The Number of Irreducible Transformation Shift Registers

Daniel Panario

School of Mathematics and Statistics
Carleton University
daniel@math.carleton.ca

Mathematics of Communications: Sequences, Codes and Designs

January 26, 2015, Banff

(Joint work with S. D. Cohen, S. U. Hasan and Q. Wang.)

Outline

- Brief introduction to LFSRs.
- Word-oriented Stream Cipher: σ-LFSRs.
- Word-oriented Transformation Shift Registers (TSRs).
- Number of irreducible TSRs of order two.
- Asymptotic number of irreducible TSRs of any order over finite fields with an odd number of elements.

Linear Feedback Shift Registers (LFSRs)

Linear feedback shift registers (LFSRs) are engineering devices used to generate sequences over a finite field. They have numerous applications in various disciplines including in cryptography.

An LFSR of order n over $\mathbb{F}_q$ is given by

$$s_{i+n} = s_{i+n-1}c_{n-1} + \cdots + s_{i+1}c_1 + s_i c_0 \qquad i = 0, 1, \ldots, \qquad (1)$$

where $c_0, c_1, \ldots, c_{n-1} \in \mathbb{F}_q$

- $(s_0, s_1, \ldots, s_{n-1}) \in \mathbb{F}_q^n$: initial state;
- the sequence $s^\infty = (s_0, s_1, \ldots)$ generated by the LFSR (1) is always ultimately periodic with period at most $q^n - 1$;
- the LFSR (1) is primitive if s^∞ is periodic with maximum possible period for any choice of the nonzero initial state.

Primitive LFSRs

Sequences with maximal period have been proved to have some good cryptographic properties. LFSRs corresponding to sequences with maximum period are known as primitive LFSRs.

Question: number of primitive LFSRs of order n over $\mathbb{F}_q$?

Answer: $\frac{\phi(q^n-1)}{n}$, where ϕ is Euler's totient function, since the LFSR in (1) is primitive if and only if

$f(X) = X^n - c_{n-1}X^{n-1} - \cdots - c_1X - c_0$ is a primitive polynomial.

Irreducible LFSRs

A similar formula exists for the number of irreducible LFSRs (that is, when the characteristic polynomial of the LFSR is irreducible) of order n over a finite field $\mathbb{F}_q$. This is just the number of irreducible polynomials of degree n over $\mathbb{F}_q$:

$$\frac{1}{n}\sum_{d|n}\mu(d)\,q^{n/d},$$

where μ is the Möbius function.

Problem: [Preneel (1994)] Can we design fast and secure feedback shift registers using the word operations of modern processors?

Word-oriented Stream Cipher: σ-LFSRs

Zeng, Han and He (2007) introduce the notion of σ-LFSR defined replacing (1) by

$$\mathbf{s}_{i+n} = \mathbf{s}_{i+n-1} C_{n-1} + \cdots + \mathbf{s}_{i+1} C_1 + \mathbf{s}_i C_0, \tag{2}$$

where $C_0, C_1, \ldots, C_{n-1} \in M_m(\mathbb{F}_q)$

- $(\mathbf{s}_0, \ldots, \mathbf{s}_{n-1}) \in (\mathbb{F}_q^m)^n$: initial state;
- the sequence $\mathbf{s}^\infty = (\mathbf{s}_0, \mathbf{s}_1, \ldots)$ is always ultimately periodic with period no more than $q^{mn} - 1$;
- the σ-LFSR (2) is primitive if s^∞ is periodic with maximum possible period for any choice of nonzero initial state.

What is the number of primitive σ-LFSRs?

The study of σ-LFSR can be traced back to Niederreiter (1993-96) in his works on the multiple recursive matrix method.

Problem: number of primitive σ-LFSRs of order n over $\mathbb{F}_{q^m}$?

