第43卷第2期 中国科学技术大学学报 Vol. 43, No. 2
2013年2月 JOURNAL OF UNIVERSITY OF SCIENCE AND TECHNOLOGY OF CHINA Feb. 2013

Article ID: 0253-2778(2013)02-0169-04

A fast algorithm for the 2-adic joint complexity of p^n-periodic a binary multisequence

LI Fulin, ZHU Shixin

(*Department of Applied Mathematics, Hefei University of Technology, Hefei* 230009, *China*)

Abstract: To determine the 2-adic joint complexity of p^n-periodic binary multisequences generated by feedback shift registers with carry operation (FCSR), an algorithm was presented and its theoretical derivation was provided, which yields an upper bound for the 2-adic joint complexity of a p^n-periodic binary multisequence. Under a fixed condition, this upper bound is good.

Key words: cryptology; multisequence; feedback shift register; 2-adic joint complexity

CLC number: TN918.4 **Document code**: A doi: 10.3969/j.issn.0253-2778.2013.02.013

Citation: Li Fulin, Zhu Shixin. A fast algorithm for the 2-adic joint complexity of p^n-periodic a binary multisequence[J]. Journal of University of Science and Technology of China, 2013, 43(2): 169-172.

p^n-周期二元多维序列2-adic联合复杂度快速算法

李富林,朱士信

(合肥工业大学数学学院,安徽合肥 230009)

摘要:本文提出了一个快速算法确定 p^n-周期二元FCSR多维序列2-adic联合复杂度,给出了该算法理论上的推导,产生了 p^n-周期二元多维序列2-adic联合复杂度一个上界,在确定的条件下,这个上界是好的.

关键词:密码学;多维序列;反馈移位寄存器;2-adic联合复杂度

0 Introduction

Klapper and Goresky introduced the notion of feedback with carry shift registers (FCSRs) which has received a lot of attention in cryptography[1-7]. Researches in this field mainly focused on FCSRs that generate sequences over $Z/(2)$. Some basic properties, such as periods, rational expressions, exponential representations, rational approximation algorithms and randomness of FCSR sequence based on the algebraic structure of 2-adic numbers, have been discussed.

Complexity measures, such as 2-adic complexity, 2-adic k-error complexity, are important concepts for the theory of streams ciphers in cryptology. Any sequence over $Z/(2)$ used as a key stream in a stream cipher must have large 2-adic complexity. In recent years, multisequence over finite fields has attracted a lot of attention. Recently, multisequences generated

Received: 2011-10-24; **Revised**: 2012-02-10

Foundation item: Supported by the Fundamental Research Funds for the Central Universities (2012HGBZ0622).

Biography: LI Fulin, male, born in 1979, PhD. Research field: cryptography. E-mail: lflsxx66@163.com

Corresponding author: ZHU Shixin, PhD/Prof. E-mail: zhushixin@hfut.edu.cn

by FCSRs over $Z/(2)$ have also attracted some attention. Hu et al[8] studied the expected value of the joint 2-adic complexity of periodic binary multisequence. There are no known efficient algorithms in the literature for computing the 2-adic joint complexity of a periodic multisequence. In this paper, we can compute an upper bound by giving an algorithm. Under a fixed condition, this upper bound is good.

This paper is organized as follows. In Section 1, we introduce the mathematical background of the algorithm. In Section 2, an algorithm to determine the upper bound of 2-adic joint complexity of multisequences is presented and an example is given. Finally, Section 3 concludes the paper.

1 Mathematical background of the algorithm

Suppose that the period length T of a binary multisequence $\mathbf{S}=(S_1, S_2, \cdots, S_m)$ is a power of p, i.e., $T=p^n, n\geqslant 1$. The connection integer $\boldsymbol{q}$ of the smallest FCSR that can generate S_1, S_2, $\cdots$, S_m simultaneously can be written as follows

$$\boldsymbol{q}=lcm(q_1,q_2,\cdots,q_m)=lcm\left[\frac{2^T-1}{\gcd(S_1(2),2^T-1)},\frac{2^T-1}{\gcd(S_2(2),2^T-1)},\cdots,\frac{2^T-1}{\gcd(S_m(2),2^T-1)}\right]=\frac{2^T-1}{\gcd(S_1(2),S_2(2),\cdots,S_m(2),2^T-1)},$$

where $2^{p^n}-1=\prod_{m=1}^{n}F_m^{(p)}$, with $F_n^{(p)}=\frac{2^{p^m}-1}{2^{p^{m-1}}-1}$.

