Joint Linear Complexity of Multisequences Consisting of Linear Recurring Sequences

Fang-Wei Fu

Chern Institute of Mathematics, Nankai University, Tianjin, China

15 February 2011, NTU, Singapore

Joint Work with Harald Niederreiter and Ferruh Özbudak

Contents

- Introduction
- Linear Recurring Sequences and Linear Complexity
- Multiple Linear Recurring Sequences and Joint Linear Complexity
- Expectation and Variance
- Counting Function and Generating Polynomial

Introduction

- The linear complexity of sequences is one of the important security measures for stream cipher systems.
- Rueppel 1986, 1992
- Ding, Xiao, Shan 1991
- Cusick, Ding, Renvall 1998
- Niederreiter 2003

Introduction

- High linear complexity to resist an attack by the Berlekamp-Massey algorithm.
- A stream cipher system is completely secure if the keystream is a "truly random" sequence that is uniformly distributed.
- Fundamental research problem:
  Determine the expectation and variance of the linear complexity of random sequences that are uniformly distributed.

Introduction

- Study of word-based or vectorized stream cipher systems
- Study of joint linear complexity of multisequences
- Research works on the study of expectation and variance and counting function for
- linear complexity of random finite/periodic sequences: Rueppel, Dai, Meidl, Niederreiter, et al
- joint linear complexity of random finite/periodic multisequences: Meidl, Niederreiter, Dai, Xing, Fu, Su, Wang, et al

Linear Recurring Sequences and Linear Complexity

- A sequence $\sigma = (s_n)_{n=0}^{\infty}$ of elements of $\mathbb{F}_q$ is called a *linear recurring sequence* over $\mathbb{F}_q$ with characteristic polynomial

$$\sum_{i=0}^{\ell} a_i x^i \in \mathbb{F}_q[x]$$

if $a_\ell = 1$ and

$$\sum_{i=0}^{\ell} a_i s_{n+i} = 0 \qquad \text{for} \quad n = 0, 1, \ldots .$$

Here ℓ is an arbitrary nonnegative integer.

Linear Recurring Sequences and Linear Complexity

- The minimal polynomial of σ is the uniquely determined characteristic polynomial of σ with least degree.
- The linear complexity of σ is the degree of the minimal polynomial of σ.

Multiple Sequences and Joint Linear Complexity

- m: an arbitrary positive integer.
- m-fold multisequence $\mathbf{S} = (\sigma_1, \ldots, \sigma_m)$ consisting of linear recurring sequences $\sigma_1, \ldots, \sigma_m$ over $\mathbb{F}_q$, that is, a linear recurring multisequence $\mathbf{S}$ over $\mathbb{F}_q$.
- Joint minimal polynomial $P_{\mathbf{S}} \in \mathbb{F}_q[x]$ is defined to be the (uniquely determined) monic polynomial of the least degree such that $P_{\mathbf{S}}$ is a characteristic polynomial of σ_i for each $1 \leq i \leq m$.
- The joint linear complexity $L(\mathbf{S})$ of $\mathbf{S}$ is defined to be $L(\mathbf{S}) = \deg(P_{\mathbf{S}})$.

Multiple Sequences and Joint Linear Complexity

- For $1 \leq i \leq m$, let

$$\sigma_i = (s_{i,n})_{n=0}^{\infty},$$

  and assume that σ_i is not the zero sequence for some $1 \leq i \leq m$.

- The joint linear complexity $L(\mathbf{S})$ is the smallest positive integer c for which there exist coefficients $a_1, a_2, \ldots, a_c \in \mathbb{F}_q$ such that for each $1 \leq i \leq m$, we have

$$s_{i,n} + a_1 s_{i,n-1} + \cdots + a_c s_{i,n-c} = 0 \qquad \text{for all} \;\; n \geq c.$$

Some Notations

- Given a monic polynomial $f \in \mathbb{F}_q[x]$.
- $\mathcal{M}^{(m)}(f)$: The set of m-fold multisequences $\mathbf{S} = (\sigma_1, \ldots, \sigma_m)$ such that for each $1 \le i \le m$, σ_i is a linear recurring sequence over $\mathbb{F}_q$ with characteristic polynomial f.
- $$\left|\mathcal{M}^{(m)}(f)\right| = q^{m \deg(f)}.$$

Some Notations

- The expectation $\mathrm{E}^{(m)}(f)$ and the variance $\mathrm{Var}^{(m)}(f)$ of the joint linear complexity of random m-fold multisequences from $\mathcal{M}^{(m)}(f)$, which are uniformly distributed over $\mathcal{M}^{(m)}(f)$.
- Counting function $\mathcal{N}^{(m)}(f;t)$: The number of m-fold multisequences from $\mathcal{M}^{(m)}(f)$ with a given joint linear complexity t.

