On the binary sequences with high $GF(2)$ linear complexities and low $GF(p)$ linear complexities

Hao Chen
Liqing Xu
Department of Computing and
Information Technology
Fudan University
Shanghai 200433
People's Republic of China

May.2005

Abstract

Klapper [1] showed that there are binary sequences of period $q^n - 1$(q is a prime power p^m, p is an odd prime) with the maximal possible linear complexity $q^n - 1$ when considered as sequences over $GF(2)$, while the sequences have very low linear complexities when considered as sequences over $GF(p)$. This suggests that the binary sequences with high $GF(2)$ linear complexities and low $GF(p)$ linear complexities are note secure in cryptography. In this note we give some simple constructions of the binary sequences with high $GF(2)$ linear complexities and low $GF(p)$ linear complexities. We also prove some lower bounds on the $GF(p)$ linear complexities of binary sequences and a lower bound on the number of the binary sequences with high $GF(2)$ linear complexities and low $GF(p)$ linear complexities .

Index Terms—Cryptography, stream cipher, $GF(2)$ linear complexity, $GF(p)$ linear complexity

I. Introduction and Preliminaries

In cryptography stream ciphers use binary sequences with good pseudo-randomness as key streams to encrypt messages [2]. The linear complexity of a periodic binary sequence is defined as the length of the shortest linear feedback shift register to generate the sequence. The periodic binary sequences with low linear complexity are not secure, since people can compute the whole sequence based on given knowledge of a few initial bits of the sequence. For example, for any period n binary sequence the Berlekamp-Massey algorithm can be used to compute its linear complexity and minimal connection polynomial with the time complexity $O(n^2)$ ([2]).

For a binary sequence $\mathbf{a} = a_0, a_1, ..., a_{l-1}, a_0, ...$, where $a_i \in GF(2)$, with period l, its generating function $A(x) = a_0 + a_1x + ... + a_ix^i + ... = \Sigma_{i\geq 0}a_ix^i = \frac{a_0+a_1x+...a_{l-1}x^{l-1}}{1-x^l}$. Let $gcd(a_0 + a_1x + ... + a_{l-1}x^{l-1}, 1 - x^l)$ be the greatest common divisor of the two polynomials in $GF(2)[x])$. It is well-known (see [2]) that the $(GF(2))$linear complexity of the sequence $\mathbf{a}$ is $LC_2(\mathbf{a}) = deg(1 - x^l) - deg(gcd(a_0 + a_1x + ... + a_{l-1}x^{l-1}, 1 - x^l))$ and the minimal connection polynomial is $m(\mathbf{a})(x) = \frac{1-x^l}{gcd(a_0+a_1x+...+a_{l-1}x^{l-1},1-x^l)}$ (see [2]).

A very important progress was made in Klapper's pioneering work[1]. It is suggested the consideration, for a periodic binary sequences, of the linear complexity relative to an odd prime. That is, for cryptographic purpose we should study the linear complexity of the binary sequence considered as a sequence over $GF(p)$(whose elements happen to be the 0 and 1 in $GF(p)$). If this linear complexity relative to $GF(p)$ is small, it is easy to get the whole sequence by the Berlekamp-Massey algorithm over $GF(p)$ based the knowledge of the few initial elements of the sequence, thus this binary sequence is not secure in cryptography. We call this linear complexity relative to $GF(p)$ as $GF(p)$ linear complexity. It is defined as follows. For a (binary) sequence $\mathbf{a} = a_0, a_1, ..., a_{l-1}, a_0, ...$, where $a_i = 0$ or $1, \in GF(p)$, with period l, let $g(x) = gcd_p(a_0 + a_1x + ... + a_{l-1}x^{l-1}, 1 - x^l)$ be the greatest common divisor of the two polynomials $a_0 + a_1x + ... + a_{l-1}x^{l-1}$ and $1 - x^l$ considered as polynomials in $GF(p)[x]$. Then the $GF(p)$ linear complexity $LC_p(\mathbf{a})$ of the binary sequence $\mathbf{a}$ is $deg(1 - x^l) - deg(g(x))$. As indicated in [1] for crypto-

graphic purpose we should at least consider the $GF(p)$ linear complexity of a binary sequence for small $p's$.