Now we have to detect all $F_m^{(p)}, 1\leqslant m\leqslant n$, which divide $S_i(2)=\sum_{j=0}^{T-1}s_{ij}2^j, i=1,2,\cdots,m$.

Theorem 1.1 Let $\mathbf{S}^T=(S_1, S_2, \cdots, S_m)$ be a T-periodic binary multisequence, where $T=p^n$, $n\geqslant 1$, and $S_i(x)=\sum_{j=0}^{T-1}s_{ij}x^j, i=1,2,\cdots,m$ be the polynomial corresponding to the i-th single binary sequence S_i. Set

$$A_j=(A_{1j}:A_{2j}:\cdots:A_{mj})=(s_{1,(j-1)p^{n-1}},\cdots,s_{1,jp^{n-1}-1}:\cdots:s_{m,(j-1)p^{n-1}},\cdots,s_{m,jp^{n-1}-1}),$$

where $j=1,2,\cdots,p$. Then

① $F_n^{(p)}$ divide $\mathbf{S}^T(2)$ if and only if $A_{k1}=A_{k2}=\cdots=A_{kp}$, for any $k\in\{1,2,\cdots,m\}$.

② $F_m^{(p)}, 1\leqslant m<n$ divides $\mathbf{S}^T(2)$ if and only if it divides $A_{k1}(2)+A_{k2}(2)+\cdots+A_{kp}(2)$, where $A_{kj}(2)=\sum_{t=0}^{p^{n-1}-1}s_{k,(j-1)p^{n-1}+t}x^j$, $j=1,2,\cdots,p$.

Proof We can write $\mathbf{S}^T(2)$ in the following form:

$$\begin{aligned}\mathbf{S}^T(2)&=A_1(2)+2^{p^{n-1}}A_2(2)+2^{2p^{n-1}}A_3(2)+\cdots+2^{(p-1)p^{n-1}}A_p(2)=\\&(A_{11}(2)+2^{p^{n-1}}A_{12}(2)+2^{2p^{n-1}}A_{13}(2)+\cdots+2^{(p-1)p^{n-1}}A_{1p}(2),\cdots,A_{m1}(2)+2^{p^{n-1}}A_{m2}(2)+2^{2p^{n-1}}A_{m3}(2)+\cdots+2^{(p-1)p^{n-1}}A_{mp}(2)).\end{aligned}$$

① For any $k\in\{1,2,\cdots,m\}$, $A_{k1}=A_{k2}=\cdots=A_{kp}$, then

$$\mathbf{S}^T(2)=(A_{11},A_{21},\cdots,A_{m1})\cdot(1+2^{p^{n-1}}+2^{2p^{n-1}}+\cdots+2^{(p-1)p^{n-1}})=(A_{11},A_{21},\cdots,A_{m1})F_n^{(p)}.$$

On the other hand, since $F_n^{(p)}$ divides $\mathbf{S}^T(2)=(S_1^T(2),S_2^T(2),\cdots,S_m^T(2))$, we can set

$$\begin{aligned}\mathbf{S}^T(2)&=({S_1}^T(2),{S_2}^T(2),\cdots,{S_m}^T(2))=\\&(A_1^*F_n^{(p)}.A_2^*F_n^{(p)},\cdots,A_m^*F_n^{(p)})=\\&(A_1^*+A_1^*2^{p^{n-1}}+\cdots+A_1^*(2^{p^{n-1}})^{p-1},\cdots,\\&A_m^*+A_m^*2^{p^{n-1}}+\cdots+A_m^*(2^{p^{n-1}})^{p-1}).\end{aligned}$$

Note that $S_k^T(2)<2^{p^n}, 1\leqslant k\leqslant m$, we have $A_k^*<2^{p^{n-1}}, 1\leqslant k\leqslant m$. Therefore, for any $k\in\{1,2,\cdots,m\}$, $A_k^*=A_{kj}, 1\leqslant j\leqslant p$.

