$$

- Linear complexity $L(S) = \max(\deg(u(x)) + 1, \deg(g(x)))$
- $g(x)$ - minimal connection polynomial.
- If purely periodic then $L(S) = \deg(g(x))$
- Shift register synthesis: Berlekamp-Massey algorithm.
**n-th Linear Complexity and k-error Linear Complexity**

- Every sequence prefix should have high linear complexity
- Linear complexity should not decrease with few changes

**Definition (Rueppel)**

The \( n \)-th linear complexity \( L^n(S) \) of \( S \) is the length of the shortest LFSR whose first \( n \) terms are \( s_0, s_2, \ldots, s_{n-1} \).

**Example 1**: Let \( S = (0, \cdot \cdot \cdot, 0, 1) \) with \( T - 1 \) zeroes and a 1. Then \( L(S) = T \) but \( L^n(S) = 0 \), for \( n = 1 \cdot \cdot \cdot T - 1 \)

**Definition (Ding)**

The \( k \)-error \( n \)-th linear complexity \( L^n_k(S) \) is the least linear complexity obtained by making at most \( k \) changes in the first \( n \) terms of \( S \).

**Example 2**: With \( S \) as in Example 1, \( L^T_1(S) = 0 \)
Let $S$ be a $2^n$-periodic binary sequence for the rest of the talk

$L_k(S)$ - $k$-error linear complexity of $S$ (upto $k$ changes per period)

Let $S(x) = s_0 + s_1x + \cdots + s_{2^n-1}x^{2^n-1}$. Then

$$
\sum_{i=0}^{\infty} s_i x^i = \frac{S(x)}{1 - x^{2^n}} = \frac{S(x)}{(1 - x)^{2^n}}
$$

$$
L(S) = 2^n - \deg(\gcd(S(x), (1 - x)^{2^n}))
$$

and

$$
S(x) = (1 - x)^{2^n - L(S)} a(x), \text{ for some } a(1) = 1.
$$
The Problem

\( \mathcal{A}(L) \) - The set of \( 2^n \)-periodic binary sequences \( S \) with \( L(S) = L \).

\( \mathcal{A}_k(L) \) - The set of \( 2^n \)-periodic binary sequences \( S \) with \( L_k(S) = L \).

For a given \( S \in \mathcal{A}(L) \)

- minimal connection polynomial is \( (1 - x)^L \)

- \( S(x) = (1 - x)^{2^n - L} a(x) \), for some \( a(x) \), \( a(1) = 1 \)

Thus \( |\mathcal{A}(L)| = 2^{L-1} \).
\( A(L) \) - The set of \( 2^n \)-periodic binary sequences \( S \) with \( L(S) = L \).

\( A_k(L) \) - The set of \( 2^n \)-periodic binary sequences \( S \) with \( L_k(S) = L \).

For a given \( S \in A(L) \)

- minimal connection polynomial is \((1 - x)^L\)
- \( S(x) = (1 - x)^{2^n-L}a(x) \), for some \( a(x), a(1) = 1 \)

Thus \(|A(L)| = 2^{L-1} \).

Problem: characterize and count \( A_k(L) \) for \( k = 1, 2, 3 \).
Approach to Characterize $\mathcal{A}_k(L)$

1. Derive some useful properties of $\mathcal{A}(L)$ and $L_k(S)$.
2. Use them to characterize and count sequences in $\mathcal{A}_k(L)$.

More notation:

$$E_{i_1,\ldots,i_l} = \{(e_0, \ldots, e_{2^n-1})^\infty : e_l = 1, l = i_1, \ldots, i_l; e_l = 0 \text{ otherwise}\}.$$ 

$$\mathcal{E}_I = \{E_{i_1,\ldots,i_l} : 0 \leq i_1 < \cdots < i_l \leq 2^n - 1\}.$$ 

$\mathcal{A}(L) + R = \{S + R : S \in \mathcal{A}(L)\}$, where $R$ is any sequence.

$\mathcal{A}(L)[\mathcal{R}]$ - The set of sets $\{\mathcal{A}(L) + R : R \in \mathcal{R}\}$, where $\mathcal{R}$ is a set of sequences

**Idea:** If $S \in \mathcal{A}(L) + E$, $w_H(E) = 0, \ldots, k$, then is $S \in \mathcal{A}_k(L)$?
A Useful Result

**Proposition (Kurosawa et al)**

For a $2^n$-periodic binary sequence $S$ the **minimum** number of changes required to **lower** the linear complexity of $S$ is $\text{merr}(S) = 2^w_H(2^n - L(S))$.