In [1] Klapper constructed some binary sequences of period $q^n - 1$ (where q is a prime power p^m, p an odd prime) with the maximal $GF(2)$ linear complexity $q^n - 1$, but with relatively very low $GF(p)$ linear complexity. In this note we give some simple constructions of binary sequences with high $GF(2)$ linear complexities and low $GF(p)$ linear complexities. We also prove some lower bounds on the $GF(p)$ linear complexities of the binary sequences with special periods. A lower bound on the number of the binary sequences with high $GF(p)$ linear complexities and low $GF(p)$ linear complexities is also given.

The following are some binary sequences of period 2^n whose $GF(3)$ linear complexities are about the half of their $GF(2)$ linear complexities. These binary sequences are constructed by using the factorization of the polynomial $1 - x^{2^n}$ in $GF(3)[x]$.

Sequence a

The binary sequence $\mathbf{a}$ of period 2^n is $\mathbf{a} = a_0, a_1, ..., a_{2^n-1}, a_0... = 1\ \underbrace{0...0}_{2^{n-2}-1}\ 1\ \underbrace{0...0}_{2^{n-3}-1}\ 1\ \underbrace{0...0}_{5\cdot 2^{n-3}-1}\ 1....$

It is clear its generating function is $A(x) = \Sigma_i a_i x^i = \frac{x^{3\cdot 2^{n-3}} + x^{2^{n-2}} + 1}{1 - x^{2^n}}$. In $GF(2)[x]$, it is clear $1 - x^{2^n} = (1 - x)^{2^n}$ and $gcd(1 - x, x^{3\cdot 2^{n-3}} + x^{2^{n-2}} + 1) = 1$ and thus $LC_2(\mathbf{a}) = 2^n$. In $GF(3)[x]$, $1 - x^{2^n} = (x^{3\cdot 2^{n-3}} + x^{2^{n-2}} + 1)(x^{2^{n-3}} + 1)(x^{2^{n-2}} + 1)(x^{2^{n-2}} + x^{2^{n-3}} + 1)$. Thus the $GF(3)$ linear complexity $LC_3(\mathbf{a}) = 5 \cdot 2^{n-3}$.

Sequence b

The binary sequence $\mathbf{b}$ of period 2^n is $\mathbf{b} = b_0, b_1, ..., b_{2^n-1}, b_0... = 1\ \underbrace{0...0}_{2^{n-4}-1}\ 1\ \underbrace{0...0}_{2^{n-5}-1}\ 1\ \underbrace{0...0}_{5\cdot 2^{n-5}-1}\ 1\ \underbrace{0...0}_{2^{n-4}-1}\ 1\ \underbrace{0...0}_{2^{n-5}-1}\ 1\ \underbrace{0...0}_{2^{n-5}-1}\ 1\ \underbrace{0...0}_{2^{n-4}-1}\ 1\ \underbrace{0...0}_{2^{n-5}-1}\ 1\ \underbrace{0...0}_{17\cdot 2^{n-5}-1}\ 1....$

It is clear its generating function is $A(x) = \Sigma_i a_i x^i = \frac{x^{15\cdot 2^{n-5}}+x^{14\cdot 2^{n-2}}+x^{12\cdot 2^{n-5}}+x^{11\cdot 2^{n-5}}+x^{10\cdot 2^{n-5}}+x^{8\cdot 2^{n-5}}+x^{3\cdot 2^{n-5}}+x^{2\cdot 2^{n-5}}+1}{1-x^{2^n}}$. In $GF(2)[x]$, it is clear $1-x^{2^n} = (1-x)^{2^n}$ and $gcd(1-x, x^{15\cdot 2^{n-5}} + x^{14\cdot 2^{n-2}} + x^{12\cdot 2^{n-5}} + x^{11\cdot 2^{n-5}} + x^{10\cdot 2^{n-5}} + x^{8\cdot 2^{n-5}} + x^{3\cdot 2^{n-5}} + x^{2\cdot 2^{n-5}} + 1) = 1$ and thus $LC_2(\mathbf{a}) = 2^n$.

