RAIRO-Theor. Inf. Appl. 46 (2012) 401–412
DOI: 10.1051/ita/2012011

Available online at:
www.rairo-ita.org

ON THE JOINT 2-ADIC COMPLEXITY OF BINARY MULTISEQUENCES *

Lu Zhao[1] and Qiao-Yan Wen[2]

Abstract. Joint 2-adic complexity is a new important index of the cryptographic security for multisequences. In this paper, we extend the usual Fourier transform to the case of multisequences and derive an upper bound for the joint 2-adic complexity. Furthermore, for the multisequences with p^n-period, we discuss the relation between sequences and their Fourier coefficients. Based on the relation, we determine a lower bound for the number of multisequences with given joint 2-adic complexity.

Mathematics Subject Classification. 11T71, 14G50, 94A60.

1. Introduction

Many modern stream ciphers combine the output of several linear feedback shift registers (LFSR) in various nonlinear fashions. Since 1955, a large amount of effort has been spent on other feedback architectures to generate nonlinear sequences. In 1994, Klapper and Goresky [5] introduced a new feedback shift register with carry operation, called feedback with carry shift register (FCSR). Some basic properties

Keywords and phrases. Cryptography, stream cipher, FCSR, joint 2-adic complexity, usual Fourier transform.

* *This work is supported by NSFC (Grant Nos. 61170270611002036087319 1, 60903152, 61003286, 60821001), and the Fundamental Research Funds for the Central Universities (Grant Nos. BUPT2011YB01, BUPT2011RC0505).*

[1] State Key Laboratory of Networking and Switching Technology, P.O. Box 305, Beijing University of Posts and Telecommunications, Beijing 100876, P.R. China.
zhaolu.nan@gmail.com

[2] State Key Laboratory of Networking and Switching Technology, Beijing University of Posts and Telecommunications, Beijing 100876, P.R. China.

Article published by EDP Sciences

© EDP Sciences 2012

https://doi.org/10.1051/ita/2012011 Published online by Cambridge University Press

of sequences generated by an FCSR were also discussed, which showed FCSR sequences share many important properties with linear recurring sequences.

2-adic complexity, as one of the properties of FCSR sequences, was proposed by Klapper and Goresky [5]. It is used to measure how large an FCSR is required to output the sequence. As with the linear complexity, a large 2-adic complexity should be possessed for binary periodic sequences to thwart an attack by the rational approximation algorithm (an analog of the Berlakamp-Massey algorithm) [5]. However, since 2-adic complexity and linear complexity represent two different sequence generating architectures, sequences with high linear complexity may have low 2-adic complexity, and *vice versa* [9]. Thus, the 2-adic complexity is an important index of the cryptographic security for sequences used in cryptosystems.

The complexity of multisequences is required in the theory of word-based stream ciphers which has aroused people's interest of study in recent years. A lot of research has been on the linear complexity of multisequences [2,7,8], but not much on the 2-adic complexity. Hu and Feng proposed the concept of joint 2-adic complexity [4], then they obtained the form of the joint 2-adic complexity of multisequence with period L and the number of multisequences with given joint 2-adic complexity, where L is positive and the canonical factorization of $2^L - 1$ is known. However, the factoring of $2^L - 1$ is very difficult when L is large. So, to avoid factoring large integers, it is necessary to look for another method to study the joint 2-adic complexity of such multisequences.

The usual (complex) Fourier transform is a useful tool to investigate the properties of complexity measures for sequences [3, 6]. In this paper, we extend the relationship between the 2-adic complexity of an L-periodic binary sequence and the usual (complex) Fourier transform of L-tuples to the case of multisequences, where L is odd. Using the usual Fourier transform, we give the form of the upper bound for joint 2-adic complexity of any L-periodic multisequence with the canonical factorization of L, which is much easier to obtain than that of $2^L - 1$. For the case of $L = p^n$, (p prime, $p > 2$), we also determine a lower bound for the number of multisequences with given joint 2-adic complexity. Our results may be helpful to further study and design stream cipher generation.

2. Preliminaries

An FCSR (Fig. 1) is determined by r coefficients $q_1, q_2, \ldots, q_r$, where $q_i \in \{0, 1\}, i = 1, 2, \ldots, r$, and an initial memory m_{r-1}. The contents of the register at any given time consist of r bits, denotes $(a_{n-1}, a_{n-2}, \ldots, a_{n-r+1}, a_{n-r})$ and the memory is m_{n-1}. The operation of the shift register is defined as follows:

(1) form the integer sum $\sigma_n = \sum_{k=1}^{r} q_k a_{n-k} + m_{n-1}$;
(2) shift the contents one step to the right, while outputting the rightmost bit a_{n-r};
(3) put $a_n \equiv \sigma_n \bmod 2$ into the leftmost cell of the shift register;
(4) replace the memory integer m_{n-1} with $\frac{\sigma_n - a_n}{2}$.

https://doi.org/10.1051/ita/2012011 Published online by Cambridge University Press

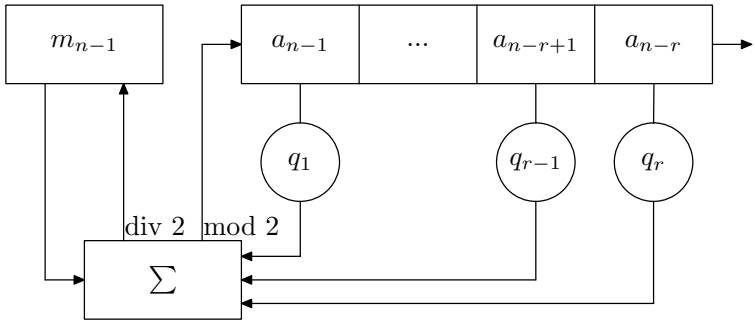


FIGURE 1. Feedback with carry shift register.