For a given $2^n$-periodic sequence $S$

1. $L(S) = 2^n$ if and only if $w_H(s_0, \ldots, s_{2^n-1})$ is odd
2. So $L_1(S) < L(S)$ if and only if $L(S) = 2^n$
3. If $L(S) = 2^n$, then $L_2(S) = L_1(S) < L(S)$

We have

$$\mathcal{A}_2(0) = \mathbb{E}_1 \cup \mathbb{E}_2 \cup \{0\} \quad \text{and} \quad |\mathcal{A}_2(0)| = \binom{2^n}{2} + 2^n + 1,$$

and

$$(2) \implies \mathcal{A}_2(2^n) = \emptyset \quad \text{and} \quad |\mathcal{A}_2(2^n)| = 0.$$

Ramakanth Kavuluru (Univ. of Kentucky)  Linear Complexity of Sequences  GSCC 2009, Lexington
\( A_2(L) \) When \( L = 2^n - 2^t \)

**Proposition (Meidl)**

For any \( 2^n \)-periodic binary sequence \( S \) and for \( k \geq 2 \), \( L_k(S) \) is different from \( 2^n - 2^t \) for every integer \( t \) with \( 0 \leq t < n \).

Proposition \( \implies A_2(L) = \emptyset \) for \( L = 2^n - 2^t \), \( 0 \leq t < n \)

Already handled cases when \( w_H(2^n - L) = 0 \) or \( 1 \)
For any $2^n$-periodic binary sequence $S$ and for $k \geq 2$, $L_k(S)$ is different from $2^n - 2^t$ for every integer $t$ with $0 \leq t < n$.

Proposition $\Rightarrow A_2(L) = \emptyset$ for $L = 2^n - 2^t$, $0 \leq t < n$

Already handled cases when $w_H(2^n - L) = 0$ or $1$

We have two more cases:

1. $w_H(2^n - L) = 2$, that is, $L = 2^n - (2^{n-r_1} + 2^{n-r_2})$
2. $w_H(2^n - L) \geq 3$

For the rest of the talk: $w_H(2^n - L) \geq 3$
Theorem 1

Let $S$ be a $T$-periodic binary sequence. Consider any two positive integers $u$, $v$ such that $0 \leq v \leq u$ and $u + v < merr(S)$. Then for any $T$-periodic binary sequence $E$ such that $w_H(E) = v$ we have

$$L_u(S + E) = L(S).$$
Characterization When $w_H(2^n - L) \geq 3$

**Theorem 1**

Let $S$ be a $T$-periodic binary sequence. Consider any two positive integers $u$, $v$ such that $0 \leq v \leq u$ and $u + v < merr(S)$. Then for any $T$-periodic binary sequence $E$ such that $w_H(E) = v$ we have

$$L_u(S + E) = L(S).$$

**Theorem 2**

If $w_H(2^n - L) \geq 3$, then

$$A_2(L) = A(L) \cup \left( \bigcup_{E_i \in E_1} (A(L) + E_i) \right) \cup \left( \bigcup_{E_{i,j} \in E_2} (A(L) + E_{i,j}) \right).$$
\( A_2(L) \) and \( |A_2(L)| \) When \( 0 < L < 2^{n-2} \)

**Theorem 3**

For a given \( r \in \{1, \cdots, n-1\} \), let \( 1 \leq L < 2^{n-r} \). Then for any two distinct sequences \( S, S' \in A(L) \) we have \( d_H(S, S') = t \cdot 2^{r+1} \) for some \( t \in \{1, 2, 3, \cdots, 2^{n-r-1}\} \), which implies

\[
d_H(S, S') \geq 2^{r+1}.
\]
Theorem 3

For a given \( r \in \{1, \cdots, n - 1\} \), let \( 1 \leq L < 2^{n-r} \). Then for any two distinct sequences \( S, S' \in A(L) \) we have \( d_H(S, S') = t \cdot 2^{r+1} \) for some \( t \in \{1, 2, 3, \cdots, 2^{n-r-1}\} \), which implies

\[
d_H(S, S') \geq 2^{r+1}.
\]