In $GF(3)[x]$, $1-x^{2^n} = -(x^{3\cdot 2^{n-3}} + x^{2^{n-2}} + 1)(x^{2^{n-4}} + 2x^{2^n-5} + 2)(x^{2^{n-4}} + x^{2^{n-5}} + 2)(x^{2^{n-2}} + 1)(x^{2^{n-2}} + x^{2^{n-3}} + 2)$ and $x^{15\cdot 2^{n-5}} + x^{14\cdot 2^{n-2}} + x^{12\cdot 2^{n-5}} + x^{11\cdot 2^{n-5}} + x^{10\cdot 2^{n-5}} + x^{8\cdot 2^{n-5}} + x^{3\cdot 2^{n-5}} + x^{2\cdot 2^{n-5}} + 1 = (x^{3\cdot 2^{n-3}} + x^{2^{n-2}} + 1)(x^{3\cdot 2^{n-5}} + x^{2\cdot 2^{n-5}} + 1) = -(x^{2^{n-5}} - 1)(x^{3\cdot 2^{n-3}} + x^{2^{n-2}} + 1)(x^{2^{n-4}} + 2x^{2^n-5} + 2)$. The generating function of the sequence $\mathbf{b}$ (as a sequence over $GF(3)$) is $A(x) = \frac{1-x^{2^{n-5}}}{(1+x^{2^{n-2}})(x^{2^{n-2}}+x^{2^{n-3}}+2)(x^{2^{n-4}}+x^{2^{n-5}}+2)}$. When we set $x^{2^{n-5}} = y$, $A(x) = (1-y)/(1+y^8)(y^8+y^4+2)(y^2+y+2)$ and $gcd(1-y, (1+y^8)(y^8+y^4+2)(y^2+y+2)) = 1$ in $GF(3)[x]$. Thus the $GF(3)$ linear complexity $LC_3(\mathbf{b}) = 9 \cdot 2^{n-4}$.

Sequence c

The binary sequence $\mathbf{c}$ of period 2^n is $\mathbf{c} = c_0, c_1, ..., c_{2^n-1}, c_0... = 1\ \underbrace{0...0}_{2^{n-3}-1}\ 1\ \underbrace{0...0}_{2^{n-4}-1}\ 1\ \underbrace{0...0}_{2^{n-4}-1}\ 1\ \underbrace{0...0}_{2^{n-3}-1}\ 1\ \underbrace{0...0}_{2^{n-4}-1}\ 1\ \underbrace{0...0}_{2^{n-4}-1}\ 1\ \underbrace{0...0}_{2^{n-3}-1}\ 1\ \underbrace{0...0}_{2^{n-4}-1}\ 1\ \underbrace{0...0}_{5\cdot 2^{n-4}-1}\ 1....$

It is clear its generating function is $A(x) = \Sigma_i a_i x^i = \frac{x^{11\cdot 2^{n-4}}+x^{10\cdot 2^{n-4}}+x^{8\cdot 2^{n-4}}+x^{7\cdot 2^{n-4}}+x^{6\cdot 2^{n-4}}+x^{4\cdot 2^{n-4}}+x^{3\cdot 2^{n-4}}+x^{2\cdot 2^{n-4}}+1}{1-x^{2^n}}$. In $GF(2)[x]$, it is clear $1-x^{2^n} = (1-x)^{2^n}$ and $gcd(1-x, x^{11\cdot 2^{n-4}} + x^{10\cdot 2^{n-4}} + x^{8\cdot 2^{n-4}} + x^{7\cdot 2^{n-4}} + x^{6\cdot 2^{n-4}} + x^{4\cdot 2^{n-4}} + x^{3\cdot 2^{n-4}} + x^{2\cdot 2^{n-4}} + 1) = 1$ and thus $LC_2(\mathbf{a}) = 2^n$.