Conjecture: [Zeng, Han and He (2007)] This number is given by

$$\frac{\phi(q^{mn}-1)}{mn} \cdot q^{m(m-1)(n-1)} \prod_{i=1}^{m-1}(q^m - q^i).$$

- $n = 1$, any m : Ghorpade, Hasan and Kumari (DCC, 2011).
- $m = 2$, any n : Ghorpade and Ram (FFA, 2011).
- Conjecture settled by Chen and Tseng (FFA, 2013).

Irreducible σ-LFSRs

It is now also known from Ghorpade and Ram (FFA, 2011) and Chen and Tseng (FFA, 2013) that the number of irreducible σ-LFSRs is (obviously!)

$$q^{m(m-1)(n-1)} \prod_{i=1}^{m-1} (q^m - q^i) \cdot \frac{1}{mn} \sum_{d|mn} \mu(d)\, q^{\frac{mn}{d}}.$$

Transformation Shift Registers (TSR) were given as another solution to the problem posed by Preneel.

Word-oriented Transformation Shift Registers (TSRs)

Tsaban and Vishne (FFA, 2002) introduce the notion of TSR defined replacing (1) by

$$\mathbf{s}_{i+n} = \mathbf{s}_{i+n-1}(c_{n-1}A) + \cdots + \mathbf{s}_{i+1}(c_1 A) + \mathbf{s}_i(c_0 A), \tag{3}$$

where $c_0, c_1, \ldots, c_{n-1} \in \mathbb{F}_q$ and $A \in M_m(\mathbb{F}_q)$

- $(\mathbf{s}_0, \ldots, \mathbf{s}_{n-1})$ is in $(\mathbb{F}_q^m)^n$: initial state;
- the sequence $\mathbf{s}^\infty = (\mathbf{s}_0, \mathbf{s}_1, \ldots)$ is always ultimately periodic with period no more than $q^{mn} - 1$;
- the TSR (3) is primitive if s^∞ is periodic with maximum possible period.

The family of TSRs is a subclass of the family of σ-LFSRs.

What is the number of primitive TSRs?

Open problem: number of primitive TSRs of order n over $\mathbb{F}_q^m$?

We do not know yet any explicit nice formula like for the number of primitive LFSRs and σ-LFSR for the number of primitive TSRs.

The problem of enumerating primitive TSRs was first considered in Hasan, Panario and Wang (SETA, 2012). To count primitive TSRs, it is sufficient to enumerate certain block companion matrices in a corresponding general linear group. However, except few initial cases, this problem seems rather difficult and still remains open.

Dewar and Panario (2003-04) developed the theory of TSRs.

Irreducible TSRs

Based on empirical evidence, Tsaban and Vishne (FFA, 2002) point out that irreducible TSRs contain a high proportion of primitive TSRs. To find a primitive TSR one might try an exhaustive search only among the irreducible ones instead over all TSRs.

Motivated in part by this and in an attempt to obtain a nice formula for the number of irreducible TSRs, we consider the problem of enumerating irreducible TSRs.

This problem was first considered by Ram (DCC, to appear). He gives a formula for the number of irreducible TSRs of order $n = 2$.

Our results

- We give a short proof of Ram's result for the number of irreducible TSRs of order two using a variant of a theorem of Carlitz proved by Ahmadi (FFA, 2011).

- We prove an asymptotic formula for the number of irreducible TSRs of any order over $\mathbb{F}_q$ using classical results due to Cohen (Acta Arith., 1970) when q is odd.

  The case q even remains completely open.

State transition matrix of the TSR

Corresponding to the characteristic polynomial of (1) we have

$$X^n - (c_{n-1}A)X^{n-1} - \cdots - (c_1A)X - (c_0A) \in M_m(\mathbb{F}_q)[X].$$

We can associate a (m, n)-block companion matrix $T \in M_{mn}(\mathbb{F}_q)$

$$T = \begin{pmatrix} \mathbf{0} & \mathbf{0} & \mathbf{0} & . & . & \mathbf{0} & \mathbf{0} & c_0A \\ I_m & \mathbf{0} & \mathbf{0} & . & . & \mathbf{0} & \mathbf{0} & c_1A \\ . & . & . & . & . & . & . & . \\ . & . & . & . & . & . & . & . \\ \mathbf{0} & \mathbf{0} & \mathbf{0} & . & . & I_m & \mathbf{0} & c_{n-2}A \\ \mathbf{0} & \mathbf{0} & \mathbf{0} & . & . & \mathbf{0} & I_m & c_{n-1}A \end{pmatrix}, \tag{4}$$

where $c_0, c_1, \ldots, c_{n-1} \in \mathbb{F}_q$ and $A \in M_m(\mathbb{F}_q)$.