Preliminaries

- For a monic polynomial $f \in \mathbb{F}_q[x]$ with $\deg(f) \geq 1$, let

$$C(f) := \{h \in \mathbb{F}_q[x] : \deg(h) < \deg(f)\},$$

$$R^{(m)}(f) := \{(h_1, \ldots, h_m) \in C(f)^m : \\ \gcd(h_1, \ldots, h_m, f) = 1\},$$

$$\Phi_q^{(m)}(f) := \left|R^{(m)}(f)\right|, \text{ and } \Phi_q^{(m)}(1) := 1.$$

- $\Phi_q^{(m)}(f)$ is the number of m-fold multisequences $\mathbf{S}$ with the joint minimal polynomial $f(x)$.

Preliminaries

Lemma

If $f = r_1^{e_1} r_2^{e_2} \cdots r_k^{e_k}$ *is the canonical factorization of* f *into monic irreducible polynomials over* $\mathbb{F}_q$*, then*

$$\Phi_q^{(m)}(f) = q^{m\deg(f)} \prod_{i=1}^{k} \left(1 - q^{-m\deg(r_i)}\right).$$

Expectation and Variance

- Monic polynomial $f \in \mathbb{F}_q[x]$ with $\deg(f) \geq 1$.
- Canonical factorization

$$f = r_1^{e_1} r_2^{e_2} \cdots r_k^{e_k}$$

- For $1 \leq i \leq k$, let $\alpha_i = q^{m \deg(r_i)}$.

Expectation and Variance

Theorem

Expectation $\mathrm{E}^{(m)}(f)$ *and Variance* $\mathrm{Var}^{(m)}(f)$*:*

$$\mathrm{E}^{(m)}(f) = \deg(f) - \sum_{i=1}^{k} \frac{1-\alpha_i^{-e_i}}{\alpha_i - 1} \deg(r_i),$$

$$\mathrm{Var}^{(m)}(f) = \sum_{i=1}^{k} \left(\frac{\deg(r_i)}{1-\alpha_i^{-1}} \right)^2$$
$$\times [(2e_i+1)\left(\alpha_i^{-e_i-2} - \alpha_i^{-e_i-1}\right) - \alpha_i^{-2e_i-2} + \alpha_i^{-1}].$$

Expectation and Variance

Remark:

- When $f(x) = x^N - 1 \in \mathbb{F}_q[x]$ and N is an arbitrary positive integer, This is the case of m-fold N-periodic multisequences over $\mathbb{F}_q$.
- This theorem yields the corresponding results of Meidl-Niederreiter and Fu-Niederreiter-Su by a simpler method.
- These corresponding results are the general formulas for the expectation and the variance of the joint linear complexity of random m-fold N-periodic multisequences over $\mathbb{F}_q$.

Expectation and Variance

Cyclotomic coset:

- Let n be a positive integer with $\gcd(n, q) = 1$.

- For $j \in \mathbf{Z}_n := \{0, 1, \ldots, n-1\}$, the cyclotomic coset C_j of j modulo n relative to powers of q is defined as

$$C_j = \{j, j \cdot q, \ldots, j \cdot q^{l_j - 1}\} \pmod{n},$$

where l_j is the least positive integer l satisfying $j \cdot q^l \equiv j \pmod{n}$.

Expectation and Variance

Let $N = p^v n$ with $v \geq 0$, $p = \mathrm{char}\,\mathbb{F}_\mathrm{q}$, and $\gcd(n, p) = 1$. Let $D_1, \ldots, D_h$ be the different cyclotomic cosets modulo n and let $d_r = |D_r|$, $1 \leq r \leq h$, be the sizes of these cyclotomic cosets, respectively.