In $GF(3)[x]$, $1-x^{2^n} = -(x^{2^{n-1}} + 1)(x^{2^{n-3}} + x^{2^{n-4}} + 2)(x^{2^{n-3}} + 2x^{2^{n-4}} + 2)(x^{2^{n-2}} - 1)$ and $x^{11\cdot 2^{n-4}} + x^{10\cdot 2^{n-4}} + x^{8\cdot 2^{n-4}} + x^{7\cdot 2^{n-4}} + x^{6\cdot 2^{n-4}} + x^{4\cdot 2^{n-4}} + x^{3\cdot 2^{n-4}} + x^{2\cdot 2^{n-4}} + 1 = (x^{2^{n-2}} - 1)^2(x^{2^{n-4}} - 1)(x^{2^{n-3}} + 2x^{2^{n-4}} + 2)$. The generating function of the sequence $\mathbf{c}$ (as a sequence over $GF(3)$) is $A(x) = \frac{(1-x^{2^{n-2}})(x^{2^{n-4}}-1)}{(1+x^{2^{n-1}})(x^{2^{n-3}}+x^{2^{n-4}}+2)}$. When we set $x^{2^{n-4}} = y$, $A(x) = (1-y)(y^4-1)/(1+y^8)(y^2+y+2)$ and $gcd((1-y)(y^4-1), (1+y^8)(y^2+y+2)) = 1$ in $GF(3)[x]$. Thus the $GF(3)$ linear complexity $LC_3(\mathbf{c}) = 5 \cdot 2^{n-3}$.

From the above elementary examples we can see that it is easy to get the binary sequences with the property that their $GF(3)$ linear complexities are lower than their $GF(2)$ linear complexities. However it seems difficult to make the $GF(3)$ linear complexities "*very low*". In the following section we give some lower bounds on the $GF(p)$ linear complexities for the binary sequences with periods 2^n and p^n.

II. Lower bounds on the $GF(p)$ linear complexities of binary sequences with periods 2^n and p^n

In this section we prove the following result.

Theorem 1. i). Suppose p is an odd prime such that $p \equiv 3 \ mod \ 4$. Let u be the largest positive integer such that $2^u | p+1$. If $\mathbf{a}$ is a binary sequence which is strictly of period 2^n with $n \geq u+1$, then its $GF(p)$ linear complexity $LC_p(\mathbf{a}) \geq 2^{n-u}$.

ii). Suppose p is an odd prime such that $p \equiv 3 \ mod \ 4$. Let u be the largest positive integer such that $2^u | p+1$. If $\mathbf{a}$ is a binary sequence of period 2^n ($n \geq u+1$) with its $GF(2)$ linear complexity $LC_2(\mathbf{a}) \geq 2^n - 2^{n-2} + 1$, then we have that its $GF(p)$ linear complexity $LC_p(\mathbf{a}) \geq 2^{n-u} + 2^{n-u-1}$.

iii). Suppose that p is an odd prime. If $\mathbf{a}$ is a binary sequence which is strictly of period p^n, then its $GF(p)$ linear complexity $LC_p(\mathbf{a}) \geq (p-1)p^{n-1} + 1$.

Proof. If $\mathbf{a} = a_0, a_1, ..., a_{2^n-1}, a_0, ...$ is a binary sequence (strictly) of period 2^n, then the polynomial $f(x) = a_0 + a_1 x + ... + a_i x^i + ... + a_{2^n-1} x^{2^n-1}$ cannot be divided by $x^{2^{n-1}} + 1$ in $GF(p)[x]$ for any prime p. In fact if $f(x) = (x^{2^{n-1}} + 1) g(x)$ in $GF(p)[x]$ for $g(x) \in GF(p)[x]$. Then $deg(g(x)) \leq 2^{n-1} - 1$ and $f(x) = g(x) + x^{2^{n-1}} g(x)$. Here we note that every monomial in the 1st part $g(x)$ has its degree less than 2^{n-1} and every monomial in the 2nd part $x^{2^{n-1}} g(x)$ has its degree greater than or equal to 2^{n-1}. Therefore we know $\mathbf{a}$ is of period 2^{n-1}. This is a contradiction.