The integer $q = -1 + q_1 2 + q_2 2^2 + \ldots + q_r 2^r$ is called the connection integer of the FCSR.

Any infinite binary sequence $S = \{a_i\}_{i=0}^{\infty}$ can be presented by a formal power series $\alpha = \sum_{i=0}^{\infty} a_i 2^i$ called a 2-adic number. Such power series forms the ring of 2-adic numbers, denoted as Z_2. If S is strictly periodic with minimal period L, then $\alpha = \sum_{i=0}^{\infty} a_i 2^i = -\frac{\sum_{i=0}^{L-1} a_i 2^i}{2^L - 1} = -\frac{p}{q}$, where $0 \le p \le q$. If $\gcd(p, q) = 1, -\frac{p}{q}$ is called the reduced rational expression of S.

Definition 2.1 ([5]). Let S be a periodic binary sequence with reduced rational expression $-\frac{p}{q}$, then the 2-adic complexity $\lambda_2(S)$ is the real number $\log_2 q$.

Consider m periodic sequences $S_1, S_2, \ldots, S_m$. Let $S_i = \{a_{i,0}, a_{i,1}, \ldots\}$ be a periodic binary sequence with period L, and the reduced rational expression of S_i be $-\frac{p_i}{q_i}$, where $1 \le i \le m$. Then $q = \mathrm{lcm}(q_1, q_2, \ldots, q_m)$ is the smallest integer such that there exists an FCSR with connection integer q which can generate $S_1, S_2, \ldots, S_m$ simultaneously, where lcm denotes the least common multiple.

Definition 2.2 ([4]). $\log_2 \mathrm{lcm}(q_1, q_2, \ldots, q_m)$ is called the joint 2-adic complexity of the m sequences $S_1, S_2, \ldots, S_m$, and is denoted by $\lambda_2(S_1, S_2, \ldots, S_m)$.

Definition 2.3. For $k = 0, 1, \ldots, L-1, \gcd(L, 2) = 1$, the kth Fourier coefficient of the m L-tuples $S_1, S_2, \ldots, S_m$ is $\hat{\mathbf{a}}_k = (\hat{a}_{1,k}, \hat{a}_{2,k}, \ldots, \hat{a}_{m,k})$, where $\hat{a}_{i,k} = \sum_{j=0}^{L-1} a_{i,j} \zeta^{kj}$, $0 \le k \le L-1, 1 \le i \le m$, and $\zeta \in \mathbb{C}$ is a complex primitive Lth root of unity.

The set of Fourier coefficients $\{\hat{\mathbf{a}}_0, \hat{\mathbf{a}}_1, \ldots, \hat{\mathbf{a}}_{L-1}\}$ is the usual Fourier transform of $S_1, S_2, \ldots, S_m$. We denote by $\sigma(S_1, S_2, \ldots, S_m)$ the number of nonzero Fourier coefficients of $S_1, S_2, \ldots, S_m$, that is $\sigma(S_1, S_2, \ldots, S_m) = |\{\hat{\mathbf{a}}_k \ne \mathbf{0}, 0 \le k \le L-1\}|$, where $\mathbf{0} = (0, 0, \ldots, 0)$.

For any $1 \le i \le m$, let $S_i^L = \{a_{i,0}, a_{i,1}, \ldots, a_{i,L-1}\}$, $A_i^L = \{\hat{a}_{i,0}, \hat{a}_{i,1}, \ldots, \hat{a}_{i,L-1}\}$. If S_i^L and A_i^L are written as row vectors, then we can describe the usual Fourier

https://doi.org/10.1051/ita/2012011 Published online by Cambridge University Press

transform of S_i in matrix form by $A_i^L = S_i^L T$, where

$$T = \begin{pmatrix} 1 & 1 & 1 & \dots & 1 \\ 1 & \zeta & \zeta^2 & \dots & \zeta^{L-1} \\ 1 & \zeta^2 & \zeta^4 & \dots & \zeta^{2(L-1)} \\ \vdots & \vdots & \vdots & \dots & \vdots \\ 1 & \zeta^{L-1} & \zeta^{2(L-1)} & \dots & \zeta^{(L-1)^2} \end{pmatrix}.$$

Evidently, the matrix T is nonsingular, so the usual Fourier transform of $S_1, S_2, \dots, S_m$ is a bijection.

Let $\mathbb{Q}$ denote the field of rational numbers, the splitting field of $x^L - 1$ over $\mathbb{Q}$ is called a cyclotomic field extension and denoted by $\mathbb{Q}(\zeta)$.

Definition 2.4 ([1])**.** The Lth cyclotomic polynomial is defined to be that polynomial whose roots are exactly the primitive Lth roots of unity, denoted by $\Phi_L(x)$.

Obviously, the degree of $\Phi_L(x)$ is $\varphi(L)$, where $\varphi(\cdot)$ is the Euler function.

Lemma 2.5 ([1])**.** *$\Phi_L(x)$ is irreducible over the rationals.*

Lemma 2.6 ([1])**.** *Let $\mathbb{F}$ be a field, n an integer and η a primitive nth root of unity. If $\Phi_n(x)$ is irreducible over $\mathbb{F}$, then $\mathbb{F}(\eta)$ is a vector space over $\mathbb{F}$ of dimension $\varphi(n)$, and $\{1, \eta, \eta^2, \dots, \eta^{\varphi(n)-1}\}$ is a basis.*

Corollary 2.7. *$\{1, \zeta, \zeta^2, \dots, \zeta^{\varphi(L)-1}\}$ is a basis of $\mathbb{Q}(\zeta)$ over $\mathbb{Q}$.*

3. The upper bound for joint 2-adic complexity of multisequences

In this section, we introduce the usual Fourier transform of binary multisequences, and then by using it, we derive the form of an upper bound for joint 2-adic complexity of multisequences with period L, where $\gcd(L, 2) = 1$.