② Since $2^{p^n}-1=\prod_{m=1}^{n}F_m^{(n)}$, for any $k\in\{1,2,\cdots,m\}$ there exists an integer $k_m=\prod_{u=1,u\neq m}^{n-1}F_u^{(p)}$ such that $2^{p^{n-1}}=F_m^{(p)}k_m+1$. Thus, we have

$$\begin{aligned}\mathbf{S}^T(2)&=(A_{11}(2)+2^{p^{n-1}}A_{12}(2)+2^{2p^{n-1}}A_{13}+\cdots+2^{(p-1)p^{n-1}}A_{1p}(2),\cdots,A_{m1}(2)+2^{p^{n-1}}A_{m2}(2)+2^{2p^{n-1}}A_{m3}+\cdots+2^{(p-1)p^{n-1}}A_{mp}(2))\cdot\\&(A_{11}(2)+(F_m^{(p)}k_m+1)A_{12}(2)+\cdots+(F_m^{(p)}k_m+1)^{p-1}A_{1p}(2),\cdots,A_{m1}(2)+(F_m^{(p)}k_m+1)A_{m2}(2)+\cdots+(F_m^{(p)}k_m+1)^{p-1}A_{mp}(2))=\end{aligned}$$

$(A_{11}(2)+\cdots+A_{1p}(2)+F_m^{(p)}\lambda_1,\cdots,$
$A_{m1}(2)+\cdots+A_{mp}(2)+F_m^{(p)}\lambda_m)$,

where $\lambda_k, 1\leqslant k\leqslant m$ is an integer depending on m, $A_{k1},\cdots,A_{kp}$. Therefore, $F_m^{(p)}, 1\leqslant m\leqslant n$ divides $\mathbf{S}^T(2)$ if and only if it divides $A_{k1}(2)+A_{k2}(2)+\cdots+A_{kp}(2)$, for any $k\in\{1,2,\cdots,m\}$.

2 An algorithm for computing the upper bound of the 2-adic joint complexity of a binary multisequence with period p^n

Form the conclusion in Section 1, we immediately gain an algorithm, which can be used to establish an upper bound $\mathcal{Q}$ for the connection integer of the smallest FCSR that can generate a p^n-periodic multisequence $\mathbf{S}=(S_1,S_2,\cdots,S_m)$. In this algorithm we denote this 2-adic addition by $\oplus$.

Algorithm 2.1

A=S^T, T=p^n, $\mathcal{Q}$=1
  while n>0
    $A_{kj}=(a_{k,(j-1)p^{n-1}},\cdots,a_{k,jp^{n-1}-1})$; j=1,2,⋯,p; k=1,2,⋯,m
    if $A_{k1}=A_{k2}=\cdots=A_{kp}$, for any k∈{1,2,⋯,m}
      A=(A_{11},A_{21},⋯,A_{m1})
    else
      $\mathcal{Q}=\mathcal{Q}F_n^{(p)}$
      A=($A_{11}\oplus\cdots\oplus A_{1p}$,⋯,$A_{m1}\oplus\cdots\oplus A_{mp}$)
      if B=($a_{1,p^{n-1}},\cdots,a_{1,p^{n-1}+\lceil\log_2(p)\rceil-1}$: ⋯ : $a_{m,p^{n-1}},\cdots,a_{m,p^{n-1}+\lceil\log_2(p)\rceil-1}$)≠0
        A=(a_{10}, a_{11}, ⋯, $a_{1,p^{n-1}-1}$: ⋯ : s_{m0}, a_{m1}, ⋯, $a_{m,p^{n-1}-1}$)
      A=A⊕B
    n=n−1
  end while

Theorem 2.1 The algorithm is correct, furthermore, $q<\mathcal{Q}$, $\Phi(\mathbf{S})\leqslant\log_2(\mathcal{Q})$.

Proof By Theorem 1.1, if for any $k\in\{1,2,\cdots,m\}$, $A_{k1}=A_{k2}=\cdots=A_{kp}$ can be satisfied, then $F_n^{(p)}$ does not divide $\mathbf{S}^T(2)$. Otherwise, $F_n^{(p)}\mid\mathbf{S}^T(2)$ if and only if $F_n^{(p)}\mid A_{k1}+A_{k2}+\cdots+A_{kp}$, for any $k\in\{1,2,\cdots,m\}$. Since $A_{k1}(2)+A_{k2}(2)+\cdots+A_{kp}(2)\leqslant p(2^{p^{n-1}}-1)$, its 2-adic expression may have more than p^{n-1} digits, namely up to $p^{n-1}+\lceil\log_2(p)\rceil$ digits. Suppose its 2-adic expression can be written in the form $a_k+b_k2^{p^{n-1}}$, where $0\leqslant a_k\leqslant 2^{p^{n-1}}$ and $1\leqslant b\leqslant p$. Note that $2^{p^{n-1}}=F_m^{(p)}k_m+1$, we have $F_m^{(p)}\mid\mathbf{S}^T(2)$ if and only if $F_m^{(p)}\mid a_k+b_k$, for any $k\in\{1,2,\cdots,m\}$ by Theorem 1.1. Furthermore, $q<\mathcal{Q}$, $\Phi(\mathbf{S})\leqslant\log_2(\mathcal{Q})$.