From the main result in [6], for the odd primes p such that $p \equiv 3 \ \mathrm{mod} \ 4$, we have the factorization $x^{2^{n-1}} + 1$ to 2^u irreducible factors of the form

$x^{2^{n-u}} - 2hx^{2^{n-u-1}} - 1$ in $GF(p)[x]$ (we refer to [6] for the explicit values of h's). Therefore $f(x)$ cannot be divided by at least one polynomial (of degree 2^{n-u}) among these 2^u irreducible factors. The conclusion of i) is proved.

If $\mathbf{a} = a_0, a_1, ..., a_{2^n-1}, a_0, ...$ is a binary sequence (strictly) of period 2^n with its $GF(2)$ linear complexity $LC_2(\mathbf{a}) \geq 2^n - 2^{n-2} + 1$, then the polynomial $f(x) = a_0 + a_1x + ... + a_ix^i + ... + a_{2^n-1}x^{2^n-1}$ cannot be divided by $x^{2^{n-2}} + 1$ in $GF(p)[x]$. Otherwise we have that $f(x) = (x^{2^{n-2}} + 1)g(x)$ in $GF(p)[x]$ for $g(x) \in GF(p)[x]$. It is clear that $deg(g(x)) \leq 3 \cdot 2^{n-2} - 1$. Let $g(x) = g_1(x) + x^{2^{n-2}}g_2(x) + x^{2^{n-1}}g_3(x)$ where $g_i(x) \in GF(p)[x]$ with $deg(g_i(x)) \leq 2^{n-2} - 1$. we have that $f(x) = g_1(x) + (g_1(x) + g_2(x))x^{2^{n-2}} + (g_2(x) + g_3(x))x^{2^{n-1}} + g_3(x)x^{3\cdot 2^{n-2}}$. Because the coefficients of $f(x)$ are 0 or 1 in $GF(3)$, the coefficients of $g_1(x)$ and $g_3(x)$ are 0 or 1 in $GF(3)$. Therefore the coefficients of $g_2(x)$ has to be 0 or 1 or $p-1$ in $GF(p)$. It is clear that the positions at which $g_2(x)$ have coefficients $p-1$ have to be included in the positions at which both $g_1(x)$ and $g_3(x)$ have coefficients 1. Suppose $g_2(x) = g_2'(x) + (p-1)g_2''(x)$ where $g_2'(x)$ and $g_2''(x)$ have their coefficients 0 or 1. then we can write $g_1(x) = g_1'(x) + g_2''(x)$ and $g_3(x) = g_3'(x) + g_2''(x)$. Here we should note that $g_2'(x)$ and $g_2''(x)$ have no common nonzero positions, $g_1'(x)$ and $g_2''(x)$ have no common nonzero positions, $g_3'(x)$ and $g_2''(x)$ have no common nonzero positions,

Thus we have $f(x) = [g_1'(x) + g_2''(x)] + [g_1'(x) + g_2'(x)]x^{2^{n-2}} + [g_2'(x) + g_3'(x)]x^{2^{n-1}} + [g_3'(x) + g_2''(x)]x^{3\cdot 2^{n-2}}$ in $GF(p)[x]$. It is clear that $g_1'(x)$ and $g_2'(x)$ have no common nonzero positions, $g_3'(x)$ and $g_2'(x)$ have no common nonzero positions.

In this way we have $f(x) = ([g_1'(x) + g_2''(x)] + [g_2'(x) + g_2''(x)]x^{2^{n-2}} + [g_3'(x) + g_2''(x)]x^{3\cdot 2^{n-2}})(x^{2^{n-2}} + 1)$ is valid in $GF(2)[x]$. This is a contradiction to the condition that $LC_2(\mathbf{a}) \geq 2^n - 2^{n-2} + 1$. We know that $f(x)$ cannot be divided by $x^{2^{n-2}} + 1$ in $GF(p)[x]$. We have $1 - x^{2^n} = (1-x)(1+x)(1+x^2)...(1+x^{2^{n-2}})(1+x^{2^{n-1}})$ in $GF(p)[x]$. From the main result in [6] we know that $1 + x^{2^{n-2}}$ (resp. $1 + x^{2^{n-1}}$) can be factorized to u irreducible factors of degree 2^{n--u-1}(resp. 2^{n-u}) in $GF(p)[x]$. Similarly as in the proof of i), we have $LC_p(\mathbf{a}) \geq 2^{n-u} + 2^{n-u-1}$. The conclusion of ii) is proved.