Let $S_i^L(x) = \sum_{j=0}^{L-1} a_{i,j} x^j = u_i(x) f_i(x)$, $x^L - 1 = u_i(x) g_i(x)$ and $\gcd(f_i(x), g_i(x)) = 1$, where $1 \le i \le m$. Put $g(x) = \mathrm{lcm}(g_1(x), g_2(x), \dots, g_m(x))$. Note that $f_i(2)$ and $g_i(2)$ are not always relatively prime even if $\gcd(f_i(x), g_i(x)) = 1$. Then $q \le g(2)$, that is $\lambda_2(S_1, S_2, \dots, S_m) \le \log_2(g(2))$.

Lemma 3.1. $\deg(g(x)) = \sigma(S_1, S_2, \dots, S_m)$.

Proof. For all $k, 0 \le k \le L-1, \hat{\mathbf{a}}_k \ne \mathbf{0}$, then there exists an $i, 1 \le i \le m$, such that $\hat{a}_{i,k} \ne 0$, that is $S_i^L(\zeta^k) \ne 0$. Hence $u_i(\zeta^k) \ne 0$, that is $g_i(\zeta^k) = 0$. So $g(\zeta^k) = 0$. Conversely, if $g(\zeta^k) = 0$, then there also exists an $i, 1 \le i \le m$, such that $g_i(\zeta^k) = 0$. Because $x^L - 1$ has no multiple roots, we have $u_i(\zeta^k) \ne 0$. Hence $S_i^L(\zeta^k) \ne 0$, that is $\hat{a}_{i,k} \ne 0$. So $\hat{\mathbf{a}}_k \ne \mathbf{0}$. In a word, for all $k, 0 \le k \le L-1$, $\hat{\mathbf{a}}_k \ne \mathbf{0}$

https://doi.org/10.1051/ita/2012011 Published online by Cambridge University Press

if and only if $g(\zeta^k) = 0$. On the other hand, $g(x)$ has $\deg(g(x))$ complex roots and all are of the form ζ^k. Hence $\deg(g(x)) = \sigma(S_1, S_2, \ldots, S_m)$. □

Since $g(x)$ divides $x^L - 1$, let $g(x) = \prod_{j=1}^{t} \Phi_{n_j}(x)$, where $n_j | L$. Let n be a positive integer and let $m = \prod_{p|n} p = s(n)$ denote the largest square-free integer dividing n. For any positive integer n, the Moebius function is defined by:

$$\nu(n) = \begin{cases} (-1)^k, & \text{if } n \text{ is square-free and has } k \text{ distinct positive prime factors,} \\ 0, & \text{otherwise.} \end{cases}$$

Lemma 3.2 ([3])**.** *Fix a positive square-free integer $m \geq 1$. Then*

$$\sum_{s(n)=m} \log_2 \left(\frac{\Phi_n(2)}{2^{\varphi(n)}} \right) = -\nu(m)$$

and all terms in the sum have the same sign.

Similar to the reduction of Theorem II.2 in [3], we derive an upper bound for the joint 2-adic complexity of multisequences with period L.

Theorem 3.3. *Let $S_1, S_2, \ldots, S_m$ be m binary sequences with period L, where $\gcd(L, 2) = 1$. Then the 2-adic complexity $\lambda_2(S_1, S_2, \ldots, S_m)$ is bounded as follows:*

$$\lambda_2(S_1, S_2, \ldots, S_m) < \sigma(S_1, S_2, \ldots, S_m) + 2^{\omega(L)-1}$$

where $\omega(L)$ denotes the number of distinct positive prime divisions of L.

Proof. We have $\log_2(g(2)) = \sum_{j=1}^{t} \log_2(\Phi_{n_j}(2)) = \sum_{j=1}^{t} \left(\varphi(n_j) + \log_2 \left(\frac{\Phi_{n_j}(2)}{2^{\varphi(n_j)}} \right) \right) =$ $\deg(g(x)) + \sum_{j=1}^{t} \log_2 \left(\frac{\Phi_{n_j}(2)}{2^{\varphi(n_j)}} \right)$. Let $O = \{n_j | s(n_j) = m_j \text{ and } \nu(m_j) = -1\}$. Then $\log_2(g(2)) \leq \deg(g(x)) + \sum_{m_j \in O} \log_2 \left(\frac{\Phi_{n_j}(2)}{2^{\varphi(n_j)}} \right)$, from Lemma 2.2, we have $\log_2(g(2)) < \deg(g(x)) + 2^{\omega(L)-1}$, that is $\log_2(g(2)) < \sigma(S_1, S_2, \ldots, S_m) + 2^{\omega(L)-1}$. □

Next we obtain a simpler form of the upper bound in Theorem 3.3. From the definition of Fourier coefficient, we have $\hat{a}_{i,t} = S_i^L(\zeta^t)$. Consider $S_i^L(x)$ as a polynomial whose coefficients belong to $\mathbb{Q}$.