Remark 2.1 If $F_m^{(p)}, 1\leqslant m\leqslant n$ is prime in the factorization $2^{p^n}-1=\prod_{m=1}^{n}F_m^{(p)}$, our upper bound is good since the equality holds.

Example 2.1 Note that $2^{32}-1$ can be written as the product $2^{32}-1=F_1^{(2)}F_2^{(2)}F_3^{(2)}F_4^{(2)}F_5^{(2)}$ of the Fermat numbers $F_m^{(2)}=2^{2^m-1}+1$. We apply the described algorithm to the 32-periodic binary multisequence with

$\mathbf{S}^{32}$ = (00110011001100111001100110011001, 10101010110010100110101101100111).

Step 1

A_1=0011001100110011, 1010101011001010

A_2=1001100110011001, 0110101101100111

$A_1\neq A_2$

A=10100110011001101, 11010100010111001

A=1010011001100110, 1101010001011100

B=**1,1**

A=0110011001100110, 0011010001011100

$\mathcal{Q}=F_5^{(2)}=2^{16}+1$

Step 2

A_1=01100110,00110100

A_2=01100110, 01011100

$A_1\neq A_2$

A=00000000, 01100110

$\mathcal{Q}=\mathcal{Q}F_5^{(2)}=F_5^{(2)}F_4^{(2)}=(2^{16}+1)(2^8+1)$

Step 3

A_1=0000, 0110

A_2=0000, 0110

$A_1=A_2$

Step 4

A_1=00,01

A_2=00,10

$A_1\neq A_2$

Step 5

A_1=0,1

$A_2=0,1$

$A_1=A_2$

$\mathcal{Q}=\mathcal{Q}F_5^{(2)}\ F_4^{(2)}=F_5^{(2)}\ F_4^{(2)}\ 5=(2^{16}+1)(2^8+1)5$

Therefore, $F_1^{(2)}\ F_3^{(2)}$ divides $\gcd_2(2_1^{32}, S_1(2), S_2(2))$, and we have $q<F_2^{(2)}\ F_4^{(2)}\ F_5^{(2)}$, $\Phi(S)\leqslant \log_2((2^{16}+1)(2^8+1)5)\approx 26.33$.

3 Conclusion

Cryptsystems are used to provide security in communications and data transmissions. Based on different schemes to generate sequences and different ways to represent them, there are a variety of stream cipher analyses. In order to have security, complexity measures for keystream sequences play a crucial role in designing good stream cipher systems. In this paper, we showed an algorithm for determining upper bound for 2-adic joint complexity of p^n-periodic binary multisequences over $Z/(2)$. The time complexity of the algorithm is $O(mpn)$. Further research is needed to design efficient algorithms for computing the exact 2-adic joint complexity of a periodic multisequence.

References

[1] Klapper A, Goresky M. 2-adic shift registrs[C]//Fast Software Encryption. Cambridge: Cambridge security workshop, 1993:174-178.

[2] Goresky M, Klapper A. Feedback registers based on ramified extensions of the 2-adic numbers [C]// Advances in Cryptology-Eurocrypt'94. Berlin: Springer,1995:215-222.

[3] Klapper A, Goresky M. Large periods nearly deBruijn FCSR sequences [C]//Advances in Cryptology-Eurocrypt'95. Berlin: Springer,1995:263-273.

[4] Klapper A, Goresky M. Cryptanalysis based on 2-adic rational approximation[C]//Advances in Cryptology-Crypt'95. Berlin: Springer,1995:262-273.

[5] Hu H, Feng D. On the 2-adic complexity and the k-error 2-adic complexity of periodic bianry sequences [C]//Proceedings of SETA'04. Berlin: Springer, 2004:185-196.

[6] Klapper A, Goresky M. Feedback shift registers, 2-adic span, and combiners with memory[J]. Journal of Cryptology, 1997,10(2):111-147.

[7] Meidl W. Extended Games-Chan algorithm for the 2-adic complexity of FCSR-sequences[J]. Theoretical Computer Science, 2003,290(3): 2 045-2 051.

[8] Hu H, Hu L, Feng D. On the expected value of the joint 2-adic complexity of periodic bianry multisequences[C]//Proceedings of SETA'06. Berlin: Springer,2006:199-208.