If $\mathbf{a} = a_0, a_1, ..., a_{p^n-1}, a_0, ...$ is a binary sequence (strictly) of period p^n. Let $A_i = (a_{ip^{n-1}}, ..., a_{(i+1)p^{n-1}-1})$ for $i = 0, 1, ..., p-1$. From the generalized Games-Chan algorithm (see [3,4]) we know that $LC_p(\mathbf{a}) \geq (p-1)p^{n-1}+1$ if $A_0+A_1+...+A_{p-1} \neq 0$ in $GF(p)^{p^{n-1}}$. However we note that every coordinate in A_i is 0 or 1 in $GF(p)$. Thus if $A_0 + ... + A_{p-1} = 0$ in $GF(p)^{p^{n-1}}$ then we have $A_0 = A_1 = ... = A_{p-1}$. This is the contradiction to the condition that $\mathbf{a}$ is strictly of period p^n. The conclusion iii) is proved.

From Theorem 1 i) we know that each de Bruijn sequence $\mathbf{a}$ with period 2^n has its $GF(p)$ linear complexity $LC_p(\mathbf{a}) \geq 2^{n-u}$ if $p \equiv 3 \bmod 4$, especially $LC_3(\mathbf{a}) \geq 2^{n-2}$.

III. A construction based on generalized Game-Chan algorithm and Xiao-Wei-Lam-Imamura algorithm and a lower bound

In this section we give a construction of binary sequences with the property that their $GF(p)$ linear complexities are about $\frac{p-1}{p}$ of their $GF(2)$ linear complexities for some odd primes $p's$. From this construction many such binary sequences can be given. This construction is derived from the Xiao-Wei-Lam-Imamua algorithm in [5] and the generalized Games-Chan algorithm (see [3] or [4]). We also prove a lower bound on the number of the binary sequences with their $GF(p)$ linear complexities about $\frac{1}{p+1}$ of their $GF(2)$ linear complexities.

Let p be an odd prime with the property that 2 is a primitive root *mod* p^2, that is, 2 is a generator of the multiplicative group of all residue classes (*mod* p^2) coprime to p. There are may such odd primes, for example $p = 3, 5, 11, 13, 19, 29, ...$ (see [5]). For a binary sequences $\mathbf{a} = a_0, a_1, ..., a_{p^n-1}, a_0, ...$ with period p^n (p satisfying the above condition), an fast algorithm for determining its $GF(2)$ linear complexity $LC_2(\mathbf{a})$ was given in [5]. Set $A_i = (a_{(i-1)p^{n-1}}, ...a_{ip^{n-1}-1})$, where $i = 0, 1, ..., p-1$. From the algorithm in [5], if $A_0 = A_1 = ... = A_{p-1}$ is not valid (in $GF(2)$), then $LC_2(\mathbf{a}) = (p-1)p^{n-1} + LC_2(\mathbf{b})$ where $\mathbf{b}$ is a binary sequence of period p^{n-1} with its first p^{n-1} bits $A_0+A_1+...+A_{p-1}$. On the other hand, from the generalized Games-Chan algorithm (see [3] or [4]), if $A_0+A_1+...+A_{p-1} \neq 0$ over the field $GF(p)$, then the $GF(p)$ complexity $LC_p(\mathbf{a}) = (p-1)p^{n-1}+LC_p(\mathbf{b}')$,

where $\mathbf{b}'$ is a sequence of period p^{n-1} over $GF(p)$ with its first p^{n-1} elements $A_0 + A_1 + ... + A_{p-1}$ (Here the operations are in $GF(p)$).