Theorem 4

If \( w_H(2^n - L) \geq 3 \) and \( 1 \leq L < 2^{n-2} \), then the sets \( A(L), A(L) + E_i, E_i \in E_1 \), and \( A(L) + E_{i,j}, E_{i,j} \in E_2 \), are disjoint. Furthermore,

\[
|A_2(L)| = \left( \binom{2^n}{2} + 2^n + 1 \right) 2^{L-1}.
\]
For any $S \in A(L)$, where $2^n - 2^{n-r} < L < 2^n - 2^{n-r-1}$ for some $1 \leq r \leq n-2$, and for any $0 \leq i \leq 2^n - 1$, the number of sequences $S + E_{i,j} \in A(L)$, where $j \neq i$, is exactly $2^r - 1$ corresponding to all $j \in \{i \oplus t2^{n-r} : 1 \leq t \leq 2^r - 1\}$. 
Cardinality of $\mathcal{A}(L)[E_1]$ When $2^{n-2} < L < 2^n - 3$

**Theorem 5 (Fu et al.)**

For any $S \in \mathcal{A}(L)$, where $2^n - 2^{n-r} < L < 2^n - 2^{n-r-1}$ for some $1 \leq r \leq n - 2$, and for any $0 \leq i \leq 2^n - 1$, the number of sequences $S + E_{i,j} \in \mathcal{A}(L)$, where $j \neq i$, is exactly $2^r - 1$ corresponding to all $j \in \{i \oplus t2^{n-r} : 1 \leq t \leq 2^r - 1\}$.

For any $L$ where $w_H(2^n - L) \geq 3$ we have unique $1 \leq r_1 \leq r_2$ such that

$$2^n - (2^{n-r_1} + 2^{n-r_2}) < L < 2^n - (2^{n-r_1} + 2^{n-r_2-1}),$$

which implies $2^n - 2^{n-r_1+1} < L < 2^n - 2^{n-r_1}$. 
Cardinality of $\mathcal{A}(L)[E_1]$ When $2^{n-2} < L < 2^n - 3$

**Theorem 5 (Fu et al.)**

For any $S \in \mathcal{A}(L)$, where $2^n - 2^{n-r} < L < 2^n - 2^{n-r-1}$ for some $1 \leq r \leq n - 2$, and for any $0 \leq i \leq 2^n - 1$, the number of sequences $S + E_{i,j} \in \mathcal{A}(L)$, where $j \neq i$, is exactly $2^r - 1$ corresponding to all $j \in \{i \oplus t2^{n-r} : 1 \leq t \leq 2^r - 1\}$.

For any $L$ where $w_H(2^n - L) \geq 3$ we have unique $1 \leq r_1 \leq r_2$ such that

$$2^n - (2^{n-r_1} + 2^{n-r_2}) < L < 2^n - (2^{n-r_1} + 2^{n-r_2-1}),$$

which implies $2^n - 2^{n-r_1+1} < L < 2^n - 2^{n-r_1}$.

Theorem 5 $\implies (\mathcal{A}(L) + E_u) \cap (\mathcal{A}(L) + E_v) = \emptyset$, $0 \leq u < v \leq 2^{n-r_1+1} - 1$.

Also, for each $u = 0, \cdots, 2^{n-r_1+1} - 1$,

$$\mathcal{A}(L) + E_u = \mathcal{A}(L) + E_{u+t2^{n-r_1+1}}, \quad t = 0, \cdots, 2^{r_1-1} - 1.$$

Thus $|\mathcal{A}(L)[E_1]| = 2^{n-r_1+1}$. 

Ramakanth Kavuluru (Univ. of Kentucky)
Linear Complexity of Sequences
GSCC 2009, Lexington 14 / 18
Theorem 6

Let \( S \in \mathcal{A}(L) \) where \( 2^n - (2^{n-r_1} + 2^{n-r_2}) < L < 2^n - (2^{n-r_1} + 2^{n-r_2-1}) \), for some \( r_1, r_2 \in \{2, \cdots, n-1\} \) satisfying \( 1 < r_1 \leq r_2 \) or \( 1 = r_1 < r_2 \). We have the following two results.

1. Consider any four integers \( i, j, k, \) and \( l \) such that \( 0 \leq i < j < k < l \leq 2^{n-r_1+1} - 1 \). Then \( L(S + E_{i,j,k,l}) = L(S) \) if and only if \( i, j, k, \) and \( l \) are in the form

\[
i = u + g_1 2^{n-r_2}, \quad j = u + g_2 2^{n-r_2}, \quad k = i + 2^{n-r_1}, \quad \text{and} \quad l = j + 2^{n-r_1},
\]

where \( 0 \leq u \leq 2^{n-r_2} - 1 \) and \( 1 \leq g_1 < g_2 \leq 2^{r_2-r_1} - 1 \).