- Meidl-Niederreiter 2003
  The expectation $E_N^{(m)}$ of the joint linear complexity of m random N-periodic sequences with terms in $\mathbb{F}_q$ is given by

$$E_N^{(m)} = N - \sum_{r=1}^{h} \frac{d_r a_r (1 - a_r^{p^v})}{1 - a_r},$$

  where $a_r = q^{-d_r m}$.

Expectation and Variance

- Fu-Niederreiter-Su 2005
  The variance $V_N^{(m)}$ of the joint linear complexity of m random N-periodic sequences with terms in $\mathbb{F}_q$ is given by

$$V_N^{(m)} = \sum_{r=1}^{h} d_r^2 \cdot \frac{(2p^v + 1)(a_r^{p^v+2} - a_r^{p^v+1}) - a_r^{2p^v+2} + a_r}{(1 - a_r)^2},$$

  where $a_r = q^{-d_r m}$.

Expectation and Variance

Some Examples:

- $N = p^v$, $p = \mathrm{char}\ \mathbb{F}_\mathrm{q}$:

$$E_N^{(m)} = N - \frac{1}{q^m - 1}\left(1 - \frac{1}{q^{mN}}\right),$$

$$V_N^{(m)} = \frac{(q^m + q^{-Nm})(1 - q^{-Nm})}{(q^m - 1)^2} - \frac{2q^{-Nm}}{q^m - 1}N.$$

Expectation and Variance

- N is a prime different from p:
  Let d be the multiplicative order of q in the prime field $\mathbb{F}_N$.

$$E_N^{(m)} = N - \frac{N-1}{q^{dm}} - \frac{1}{q^m},$$

$$V_N^{(m)} = q^{-m} - q^{-2m} + (N-1)d(1-q^{-dm})q^{-dm}.$$

Expectation and Variance

- $N = q^k - 1$ and k is a prime:

$$E_N^{(m)} = N - (q-1)q^{-m} - (q^k - q)q^{-km},$$

$$V_N^{(m)} = (q-1)q^{-m}(1 - q^{-m}) + k(q^k - q)q^{-km}(1 - q^{-km}).$$

Reference Papers

- W. Meidl, H. Niederreiter, On the expected value of the linear complexity and the *k*-error linear complexity of periodic sequences, IEEE Trans. Inform. Theory 48 (2002) 2817–2825.
- W. Meidl, H. Niederreiter, The expected value of the joint linear complexity of periodic multisequences, J. Complexity 19 (2003) 61–72.
- F.-W. Fu, H. Niederreiter, M. Su, The expectation and variance of the joint linear complexity of random periodic multisequences, J. Complexity 21 (2005) 804–822.

Counting Function

Theorem

Counting function $\mathcal{N}^{(m)}(f;t)$ *where* $t \leq \deg(f)$*:*

$$\mathcal{N}^{(m)}(f;t) = \sum_{\substack{d|f \\ \deg(d)=t}} \Phi_q^{(m)}(d),$$

where the summation is over all monic polynomials $d \in \mathbb{F}_q[x]$ *of degree* t *and dividing* f*.*

Counting Function

- We determine closed-form expressions for $\mathcal{N}^{(m)}(f; \deg(f))$, $\mathcal{N}^{(m)}(f; \deg(f) - 1)$, and $\mathcal{N}^{(m)}(f; \deg(f) - 2)$.
- We also give tight upper and lower bounds on the counting function $\mathcal{N}^{(m)}(f; t)$ in general.
- We give concrete examples determining the counting functions in closed form in some special cases.

Generating Polynomial

- Generating polynomial $\mathcal{G}^{(m)}(f; z)$ for the distribution of joint linear complexities of m-fold multisequences from $\mathcal{M}^{(m)}(f)$:

$$\mathcal{G}^{(m)}(f; z) := \sum_{t \geq 0} \mathcal{N}^{(m)}(f; t) z^t.$$

- We now determine $\mathcal{G}^{(m)}(f; z)$ as a product of certain polynomials in z depending on the canonical factorization of f into monic irreducibles over $\mathbb{F}_q$.