Lemma 3.4. *Let $0 \leq t_1, t_2 < L$, for $\gcd(t_1, L) = \gcd(t_2, L)$, then $\hat{\mathbf{a}}_{t_1} = \boldsymbol{0}$ if and only if $\hat{\mathbf{a}}_{t_2} = \boldsymbol{0}$, where $\boldsymbol{0} = (0, 0, \ldots, 0)$.*

Proof. For any $i, 1 \leq i \leq m$, we have $\hat{a}_{i,t_1} = S_i^L(\zeta^{t_1})$ and $\hat{a}_{i,t_2} = S_i^L(\zeta^{t_2})$. Let $\gcd(t_1, L) = \gcd(t_2, L) = d$, then ζ^{t_1} and ζ^{t_2} are both primitive $\frac{L}{d}$th roots of unity. From Lemma 2.5, $\Phi_{\frac{L}{d}}(x)$ is irreducible over $\mathbb{Q}$. Hence ζ^{t_1} and ζ^{t_2} are Galois conjugates and have the same minimal polynomial. Let $q(x)$ be the minimal polynomial of ζ^{t_1} and ζ^{t_2} over $\mathbb{Q}$. Then $S_i^L(\zeta^{t_1}) = 0$ if and only if $q(x) \mid S_i^L(x)$ if and

https://doi.org/10.1051/ita/2012011 Published online by Cambridge University Press

only if $S_i^L(\zeta^{t_2}) = 0$, that is $\hat{a}_{i,t_1} = 0$ if and only if $\hat{a}_{i,t_2} = 0$. So $\hat{\mathbf{a}}_{t_1} = \mathbf{0}$ if and only if $\hat{\mathbf{a}}_{t_2} = \mathbf{0}$. □

Let $C_j = \{t | \gcd(t, L) = j, 0 \le t < L\}$, h be an integer. Let $\{j_1, j_2, \ldots, j_h\}$ be the set of positive divisors of L. The $C_{j_1} \cup C_{j_2} \cup \ldots \cup C_{j_h} = \{0, 1, \ldots, L-1\}$ and these sets are pairwise disjoint. Let $|C_{j_i}| = l_{j_i}$, $1 \le i \le h$. We choose any h numbers from $\{0, 1, \ldots, L-1\}$,denoted by $t_{j_1}, t_{j_2}, \ldots, t_{j_h}$, which satisfy $\gcd(t_{j_i}, L) = j_i$, that is $t_{j_i} \in C_{j_i}, 1 \le i \le h$. From Lemma 3.4, we know that $\hat{\mathbf{a}}_0, \hat{\mathbf{a}}_1, \ldots, \hat{\mathbf{a}}_{L-1}$ are not independent, and $\sigma(S_1, S_2, \ldots, S_m) = \sum_{\hat{\mathbf{a}}_{t_{j_i}} \neq \mathbf{0}, 1 \le i \le h} l_{j_i}$. So the upper bound for joint 2-adic complexity of $S_1, S_2, \ldots, S_m$ can be written as a linear combination of the cardinalities of $C_{j_1}, C_{j_2}, \ldots, C_{j_h}$, exactly as described in the following theorem.

Theorem 3.5. *Let $S_1, S_2, \ldots, S_m$ be m L-tuples binary sequences, where $\gcd(L, 2) = 1$. Put $C_{j_i} = \{t | \gcd(t, L) = j_i, 0 \le t < L\}, 1 \le i \le h$, and $|C_{j_i}| = l_{j_i}$. Then the joint 2-adic complexity $\lambda_2(S_1, S_2, \ldots, S_m)$ is bounded as follows:*

$$\lambda_2(S_1, S_2, \ldots, S_m) < \sum_{i=1}^{h} \mu_i l_{j_i} + 2^{\omega(L)-1}, \quad \mu_i \in \{0, 1\},$$

where $\omega(L)$ denotes the number of distinct positive prime divisors of L.

Remark 3.6. We keep the above notation, in Theorem 3.5,

$$\mu_i = \begin{cases} 1, & \hat{\mathbf{a}}_{t_{j_i}} \neq \mathbf{0}, t_{j_i} \in C_{j_i} \\ 0, & \hat{\mathbf{a}}_{t_{j_i}} = \mathbf{0}, t_{j_i} \in C_{j_i} \end{cases}, \quad 0 \le t_{j_i} < L, \quad 1 \le i \le h.$$

The above theorem shows that the upper bound of joint 2-adic complexity is determined by h vectors $\hat{\mathbf{a}}_{t_{j_i}}, 1 \le i \le h$, one vector corresponding to each C_{j_i}.

4. The upper bound for joint 2-adic complexity and counting function of p^n-periodic binary multisequences

In this section, we study the joint 2-adic complexity of multisequences with period p^n, where p is a prime and $p > 2$. A sufficient and necessary condition for zero Fourier coefficient is firstly given out, and with the condition, we derive a lower bound for the number of p^n-periodic multisequences with given joint 2-adic complexity. Define $\mathcal{N}_{L,\sigma}(c)$ and $\mathcal{N}_{L,\lambda_2}(c')$ to be the number of m L-tuples $S_1, S_2, \ldots, S_m$ with $\sigma(S_1, S_2, \ldots, S_m) = c$ and $\lambda_2(S_1, S_2, \ldots, S_m) = c'$, respectively.

https://doi.org/10.1051/ita/2012011 Published online by Cambridge University Press

Theorem 4.1. *Let $L = p^n$, p is a prime and $p > 2$, for any t with $\gcd(t, L) = p^{n-d}, 0 < t < L, 0 < d \leq n$, $\hat{\mathbf{a}}_t = \boldsymbol{0}$ if and only if $\sum_{l=0}^{p^{n-d}-1}(a_{i,lp^d+(k-1)p^{d-1}+j} - a_{i,(l+1)p^d-p^{d-1}+j}) = 0$, for all $1 \leq i \leq m, 0 \leq j \leq p^{d-1}-1, 1 \leq k \leq p-1$. Also $\hat{\mathbf{a}}_0 = \boldsymbol{0}$ if and only if $(a_{i,0}, a_{i,1}, \ldots, a_{i,L-1}) = (0, 0, \ldots, 0)$, $1 \leq i \leq m$.*