2. There do not exist integers \( i_1, \cdots, i_6 \) such that

\[
0 \leq i_1 < \cdots < i_6 \leq 2^{n-r_1+1} - 1 \quad \text{and} \quad L(S + E_{i_1, \cdots, i_6}) = L(S).
\]
We only need to find \(|\mathcal{A}(L)[\mathbb{E}_2]|, \mathbb{D}_2(L) = \{E_{i,j} : 0 \leq i < j \leq 2^{n-r_1+1} - 1\}. \\

For all settings of \(i\) and \(j\) in part 1 of Theorem 6 we have set equalities

\[
\mathcal{A}(L) + E_{i,j} = \mathcal{A}(L) + E_{i+2^{n-r_1},j+2^{n-r_1}},
\]

\[
\mathcal{A}(L) + E_{i,j+2^{n-r_1}} = \mathcal{A}(L) + E_{i+2^{n-r_1},j},
\]

resulting in \(2 \cdot 2^{n-r_2} \binom{2^{r_2-r_1}}{2}\) doubly counted sets.

Also, for each \(u = 0, \ldots, 2^{n-r_2} - 1\), we have \(2^{r_2-r_1} - 1\) set equalities

\[
\mathcal{A}(L) + E_{u,u+2^{n-r_1}} = \mathcal{A}(L) + E_{i,i+2^{n-r_1}}, \quad \text{where} \quad i = u + t2^{n-r_2}
\]

for \(1 \leq t \leq 2^{r_2-r_1} - 1\), resulting in \(2^{n-r_2}(2^{r_2-r_1} - 1)\) doubly counted sets.

Thus \(|\mathcal{A}(L)[\mathbb{F}_2]| = |\mathcal{A}(L)[\mathbb{D}_2(L)]| = \binom{2^{n-r_1+1}}{2} - 2^{n-r_2} \left(2^{r_2-r_1} + 2\binom{2^{r_2-r_1}}{2}\right).\)
\( A_2(L) \) and \(|A_2(L)|\) When \( 2^{n-2} < L < 2^n - 3 \)

**Theorem 7**

Let \( w_H(2^n - L) \geq 3 \) where \( 2^n - (2^{n-r_1} + 2^{n-r_2}) < L < 2^n - (2^{n-r_1} + 2^{n-r_2-1}) \) for some \( r_1, r_2 \) satisfying \( 1 < r_1 \leq r_2 \leq n - 1 \). Define the sets

\[
D_1(L) = \{E_i : 0 \leq i < 2^{n-r_1+1}\} \quad \text{and} \quad D_2(L) = \{E_{i,j} : 0 \leq i < j < 2^{n-r_1+1}\}.
\]

For \( u = 0, \cdots, 2^{n-r_2} - 1 \) define the sets

\[
D_{1u}^1(L) = \{E_{i,i+2^{n-r_1}} : i = u + t2^{n-r_2}, 1 \leq t \leq 2^{r_2-r_1} - 1\},
\]

\[
D_{2u}^2(L) = \{E_{i,j}, E_{i,j+2^{n-r_1}} : i = u + t_12^{n-r_2}, j = u + t_22^{n-r_2}, 0 \leq t_1 < t_2 \leq 2^{r_2-r_1} - 1\}.
\]

Consider the set \( D(L) = D_2(L) - \bigcup_{u=0}^{2^{n-r_2}-1}(D_{1u}^1(L) \cup D_{2u}^2(L)) \). Then the sets \( A(L), A(L) + E_i, E_i \in D_1(L) \), and \( A(L) + E_{i,j}, E_{i,j} \in D(L) \), are disjoint. Furthermore,

\[
|A_2(L)| = \left(\binom{2^{n-r_1+1}}{2} - 2^{n-r_2}(2^{2r_2-2r_1} - 1) + 2^{n-r_1+1} + 1\right)2^{L-1}.
\]
1. These results were presented at SETA 2008. Full results including cases \( w_H(2^n - L) = 2 \) and when \( k = 3 \) are submitted to *Designs, Codes, and Cryptography*.

2. Similar approach can be used for \( p^n \)-periodic sequences over \( \mathbb{F}_p \).

3. Results for arbitrary periods or for periods of other forms are desirable.

4. Counting functions can also be considered for
   - Periodic and finite length multisequences
   - Complexity measures based on nonlinear feedback shift registers (FCSRs, AFSRs, and general NLFSRs)