Our construction is as follows. Let $\mathbf{Q_1}$ be a binary sequence of period p^{n-1} with its $GF(2)$ linear complexity $LC_2(\mathbf{Q_1}) = p^{n-1}$, and $\mathbf{Q_2}$ be a nonzero binary sequence of period p^t $(t \leq n-1)$ with its $GF(p)$ linear complexity $LC_p(\mathbf{Q_1})$ very small. We need to impose the following condition on Q_1 and Q_2.

Condition: The set of positions of 1 in Q_1 and the set of positions of 1 in Q_2 do not intersect.

The binary sequence $\mathbf{a}$ of period p^n is constructed as follows. Let $A_0 = Q_1, A_1 = A_2 = ... = A_{p-1} = Q_1 + Q_2$ (Here we just take the first p^{n-1} bits of Q_1 and Q_2). From the above condition it is clear that $A_0, A_1, ..., A_{p-1}$ are binary sequence. Then $\mathbf{a}$ is the binary sequence of period p^n with its first p^n bits $(A_0, A_1, ..., A_{p-1})$. It is clear that $A_0 = A_1$ is not valid (in $GF(2)$), thus $LC_2(\mathbf{a}) = (p-1)p^{n-1} + LC_2(Q_1) = p^n$ from Xiao-Wei-Lam-Imamura algorithm, since $\mathbf{b} = A_0 + A_1 + .. + A_{p-1} = A_0 + (p-1)A_1 = A_0 = Q_1$ over $GF(2)$. On the other hand $\mathbf{b}' = A_0 + A_1 + ... + A_{p-1} = pQ_1 + (p-1)Q_2 = -Q_2$ over $GF(p)$, thus $LC_p(\mathbf{a}) = (p-1)p^{n-1} + LC_p(Q_2)$ from the generalized Games-Chan algorithm. Because $LC_p(\mathbf{Q_2})$ is small, $LC_p(\mathbf{a})$ is about $\frac{p-1}{p}$ of $LC_2(\mathbf{a})$. We can see that there are many such binary sequences satisfying our condition and thus many binary sequence with the above property can be given.

Example 1. The period p^{n-1} sequence $\mathbf{Q_1} = s_0, ..., s_{p^{n-1}-1}, s_0, ... = \underbrace{0...0}_{h} 1 \underbrace{0...0}_{p^{n-1}-h-1} 0...$, where $h \leq p^{n-1}$ is a positive integer such that $h \neq 0 (mod\ p)$. The period p sequence $\mathbf{Q_2} = t_0, ..., t_{p-1}, t_0... = 1 \underbrace{0...0}_{p-1} 1....$ we can check that $\mathbf{Q_1}$ and $\mathbf{Q_2}$ satisfy the condition and $LC_2(\mathbf{Q_1}) = p^{n-1}$ and $LC_p(\mathbf{Q_2}) = p$. Thus $LC_2(\mathbf{a}) = p^n$ and $LC_p(\mathbf{a}) = (p-1)p^{n-1} + p$.

Example 2. Let $p = 3$. The period 3^{n-1} binary sequence $\mathbf{Q_1} = \underbrace{0...0}_{h} 1 \underbrace{0...0}_{3^{n-1}-h-1} 0...$, where $h \neq 0, 3^{n-2}, 2 \cdot 3^{n-2}$. The period 3^{n-1} period binary

sequence $\mathbf{Q_2} = 1\ \underbrace{0...0}_{3^{n-2}-1}\ 1\ \underbrace{0...0}_{3^{n-2}-1}\ 1\ \underbrace{0...0}_{3^{n-2}-1}\ 1....$ It is clear that $LC_2(\mathbf{Q_1}) = 3^{n-1}$ and $LC_3(\mathbf{Q_2}) = 3^{n-2}$. We can check that the binary sequences $\mathbf{Q_1}$ and $\mathbf{Q_2}$ satisfy the condition. Thus $LC_2(\mathbf{a}) = 3^n$ and $LC_3(\mathbf{a}) = 7 \cdot 3^{n-2}$.

From this construction we can have a lower bound on the number of binary sequences (strictly) of period p^n with high $GF(2)$ linear complexities and low $GF(p)$ linear complexities.