Proof. Since $\gcd(t, L) = p^{n-d}, 0 < d \leq n$, it follows that ζ^t is a p^dth primitive root of unity. From Lemmas 2.5 and 2.6, we have $\{1, \zeta^t, \zeta^{2t}, \ldots, \zeta^{(p^d-p^{d-1}-1)t}\}$ is a basis of $\mathbb{Q}(\zeta^t)$. Let

$$\begin{aligned} S_i^{p^n}(x) &= a_{i,0} + a_{i,1}x + \ldots + a_{i,p^n-1}x^{p^n-1} \\ &= \sum_{l=0}^{p^{n-d}-1} x^{lp^d}(a_{i,lp^d} + a_{i,lp^d+1}x + \ldots + a_{i,lp^d+(p^d-1)}x^{p^d-1}). \end{aligned}$$

Since $\Phi_{p^d}(x) = 1 + x^{p^{d-1}} + x^{2p^{d-1}} + \ldots + x^{(p-1)p^{d-1}}$, we have $x^{lp^d} \equiv 1 \bmod \Phi_{p^d}(x)$ and

$$\begin{aligned} &a_{i,lp^d} + a_{i,lp^d+1}x + \ldots + a_{i,lp^d+(p^d-1)}x^{p^d-1} \\ &\equiv \sum_{j=0}^{p^{d-1}-1}\sum_{k=1}^{p-1}(a_{i,lp^d+(k-1)p^{d-1}+j} - a_{i,(l+1)p^d-p^{d-1}+j})x^{(k-1)p^{d-1}+j} \bmod \Phi_{p^d}(x), \end{aligned}$$

then

$$\begin{aligned} &S_i^{p^n}(x) \bmod \Phi_{p^d}(x) \\ &\equiv \sum_{j=0}^{p^{d-1}-1}\sum_{k=1}^{p-1}\left[\sum_{l=0}^{p^{n-d}-1}\left(a_{i,lp^d+(k-1)p^{d-1}+j} - a_{i,(l+1)p^d-p^{d-1}+j}\right)\right]x^{(k-1)p^{d-1}+j}. \end{aligned}$$

So, for each $1 \leq i \leq m$, $S_i^{p^n}(\zeta^t) = 0$ if and only if for all $0 \leq j \leq p^{d-1}-1$ and $1 \leq k \leq p-1$, we have $\sum_{l=0}^{p^{n-d}-1}(a_{i,lp^d+(k-1)p^{d-1}+j} - a_{i,(l+1)p^d-p^{d-1}+j}) = 0$.

For $a_{i,j} \in \{0, 1\}, 1 \leq i \leq m, 0 \leq j < L$, then $\hat{\mathbf{a}}_0 = \mathbf{0}$ if and only if $\hat{a}_{i,0} = \sum_{j=0}^{L-1} a_{i,j} = 0, 1 \leq i \leq m$ if and only if $a_{i,j} = 0$. So $\hat{\mathbf{a}}_0 = \mathbf{0}$ if and only if $(a_{i,0}, a_{i,1}, \ldots, a_{i,L-1}) = (0, 0, \ldots, 0)$, $1 \leq i \leq m$. □

From the proof of Theorem 4.1, we have $\hat{\mathbf{a}}_0 = \mathbf{0}$ if and only if $\sigma(S_1, S_2, \ldots, S_m) = 0$.

Lemma 4.2. *If $C_{p^d} = \{t | \gcd(t, p^n) = p^d, 0 < t < p^n\}, 0 \leq d < n$, then $|C_{p^d}| = p^{n-d} - p^{n-d-1}$. Also, $|C_{p^n}| = 1$.*

Hence, for m p^n-tuples, $\sigma(S_1, S_2, \ldots, S_m) = 0$ or $1 + \sum_{d \in \mathcal{A}}(p^{n-d} - p^{n-d-1})$, where $\mathcal{A} \subset \{0, 1, \ldots, n-1\}$. For $1 < u \leq n-1$, we have $\sum_{i=1}^{u-1}(p^i - p^{i-1}) = p^{u-1} - 1 < p^u - p^{u-1}$. Thus, the representation of each possible $\sigma(S_1, S_2, \ldots, S_m)$ as a partial sum of $|C_{p^d}|, (0 \leq d \leq n)$ is unique.

https://doi.org/10.1051/ita/2012011 Published online by Cambridge University Press

Let $\mathcal{O} = \{0, 1, \ldots, n-1\}$. *If* $\sigma(S_1, S_2, \ldots, S_m) = \sum_{d\in\mathcal{A}}(p^{n-d} - p^{n-d-1}) + 1 = c$, *where* $\mathcal{A} \subset \mathcal{O}$. *Then* $L - \sigma(S_1, S_2, \ldots, S_m) = \sum_{d\in\mathcal{O}\setminus\mathcal{A}}(p^{n-d} - p^{n-d-1})$. *We have*

$$\begin{cases} \hat{\mathbf{a}}_{p^{n-d}} \neq \boldsymbol{0}, & d \in \mathcal{A} \\ \hat{\mathbf{a}}_{p^{n-d}} = \boldsymbol{0}, & d \in \mathcal{O} \setminus \mathcal{A}. \end{cases}$$

With the above analysis, we establish a lower bound for $\mathcal{N}_{p^n,\lambda_2}(c')$. *For* $0 < d \leq n$, *let*

$$A_{p^{n-d}} = \Bigg\{ (S_1, S_2, \ldots, S_m) \,|S_i = (a_{i,0}, a_{i,1}, \ldots, a_{i,L-1}) \in \{0,1\}^L, \sum_{l=0}^{p^{n-d}-1} (a_{i,lp^d+(k-1)p^{d-1}+j} - a_{i,(l+1)p^d-p^{d-1}+j}) = 0, \; 1 \leq i \leq m, 0 \leq j \leq p^{d-1}-1, 1 \leq k \leq p-1 \Bigg\},$$

$$A_{p^n} = \{(S_1, S_2, \ldots, S_m) | S_i = (0, 0, \ldots, 0), 1 \leq i \leq m\}.$$

Theorem 4.3. *Let* c' *be an integer,* $c = \min\{\sum_{d\in\mathcal{A}}(p^{n-d} - p^{n-d-1}) + 1 | \sum_{d\in\mathcal{A}}(p^{n-d} - p^{n-d-1}) + 1 \geq c' - 1, \mathcal{A} \subset \mathcal{O}\}$, *then* $\mathcal{N}_{p^n,\lambda_2}(c') \geq \mathcal{N}_{p^n,\sigma}(c)$.