Generating Polynomial

Theorem

If $f = f_1 f_2$, *where* $f_1, f_2 \in \mathbb{F}_q[x]$ *are monic polynomials with* $\deg(f_1), \deg(f_2) \geq 1$, *and* $\gcd(f_1, f_2) = 1$, *then*

$$\mathcal{G}^{(m)}(f; z) = \mathcal{G}^{(m)}(f_1; z)\mathcal{G}^{(m)}(f_2; z).$$

Generating Polynomial

Theorem

If $f = r_1^{e_1} r_2^{e_2} \cdots r_k^{e_k}$ *is the canonical factorization of* f *into monic irreducibles over* $\mathbb{F}_q$*, then*

$$\mathcal{G}^{(m)}(f;z) = \prod_{j=1}^{k} \left(1 + (1 - \alpha_j^{-1}) \frac{\left(\alpha_j z^{\deg(r_j)}\right)^{e_j+1} - \alpha_j z^{\deg(r_j)}}{\alpha_j z^{\deg(r_j)} - 1} \right),$$

where $\alpha_j = q^{m \deg(r_j)}$ *for* $1 \leq j \leq k$*.*

Generating Polynomial

- For $N \geq 1$, recall that the set of m-fold N-periodic multisequences over $\mathbb{F}_q$ is the same as the set $\mathcal{M}^{(m)}(f)$, where

$$f(x) = x^N - 1 \in \mathbb{F}_q[x].$$

Generating Polynomial

- $n \geq 1$ is an integer with $\gcd(n, q) = 1$.
- Euler totient function $\phi(\ell)$: The number of nonnegative integers less than ℓ and coprime to ℓ.
- For each positive integer d dividing n, let $H_q(d)$ be the multiplicative order of q modulo d, i.e., the least positive integer h such that $q^h \equiv 1 \mod d$.

Generating Polynomial

Theorem

Let $m, N \geq 1$ be integers and p be the characteristic of $\mathbb{F}_q$. Let $n \geq 1$ and $\nu \geq 0$ be the integers such that $N = p^\nu n$ and $\gcd(n, p) = 1$. Assume that $f(x) = x^N - 1 \in \mathbb{F}_q[x]$. Then we have

$$\mathcal{G}^{(m)}(f; z) =$$

$$\prod_{d|n} \left(1 + \left(1 - q^{-mH_q(d)}\right) \frac{\left(q^{mH_q(d)} z^{H_q(d)}\right)^{p^\nu + 1} - q^{mH_q(d)} z^{H_q(d)}}{q^{mH_q(d)} z^{H_q(d)} - 1} \right)^{\phi(d)/H_q(d)}$$

Generating Polynomial

Remark:

- The counting function $\mathcal{N}^{(m)}(f;t)$ is the coefficient of the term z^t of the generating polynomial $\mathcal{G}^{(m)}(f;z)$.
- These two theorems determine $\mathcal{G}^{(m)}(f;z)$ as a product of certain polynomials in z.
- However, even for $f(x) = x^N - 1$, i.e., the periodic case, it is difficult in general to obtain the coefficient of the term z^t from the product in the above theorem.

Publication

Fang-Wei Fu, H. Niederreiter, and F. Özbudak,
Joint linear complexity of multisequences consisting of linear recurring sequences, Cryptography and Communications, vol.1, no.1, pp. 3-29, 2009.

General Case

- Let s be an arbitrary positive integer.
- Let $m_1, m_2, \ldots, m_s$ be further arbitrarily chosen positive integers.
- Let $f_1, f_2, \ldots, f_s \in \mathbb{F}_q[x]$ be monic polynomials of positive degree.

General Case

- Let $\mathcal{M}^{(m_1,m_2,\ldots,m_s)}(f_1, f_2, \ldots, f_s)$ be the set of $(m_1 + m_2 + \cdots + m_s)$-fold multisequences

$$\mathbf{S} = (\quad \begin{array}{l} \sigma_{1,1}, \sigma_{1,2}, \ldots, \sigma_{1,m_1}, \\ \sigma_{2,1}, \sigma_{2,2}, \ldots, \sigma_{2,m_2}, \\ \cdots\cdots \\ \sigma_{s,1}, \sigma_{s,2}, \ldots, \sigma_{s,m_s} \quad) \end{array}$$

such that for each $1 \le i \le s$ and $1 \le j \le m_i$, $\sigma_{i,j}$ is a linear recurring sequence over $\mathbb{F}_q$ with characteristic polynomial f_i.