Let $\mathrm{TSR}(m, n, q)$ be the set of (m, n)-block companion matrices T over $\mathbb{F}_q$.

- Using a suitable sequence of operations, we conclude that if $T \in \mathrm{TSR}(m, n, q)$ is given by (4), then $\det T = \pm \det(c_0 A)$. Consequently,

$$T \in \mathrm{GL}_{mn}(\mathbb{F}_q) \iff c_0 \neq 0 \ \text{ and } \ A \in \mathrm{GL}_m(\mathbb{F}_q),$$

  where $\mathrm{GL}_m(\mathbb{F}_q)$ is the general linear group of all $m \times m$ nonsingular matrices over $\mathbb{F}_q$.

- The block companion matrix (4) is the state transition matrix for the TSR (3). Indeed, the k-th state $\mathbf{S}_k := (\mathbf{s}_k, \mathbf{s}_{k+1}, \ldots, \mathbf{s}_{k+n-1}) \in \mathbb{F}_{q^m}^n$ of the TSR (3) is obtained from the initial state $\mathbf{S}_0 := (\mathbf{s}_0, \mathbf{s}_1, \ldots, \mathbf{s}_{n-1}) \in \mathbb{F}_{q^m}^n$ by $\mathbf{S}_k = \mathbf{S}_0 T^k$, for any $k \geq 0$.

We have that $T \in \mathrm{TSR}(m, n, q)$ is periodic if T has the form

$$\begin{pmatrix} \mathbf{0} & \mathbf{0} & \mathbf{0} & . & . & \mathbf{0} & \mathbf{0} & B \\ I_m & \mathbf{0} & \mathbf{0} & . & . & \mathbf{0} & \mathbf{0} & c_1 B \\ . & . & . & . & . & . & . & . \\ . & . & . & . & . & . & . & . \\ \mathbf{0} & \mathbf{0} & \mathbf{0} & . & . & I_m & \mathbf{0} & c_{n-2} B \\ \mathbf{0} & \mathbf{0} & \mathbf{0} & . & . & \mathbf{0} & I_m & c_{n-1} B \end{pmatrix}, \tag{5}$$

where $c_1, \ldots, c_{n-1} \in \mathbb{F}_q$ and $B \in \mathrm{GL}_m(\mathbb{F}_q)$. In what follows, we deal with periodic TSRs only, that is, a TSR of the form (5).

A TSR is primitive or irreducible if its characteristic polynomial is primitive or irreducible.

Primitive TSRs

Proposition

Let $o(T)$ denote the period of the sequence generated by $T \in \mathrm{TSR}(m, n, q)$. The number of primitive TSRs of order n over $\mathbb{F}_{q^m}$ is equal to the cardinality of the set

$$\{T \in \mathrm{TSR}(m, n, q) : T \text{ is of the form (5) and } o(T) = q^{mn} - 1\}.$$

The case $n = 1$ follows from Ghorpade et al (DCC, 2011):

$$\frac{|\mathrm{GL}_m(\mathbb{F}_q)|}{(q^m - 1)} \frac{\phi(q^m - 1)}{m}.$$

The case $m = 1$ is trivial: $\phi(q^n - 1)/n$.

The number of primitive TSRs for other values of m and n is open.

Irreducible TSRs

Let $\mathrm{TSRI}(m, n, q)$ be the set of irreducible TSRs. We first prove the following result about the number of TSRs of order $n = 2$.