Proof. Obviously, $|\ A_{p^{n-d}}\ | \leq |\ \bar{A}_{p^{n-d}}\ |$, where $\bar{A}_{p^{n-d}}$ denotes the complementary set of $A_{p^{n-d}}$. So, if $c_1 \geq c_2$, then $\mathcal{N}_{p^n,\sigma}(c_1) \geq \mathcal{N}_{p^n,\sigma}(c_2)$. From Theorem 3.3, $\lambda_2(S_1, S_2, \ldots, S_m) < \sigma(S_1, S_2, \ldots, S_m) + 2^{\omega(p^n)-1}$, $\lambda_2(S_1, S_2, \ldots, S_m) = c'$, then $\sigma(S_1, S_2, \ldots, S_m) > c' - 1$, so $\sigma(S_1, S_2, \ldots, S_m) \geq c$. Hence we have $\mathcal{N}_{p^n,\lambda_2}(c') \geq \mathcal{N}_{p^n,\sigma}(c)$. □

In the following, we obtain the value of $\mathcal{N}_{p^n,\sigma}(c)$. From Theorem 3.5, $\mathcal{N}_{p^n,\sigma}(c) = |\bigcap_{d\in\mathcal{O}\setminus\mathcal{A}} A_{p^{n-d}} \bigcap_{d\in\mathcal{A}} \bar{A}_{p^{n-d}}|$. Firstly, we calculate $|A_{p^{n-d_{j_1}}} \bigcap A_{p^{n-d_{j_2}}} \bigcap \ldots \bigcap A_{p^{n-d_{j_e}}}|$, where $n \geq d_{j_1} > d_{j_2} > \ldots > d_{j_e} \geq 1$. If $(S_1, S_2, \ldots, S_m) \in A_{p^{n-d_{j_1}}}$, then for any $i, 1 \leq i \leq m$, and $j, 0 \leq j \leq p^{d_{j_1}-1} - 1$, we have

$$\sum_{l=0}^{p^{n-d_{j_1}}-1} a_{i,lp^{d_{j_1}}+j} = \sum_{l=0}^{p^{n-d_{j_1}}-1} a_{i,lp^{d_{j_1}}+p^{d_{j_1}-1}+j}$$

$$= \ldots = \sum_{l=0}^{p^{n-d_{j_1}}-1} a_{i,lp^{d_{j_1}}+(p-1)p^{d_{j_1}-1}-p^{d_{j_1}-1}+j}$$

$$= \sum_{l=0}^{p^{n-d_{j_1}}-1} a_{i,(l+1)p^{d_{j_1}}-p^{d_{j_1}-1}+j}.$$

https://doi.org/10.1051/ita/2012011 Published online by Cambridge University Press

Similarly, if $(S_1, S_2, \ldots, S_m) \in A_{p^{n-d_{j_r}}}, 2 \le r \le e$, then for any $i, 1 \le i \le m$, and $j, 0 \le j \le p^{d_{j_r}-1} - 1$, we have

$$\sum_{l=0}^{p^{n-d_{j_r}}-1} a_{i,lp^{d_{j_r}}+j} = \ldots = \sum_{l=0}^{p^{n-d_{j_r}}-1} a_{i,(l+1)p^{d_{j_r}}-p^{d_{j_r}-1}+j}. \tag{4.1}$$

Obviously, for $i, 1 \le i \le m$, and $j, 0 \le j \le p^{d_{j_r}-1} - 1$,

$$\begin{aligned}
&\sum_{l=0}^{p^{n-d_{j_r}}-1} a_{i,lp^{d_{j_r}}+j} = \Bigg(\sum_{l=0}^{p^{n-d_{j_1}}-1} a_{i,lp^{d_{j_1}}+j} + \sum_{l=0}^{p^{n-d_{j_1}}-1} a_{i,lp^{d_{j_1}}+p^{d_{j_1}-1}+j} + \ldots \\
&+ \sum_{l=0}^{p^{n-d_{j_1}}-1} a_{i,lp^{d_{j_1}}+(p-1)p^{d_{j_1}-1}+j} \Bigg) \\
&+ \Bigg(\sum_{l=0}^{p^{n-d_{j_1}}-1} a_{i,lp^{d_{j_1}}+p^{d_{j_r}}+j} + \sum_{l=0}^{p^{n-d_{j_1}}-1} a_{i,lp^{d_{j_1}}+p^{d_{j_r}}+p^{d_{j_1}-1}+j} + \ldots \\
&+ \sum_{l=0}^{p^{n-d_{j_1}}-1} a_{i,lp^{d_{j_1}}+p^{d_{j_r}}+(p-1)p^{d_{j_1}-1}+j} \Bigg) + \ldots \\
&+ \Bigg(\sum_{l=0}^{p^{n-d_{j_1}}-1} a_{i,lp^{d_{j_1}}+\left(p^{d_{j_1}-d_{j_r}-1}-1\right)p^{d_{j_r}}+j} \\
&+ \sum_{l=0}^{p^{n-d_{j_1}}-1} a_{i,lp^{d_{j_1}}+\left(p^{d_{j_1}-d_{j_r}-1}-1\right)p^{d_{j_r}}p^{d_{j_1}-1}+j} \cdots \\
&+ \sum_{l=0}^{p^{n-d_{j_1}}-1} a_{i,lp^{d_{j_1}}+\left(p^{d_{j_1}-d_{j_r}-1}-1\right)p^{d_{j_r}}+(p-1)p^{d_{j_1}-1}+j} \Bigg), \\
&\cdots \\
&\sum_{l=0}^{p^{n-d_{j_r}}-1} a_{i,lp^{d_{j_r}}+p^{d_{j_r}-1}+j} \\
&= \Bigg(\sum_{l=0}^{p^{n-d_{j_1}}-1} a_{i,lp^{d_{j_1}}+p^{d_{j_r}-1}+j} + \ldots + \sum_{l=0}^{p^{n-d_{j_1}}-1} a_{i,lp^{d_{j_1}}+p^{d_{j_r}-1}+(p-1)p^{d_{j_1}-1}+j} \Bigg) \\
&+ \ldots \\
&+ \Bigg(\sum_{l=0}^{p^{n-d_{j_1}}-1} a_{i,lp^{d_{j_1}}+p^{d_{j_r}-1}+\left(p^{d_{j_1}-d_{j_r}-1}-1\right)p^{d_{j_r}}+j} + \ldots \\
&+ \sum_{l=0}^{p^{n-d_{j_1}}-1} a_{i,lp^{d_{j_1}}+p^{d_{j_r}-1}+\left(p^{d_{j_1}-d_{j_r}-1}-1\right)p^{d_{j_r}}+(p-1)p^{d_{j_1}-1}+j} \Bigg).
\end{aligned}$$