General Case

- Expectation $\mathrm{E}^{(m_1,m_2,\ldots,m_s)}(f_1, f_2, \ldots, f_s)$ and Variance $\mathrm{Var}^{(m_1,m_2,\ldots,m_s)}(f_1, f_2, \ldots, f_s)$ of the joint linear complexity of random $(m_1 + m_2 + \cdots + m_s)$-fold multisequences from $\mathcal{M}^{(m_1,m_2,\ldots,m_s)}(f_1, f_2, \ldots, f_s)$.

General Case

- Counting function $\mathcal{N}^{(m_1,m_2,\ldots,m_s)}(f_1, f_2, \ldots, f_s; t)$ of $(m_1 + m_2 + \cdots + m_s)$-fold multisequences from $\mathcal{M}^{(m_1,m_2,\ldots,m_s)}(f_1, f_2, \ldots, f_s)$ with a given joint linear complexity t.

General Case

- Generating polynomial $\mathcal{G}^{(m_1,m_2,\ldots,m_s)}(f_1, f_2, \ldots, f_s; z)$:

$$\mathcal{G}^{(m_1,m_2,\ldots,m_s)}(f_1, f_2, \ldots, f_s; z) := \sum_{t\geq 0} \mathcal{N}^{(m_1,m_2,\ldots,m_s)}(f_1, f_2, \ldots, f_s; t) z^t.$$

Publication

Fang-Wei Fu, H. Niederreiter, and F. Özbudak,
Joint linear complexity of arbitrary multisequences consisting of linear recurring sequences, Finite Fields and Their Applications, vol.15, no.4, pp.475-496, 2009.

$f_1, f_2, \ldots, f_s$ are pairwise coprime

Special case: $f_1, f_2, \ldots, f_s$ are pairwise coprime.

Theorem

$$\mathrm{E}^{(m_1,m_2,\ldots,m_s)}(f_1, f_2, \ldots, f_s) = \sum_{i=1}^{s} \mathrm{E}^{(m_i)}(f_i),$$

$$\mathrm{Var}^{(m_1,m_2,\ldots,m_s)}(f_1, f_2, \ldots, f_s) = \sum_{i=1}^{s} \mathrm{Var}^{(m_i)}(f_i).$$

Here $\mathrm{E}^{(m_i)}(f_i)$ *and* $\mathrm{Var}^{(m_i)}(f_i)$ *can be computed using previous theorems.*

$f_1, f_2, \ldots, f_s$ are pairwise coprime

Theorem

Counting function

$$\mathcal{N}^{(m_1,m_2,\ldots,m_s)}(f_1, f_2, \ldots, f_s; t) = \sum_{i_1,i_2,\ldots,i_s} \mathcal{N}^{(m_1)}(f_1; i_1)\mathcal{N}^{(m_2)}(f_2; i_2)\cdots\mathcal{N}^{(m_s)}(f_s; i_s),$$

where the summation is over all nonnegative integers $i_1, i_2, \ldots, i_s$ *with* $i_1 + i_2 + \cdots + i_s = t$.

$f_1, f_2, \ldots, f_s$ are pairwise coprime

Theorem

Generating polynomial

$$\mathcal{G}^{(m_1,m_2,\ldots,m_s)}(f_1, f_2, \ldots, f_s; z) = \prod_{i=1}^{s} \mathcal{G}^{(m_i)}(f_i; z).$$

$f_1, f_2, \ldots, f_s$ are pairwise coprime

If $m_1 = m_2 = \cdots = m_s$, then we can completely reduce the consideration to the case $s = 1$.

Corollary

Let $f := f_1 f_2 \cdots f_s \in \mathbb{F}_q[x]$. Then we have

$$\mathcal{N}^{(m,m,\ldots,m)}(f_1, f_2, \ldots, f_s; t) = \mathcal{N}^{(m)}(f; t).$$

Thank you for your attention!