Theorem

For $m > 1$, the number $|\mathrm{TSRI}(m, 2, q)|$ of irreducible TSRs of order two over $\mathbb{F}_{q^m}$ is given by

$$\begin{cases} \dfrac{q}{2m} \displaystyle\prod_{i=0}^{m-1} (q^m - q^i) & \text{if } q \text{ is odd and } m = 2^\ell; \\ \dfrac{q}{2m} \displaystyle\prod_{i=1}^{m-1} (q^m - q^i) \sum_{d \mid m, d \text{ odd}} \mu(d) q^{\frac{m}{d}} & \text{if } q \text{ is odd, } m = 2^\ell k, \\ & \text{and } k \geq 3 \text{ is odd;} \\ \dfrac{q-1}{2m} \displaystyle\prod_{i=1}^{m-1} (q^m - q^i) \sum_{d \mid m, d \text{ odd}} \mu(d) q^{\frac{m}{d}} & \text{otherwise.} \end{cases}$$

This exact result was first proved by Ram (DCC, to appear) but our proof is shorter and simpler.

Irreducible TSRs of order two (sketch)

We denote by $\psi_P(X)$ the characteristic polynomial of a matrix P and by $\mathcal{I}(d,q)$ be the set of monic irreducible polynomials in $\mathbb{F}_q[X]$ of degree d.

Let $g_T(X) = 1 + c_1X + \cdots + c_{n-1}X^{n-1} \in \mathbb{F}_q[x]$. Then, the characteristic polynomial of $T \in \mathrm{TSR}(m,n,q)$ satisfies

$$\psi_T(X) = g_T(X)^m \psi_B\left(\frac{X^n}{g_T(X)}\right). \tag{6}$$

We consider the characteristic map

$$\Psi : M_{mn}(\mathbb{F}_q) \longrightarrow \mathbb{F}_q[X] \quad \text{defined by} \quad \Psi(T) := \det(XI_{mn} - T)$$

and its restriction Ψ_I to $\mathrm{TSRI}(m,n,q)$.

Irreducible TSRs of order two (cont.)

It follows from (6) and Ram (DCC, to appear) that $f(X) \in \Psi_I(\mathrm{TSRI}(m,n,q))$ if and only if $f(X)$ is irreducible and can be uniquely expressed in the form

$$g(X)^m h\left(\frac{X^n}{g(X)}\right) \tag{7}$$

for some monic irreducible polynomial $h(X) \in \mathbb{F}_q[X]$ of degree m with $h(0) \neq 0$ and a not necessarily monic $g(X) \in \mathbb{F}_q[X]$ of degree at most $n-1$ with $g(0) = 1$.

In our case $n = 2$, so we need to count irreducibles f that can be written as $g(X)^m h\left(\frac{X^2}{g(X)}\right)$ for polynomials g, with $\deg(g) < 2$, and irreducible h.

Proposition (Carlitz 1967; Ahmadi 2011)

Let $e(X) = a_1X^2 + b_1X + c_1$ and $g(x) = a_2X^2 + b_2X + c_2$ be two relatively prime polynomials in $\mathbb{F}_q[X]$ with $\max(\deg(e), \deg(g)) = 2$, and let $\mathcal{I}(e, g, m, q)$ be the set of monic irreducible polynomials $h(X)$ of degree $m > 1$ over $\mathbb{F}_q$ such that

$$g(X)^m h\left(\frac{e(X)}{g(X)}\right)$$

is irreducible over $\mathbb{F}_q$. Then

$$|\mathcal{I}(e, g, m, q)| = \begin{cases} 0 & \text{if } b_1 = b_2 = 0 \text{ and } q \text{ is even;} \\ \frac{1}{2m}(q^m - 1) & \text{if } q \text{ is odd and } m = 2^l,\ l \geq 1; \\ \frac{1}{2m} \sum_{d|m, d \text{ odd}} \mu(d) q^{\frac{m}{d}} & \text{otherwise.} \end{cases}$$

Theorem.