https://doi.org/10.1051/ita/2012011 Published online by Cambridge University Press

For any $i, 1 \le i \le m$, and $k, 1 \le k \le p$, let

$$\begin{cases} \sum_{l=0}^{p^{n-d_{j_1}}-1} a_{i,lp^{d_{j_1}}+(k-1)p^{d_{j_1}-1}} = k_{i,1} \\ \sum_{l=0}^{p^{n-d_{j_1}}-1} a_{i,lp^{d_{j_1}}+(k-1)p^{d_{j_1}-1}+p^{d_{j_e}-1}} = k_{i,2} \\ \vdots \\ \sum_{l=0}^{p^{n-d_{j_1}}-1} a_{i,lp^{d_{j_1}}+kp^{d_{j_1}-1}-p^{d_{j_e}-1}} = k_{i,p^{d_{j_1}}-d_{j_e}}. \end{cases}$$

From equation (4.1), if $(S_1, S_2, \ldots, S_m) \in A_{p^{n-d_{j_1}}} \bigcap A_{p^{n-d_{j_r}}}$, then $k_{i,1}, k_{i,2}, \ldots, k_{i,p^{d_{j_1}}-d_{j_e}}$ should satisfy:

$$\begin{aligned} \sum_{l=0}^{p^{d_{j_1}}-d_{j_r}-1-1} k_{i,lp^{d_{j_r}-d_{j_e}+1}+s} &= \sum_{l=0}^{p^{d_{j_1}}-d_{j_r}-1-1} k_{i,lp^{d_{j_r}-d_{j_e}+1}+p^{d_{j_r}-d_{j_e}}+s} \\ &= \ldots \\ &= \sum_{l=0}^{p^{d_{j_1}}-d_{j_r}-1-1} k_{i,lp^{d_{j_r}-d_{j_e}+1}+(p-1)p^{d_{j_r}-d_{j_e}}+s}, \end{aligned}$$

where $1 \le s \le p^{d_{j_r}-d_{j_e}}$.

We denote the above set of equations as $B(d_{j_1}, d_{j_r})$. Let N be the number of $(k_{i,1}, k_{i,2}, \ldots, k_{i,p^{d_{j_1}}-d_{j_e}})$ which satisfies equations $B(d_{j_1}, d_{j_2}), \ldots, B(d_{j_1}, d_{j_e})$ simultaneously, where $1 \le i \le m$. From the above analysis, we know $|A_{p^{n-d_{j_1}}} \bigcap \ldots \bigcap A_{p^{n-d_{j_e}}}| = N^{p^{d_{j_e}-1}}$. So

$$\left|A_{p^{n-d_{j_1}}} \bigcap \ldots \bigcap A_{p^{n-d_{j_e}}}\right| = \left\{ \sum_{\substack{B(d_{j_1},d_{j_2}),\ldots,B(d_{j_1},d_{j_e}),\\ 0\le k_{i,t}\le p^{n-d_{j_1}},1\le i\le m,\\ 1\le t\le p^{d_{j_1}-d_{j_e}}}} \prod_{t=1}^{p^{d_{j_1}}-d_{j_e}} \left[\binom{p^{n-d_{j_1}}}{k_{i,t}}\right]^p \right\}^{p^{d_{j_e}-1}}. \tag{4.2}$$

In particular, $|A_{p^{n-d_{j_1}}} \bigcap A_{p^{n-d_{j_2}}} \bigcap \ldots \bigcap A_{p^n}| = 1$. Then according to the Inclusion-Exclusion Principle,

$$\mathcal{N}_{p^n,\sigma}(c) = \left|\bigcap_{d\in\mathcal{O}\setminus\mathcal{A}} A_{p^{n-d}}\right| - \sum_{s\in\mathcal{A}} \left|\bigcap_{d\in\mathcal{O}\setminus\mathcal{A}} A_{p^{n-d}} \bigcap A_{p^{n-s}}\right| + \sum_{s,t\in\mathcal{A}} \left|\bigcap_{d\in\mathcal{O}\setminus\mathcal{A}} A_{p^{n-d}} \bigcap A_{p^{n-s}} \bigcap A_{p^{n-t}}\right| - \ldots + (-1)^{|\mathcal{A}|} \left|\bigcap_{d\in\mathcal{O}} A_{p^{n-d}}\right|.$$

https://doi.org/10.1051/ita/2012011 Published online by Cambridge University Press