Theorem 2. Suppose p is an odd prime such that 2 is a generator of the multiplicative group of all residue classes (module p^2) coprime to p^2. Then there are at least $2^{(p-1)^2p^{n-3}}$ binary sequences $\mathbf{a}$'s (strictly) of period p^n with their $GF(2)$ linear complexities $LC_2(\mathbf{a}) \geq p^n - p^{n-2}$ and $GF(p)$ linear complexities $LC_p(\mathbf{a}) = p^n - p^{n-1} + p$.

Proof. We take $\mathbf{Q_2}$ as in Example 1, and $\mathbf{Q_1}$ to be the binary sequences $s_0, s_1, ..., s_{p^{n-1}-1}, s_0, s_1, ...,$ where $s_i = 0$ if i can be divided by p or $i \geq (p-1)p^{n-2}$. It is clear that there are exactly $2^{(p-1)^2p^{n-3}}$ such $\mathbf{Q_1}$'s.

On the other hand we know that $1-x^{p^{n-1}} = (1-x^{p^{n-2}})(1+x^{p^{n-2}}+x^{2p^{n-2}}+...+x^{(p-1)p^{n-2}})$ in $GF(2)[x]$, and the factor $1+x^{p^{n-2}}+x^{2p^{n-3}}+...+x^{(p-1)p^{n-2}}$ is an irreducible polynomial in $GF(2)[x]$ if 2 is a generator of the multiplicative group of all residue classes (module p^2) coprime to p(see [5]). Therefore the $GF(2)$ linear complexity of $\mathbf{Q_1}$, $LC_2(\mathbf{Q_1}) \geq (p-1)p^{n-2}$, since at the positions after $(p-1)p^{n-2}$ s_i is zero. From the above computation for the corresponding sequence $\mathbf{a}$ we have $LC_p(\mathbf{a}) = (p-1)p^{n-1} + LC_p(\mathbf{Q_2}) = (p-1)p^{n-1} + p$ and $LC_2(\mathbf{a}) = (p-1)p^{n-1} + LC_2(\mathbf{Q_1}) \geq (p-1)p^{n-1} + (p-1)p^{n-2} = p^n - p^{n-2}$. The conclusion is proved.

IV. Conclusion

We have give some results on the lower bounds of $GF(p)$ linear complexities of binary sequences of period 2^n and p^n and give some simple constructions of binary sequences with high $GF(2)$ linear complexities and low $GF(p)$ linear complexities. A lower bound on the number of binary sequences with high $GF(2)$ linear complexities and low $GF(p)$ linear complexities is also proved. From the view of the practical use, we think it would be interest-

ing to study the $GF(p)$ linear complexities of the particular binary sequence generators proposed for practical use in cryptography.

Acknowledgment: We are grateful to the Associate Editor K.Paterson for his very helpful comments on the preliminary version of this paper. This work was supported by Grant 60433050 and Distinguished Young Scholar grant 10225106 of NSF China.

e-mail: chenhao@fudan.edu.cn

REFERENCES

[1] A.Klapper, The vulnerability of geometric sequences based on fields of odd characteristic, J.Cryptology, Vol.7 (1994),no.1, pp.33-51

[2] A. Menezes, P. van Oorschot and S.Vanstone, Handbook of applied cryptography, CRC Press Inc. 1997

[3] C.Ding, G.Xiao and W.Shan, The stability theory of stream ciphers, Lecture Notes in Computer Science, Vol.561, Springer-Verlag, 1991

[4] K.Imamura and T.Moriuchi, A fast algorithm for determining the linear complexity of p-ary sequences with period p^n, p prime, IEICE Tech. Rep. IT 93-75(1993), pp.73-78

[5] G.Xiao, S.Wei, K.Y.Lam and K.Imamura, A fast algorithm for determining the linear complexity of a sequence with period p^n over $GF(q)$, IEEE Trans. Inform. Theory, vol.46(2000), pp.2203-2206

[6] I.F.Blake, Shuhong Gao and R.C.Mullin, Explicit factorization of $x^{2^k}+1$ over F_p with prime $p = 3 \bmod 4$, Applicable Algebra in Engineering, Communication and Computing, vol.4(1993), no.2, pp.89-94