For $m > 1$, we have,

$$|\Psi_I(\mathrm{TSRI}(m,2,q))| = \begin{cases} \dfrac{q}{2m}(q^m - 1) & \text{if } q \text{ is odd and } m = 2^\ell; \\ \dfrac{q}{2m} \displaystyle\sum_{d|m, d \text{ odd}} \mu(d) q^{\frac{m}{d}} & \text{if } q \text{ is odd and } m = 2^\ell k, \\ & \text{and } k \geq 3 \text{ is odd}; \\ \dfrac{q-1}{2m} \displaystyle\sum_{d|m, d \text{ odd}} \mu(d) q^{\frac{m}{d}} & \text{otherwise.} \end{cases}$$

Theorem

The number of irreducible TSRs of order n over $\mathbb{F}_{q^m}$ is given by the following

$$|\mathrm{TSRI}(m,n,q)| = |\Psi_I(\mathrm{TSRI}(m,n,q))| \prod_{i=1}^{m-1}(q^m - q^i).$$

Proof (sketch). Let us assume that $f(X) \in \Psi_I(\mathrm{TSRI}(m,n,q))$; then, it can be uniquely expressed as in (7). Moreover, there is $T \in \mathrm{TSRI}(m,n,q)$ such that $\psi_T(X) = f(X)$. Clearly $g_T(X) = g(X)$ and $\psi_B(X) = h(X)$. The number of such T is equal to the number of possible values of B with $\psi_B(X) = h(X)$. It can be proved that the number of such B is $\prod_{i=1}^{m-1}(q^m - q^i)$. □

Putting all pieces together we have proved the following result.

Theorem

For $m > 1$, the number $|\mathrm{TSRI}(m, 2, q)|$ of irreducible TSRs of order two over $\mathbb{F}_{q^m}$ is given by

$$\begin{cases} \dfrac{q}{2m} \displaystyle\prod_{i=0}^{m-1} (q^m - q^i) & \text{if } q \text{ is odd and } m = 2^\ell; \\ \dfrac{q}{2m} \displaystyle\prod_{i=1}^{m-1} (q^m - q^i) \sum_{d \mid m, d \text{ odd}} \mu(d) q^{\frac{m}{d}} & \text{if } q \text{ is odd, } m = 2^\ell k, \\ & \text{and } k \geq 3 \text{ is odd;} \\ \dfrac{q-1}{2m} \displaystyle\prod_{i=1}^{m-1} (q^m - q^i) \sum_{d \mid m, d \text{ odd}} \mu(d) q^{\frac{m}{d}} & \text{otherwise.} \end{cases}$$

Asymptotic formula for the number of irreducible TSRs of any order n when q is odd

Our main result is the following asymptotic formula valid for any order n but only for finite fields $\mathbb{F}_q$ with q odd.

Theorem

Suppose that q is odd and $m > 1$. Then the number $|\mathrm{TSRI}(m, n, q)|$ of irreducible TSRs of order $n > 2$ over $\mathbb{F}_{q^m}$ satisfies

$$|\mathrm{TSRI}(m, n, q)| = \frac{q^{m+n-1}}{mn} \prod_{i=1}^{m-1} (q^m - q^i) + O\left(q^{m^2+n-2}/m\right).$$

The proof is based on Cohen's work on the distribution of polynomials over finite fields (Acta Arith., 1970; JLMS, 1972).

Conclusions and open problems

In an intention to design fast and secure feedback shift registers using the word operations of modern processors some proposals have been considered. One of them is transformation shift register (TSR). In this paper we study the number of irreducible TSRs.

We comment that the number of primitive TSRs of order n over $\mathbb{F}_{q^m}$ is known only for $m = 1$ and $n = 1$.

In this paper we give an exact formula for the number of irreducible TSRs of order $n = 2$ and an asymptotic formula for the number of irreducible TSRs of any order n when q is odd. It is an open problem to derive exact formulas for the number of irreducible TSRs of order $n > 3$ and asymptotic formulas for even q.