Example 4.4. Let $L = 3^2, m = 2$. We have $C_1 = \{1,2,4,5,7,8\}, C_3 = \{3,6\}, C_9 = \{0\}$. Then $\sigma(S_1,S_2)$ is the form $6\mu_1 + 2\mu_2 + 1$ or 0, where $\mu_1, \mu_2 \in \{0,1\}$. If $\sigma(S_1,S_2) = 7 = 1+6$, and $\hat{a}_3 = \hat{a}_6 = 0, \hat{a}_1 \neq 0, \hat{a}_2 \neq 0, \hat{a}_4 \neq 0, \hat{a}_5 \neq 0, \hat{a}_7 \neq 0, \hat{a}_8 \neq 0$. Let

$$\begin{aligned}
A_1 = \{&(S_1,S_2)|S_i = (a_{i,0}, a_{i,1}, \ldots, a_{i,8}) \in \{0,1\}^9,\\
&a_{i,0} = a_{i,3} = a_{i,6}, a_{i,1} = a_{i,4} = a_{i,7}, a_{i,2} = a_{i,5} = a_{i,8},\\
&1 \leq i \leq 2\},\\
A_3 = \{&(S_1,S_2)|S_i = (a_{i,0}, a_{i,1}, \ldots, a_{i,8}) \in \{0,1\}^9,\\
&a_{i,0} + a_{i,3} + a_{i,6} = a_{i,1} + a_{i,4} + a_{i,7} = a_{i,2} + a_{i,5} + a_{i,8},\\
&1 \leq i \leq 2\},\\
A_9 = \{&(S_1,S_2)|S_i = (0,0,\ldots,0), 1 \leq i \leq 2\}.
\end{aligned}$$

From Theorem 4.1, we have $\mathcal{N}_{9,\sigma}(7) = |A_3 \cap \bar{A}_1 \cap \bar{A}_9|$. Obviously, $|A_3| = \left[\sum_{t=0}^{3}\left(\binom{3}{t}\right)^3\right]^2 = 3136, |A_3 \cap A_9| = 1, |A_1 \cap A_3 \cap A_9| = 1$. In the following we calculate $|A_1 \cap A_3|$. Let

$$\begin{cases} a_{i,0} = a_{i,3} = a_{i,6} = k_{i,1} \\ a_{i,1} = a_{i,4} = a_{i,7} = k_{i,2} \\ a_{i,2} = a_{i,5} = a_{i,8} = k_{i,3}. \end{cases}, \quad 1 \leq i \leq 2$$

If $(S_1,S_2) \in A_3$, then $k_{i,1} = k_{i,2} = k_{i,3}$. So

$$|A_1 \cap A_3| = \sum_{\substack{k_{i,1}=k_{i,2}=k_{i,3},\\ 1\leq i\leq 2,\\ 0\leq k_{i,1},k_{i,2},k_{i,3}\leq 1}} \prod_{t=1}^{3}\left[\binom{1}{k_{i,t}}\right]^3 = 2^2 = 4.$$

Hence $|A_3 \cap \bar{A}_1 \cap \bar{A}_9| = |A_3| - (|A_1 \cap A_3| + |A_3 \cap A_9|) + |A_1 \cap A_3 \cap A_9| = 3132$, that is $\mathcal{N}_{9,\sigma}(7) = 3132$.

5. Conclusion

In this paper, we extend the usual Fourier transformation to the case of multisequences. Firstly, we define the Fourier coefficients of multisequences. By analyzing properties of Fourier coefficients, these coefficients can be divided into certain sets. Then an upper bound for joint 2-adic complexity can be written as a linear combination of the cardinalities of these sets. Focusing on binary multisequences with p^n-period, we obtain a sufficient and necessary condition for the Fourier coefficient to be zero. Based on the condition, we determine a lower bound for the number of sequences with given joint 2-adic complexity. In this correspondence, our analysis

https://doi.org/10.1051/ita/2012011 Published online by Cambridge University Press

is based on the canonical factorization of the period L of a sequence, which is simpler than that of $2^L - 1$.

Acknowledgements. We would like to express our sincere thanks to the referees for their constructive and positive comments which are very helpful to the improvement of this paper.

References

[1] W. Alun, Appendix A. *Circulants (Extract)* (2008); available at http://circulants.org/circ/
[2] F. Fu, H. Niederreiter and F. Özbudak, Joint linear complexity of multisequences consisting of linear recurring sequences. *Cryptogr. Commun.* **1** (2009) 3–29.
[3] M. Goresky, A. Klapper and L. Washington, Fourier tansform and the 2-adic span of periodic binary sequences. *IEEE Trans. Inf. Theory* **46** (2000) 687–691.
[4] H. Gu, L. Hu and D. Feng, On the expected value of the joint 2-adic complexity of periodic binary multisequences, in *Proc. of International Conference on Sequences and Their Applications*, edited by G. Gong *et al.* (2006) 199–208.
[5] A. Klapper and M. Goresky, Feedback shift registers. 2-adic span, and combiners with memory. *J. Cryptol.* **10** (1997) 111–147.
[6] W. Meidl and H. Niederreiter, Linear complexity, k-error linear complexity, and the discrete Fourier transform. *J. Complexity* **18** (2002) 87–103.
[7] W. Meidl and H. Niederreiter, The expected value of the joint linear complexity of periodic multisequences. *J. Complexity* **19** (2003) 1–13.
[8] W. Meidl, H. Niederreiter and A. Venkateswarlu, Error linear complexity measures for multisequences. *J. Complexity* **23** (2007) 169–192.
[9] C. Seo, S. Lee, Y. Sung, K. Han and S. Kim, A lower bound on the linear span of an FCSR. *IEEE Trans. Inf. Theory* **46** (2000) 691–693.

Communicated by G. Cohen.
Received September 20, 2011. Accepted February 16, 2012.

https://doi.org/10.1051/ita/2012011 Published online by Cambridge University Press