Acta Mathematicae Applicatae Sinica (Chinese Series)

ISSN 0254-3079
CN 11-2040/O1

应用数学学报 英文版



应用数学学报 » 2013, Vol. 36 » Issue (3): 399-413 DOI:



# 具有$2^n$线性复杂度的$2^n$周期二元序列的3错线性复杂度

周建钦[1,2]

1. 杭州电子科技大学通信工程学院, 杭州 310018;
2. 安徽工业大学计算机学院, 马鞍山 243002

# On the 3-Error Linear Complexity of $2^n$-Periodic Binary Sequences with Linear Complexity $2^n$

ZHOU Jianqin[1,2]

1. Telecommunication School, Hangzhou Dianzi University, Hangzhou 310018;
2. Computer Science School, Anhui University of Technology, Ma'anshan 243002

- 摘要
- 参考文献
- 相关文章



摘要 线性复杂度和k错线性复杂度是度量密钥流序列的密码强度的重要指标.通过研究周期为$2^n$的二元序列线性复杂度,提出将k错线性复杂度的计算转化为求Hamming重量最小的错误序列.基于Games-Chan算法,讨论了线性复杂度为$2^n$的$2^n$周期二元序列的3错线性复杂度分布情况;给出了对应$k$错线性复杂度序列的完整计数公式,$k$=3,4.对于一般的线性复杂度为$2^n-m$的$2^n$周期二元序列,也可以使用该方法给出对应k错线性复杂度序列的计数公式.

关键词: 周期序列 线性复杂度 $k$错线性复杂度 $k$错线性复杂度分布

Abstract: The linear complexity and the k-error linear complexity of a sequence have been used as important measures of keystream sequence strength. By studying linear complexity of binary sequences with period $2^n$, it is proposed that the computing of k-error linear complexity should be converted to finding error sequences with minimal Hamming weight. Based on Games-Chan algorithm, 3-error linear complexity distribution of $2^n$-periodic binary sequences with linear complexity $2^n$ is discussed. For $k$=3,4, the complete counting functions on the $k$-error linear complexity of $2^n$-periodic binary sequences with linear complexity $2^n$ are derived. Based on those results, the counting functions for the number of all $2^n$-periodic binary sequences with given 3-error linear complexity can be obtained. Generally, the complete counting functions on the $k$-error linear complexity of $2^n$-periodic binary sequences with linear complexity $2^n-m$ can be obtained using a similar approach.

Key words: periodic sequence linear complexity $k$-error linear complexity $k$-error linear complexity distribution

收稿日期: 2011-05-13;

基金资助:浙江省自然科学基金(Y1100318);安徽省自然科学基金(1208085MF106)资助项目.

引用本文:

周建钦. 具有$2^n$线性复杂度的$2^n$周期二元序列的3错线性复杂度[J]. 应用数学学报, 2013, 36(3): 399-413.

ZHOU Jianqin. On the 3-Error Linear Complexity of $2^n$-Periodic Binary Sequences with Linear Complexity $2^n$[J]. Acta Mathematicae Applicatae Sinica, 2013, 36(3): 399-413.

[1] Ding C S, Xiao G Z, Shan W J. The Stability Theory of Stream Ciphers. Lecture Notes in Computer Science, Vol.561, Berlin, Heidelberg: Springer-Verlag, 1991, 85-88

[2] Stamp M, Martin C F. An Algorithm for the k-error Linear Complexity of Binary Sequences with Period $2^n$. *IEEE Transactions on*

*Information Theory*, 1993, 39(4): 1398-1401

[3] Kurosawa K, Sato F, Sakata T, Kishimoto W. A Relationship Between Linear Complexity and k-Error Linear Complexity. *IEEE Transactions on Information Theory*, 2000, 46(2): 694-698

[4] Rueppel R A. Analysis and Design of Stream Ciphers. Berlin: Springer-Verlag, 1986, Chapter 4.

[5] Meidl W. On the Stablity of $2^n$-periodic Binary Sequences. *IEEE Transactions on Information Theory*, 2005, 51(3): 1151-1155

[6] Zhu F X, Qi W F. The 2-error Linear Complexity of $2^n$-periodic Binary Sequences with Linear Complexity $2^n$-1. *Journal of Electronics*, 2007, 24(3): 390-395 (in Chinese)

[7] Fu F, Niederreiter H, Su M. The Characterization of $2^n$-periodic Binary Sequences with Fixed 1-error Linear Complexity. In: Gong G., Helleseth T., Song H.-Y., Yang K. (eds.), SETA 2006, LNCS, Vol. 4086, 88-103, Springer-Verlag, 2006

[8] Kavuluru R. Characterization of $2^n$-periodic Binary Sequences with Fixed 2-error or 3-error Linear Complexity. *Des. Codes Cryptogr.*, 2009, 53: 75-97

[9] Etzion T, Kalouptsidis N, Kolokotronis N, Limniotis K, Paterson K G. Properties of the Error Linear Complexity Spectrum. *IEEE Transactions on Information Theory*, 2009, 55(10): 4681-4686

[10] Games R A, Chan A H. A Fast Algorithm for Determining the Complexity of a Binary Sequence with Period $2^n$. *IEEE Transactions on Information Theory*, 1983, 29(1): 144-146

[11] Han Y K, Chung J H, Yang K. On the k-error Linear Complexity of pm-periodic Binary Sequences. *IEEE Transactions on Information Theory*, 2007, 53(6): 2297-2304

[12] Lauder A, Paterson K. Computing the Error Linear Complexity Spectrum of a Binary Sequence of Period $2^n$. *IEEE Transactions on Information Theory*, 2003, 49(1): 273-280

[13] Meidl W. How Many Bits have to be Changed to Decrease the Linear Complexity? *Des. Codes Cryptogr.*, 2004, 33: 109-122

[14] Wei S M, Xiao G Z, Chen Z. A Fast Algorithm for Determining the Minimal Polynomial of a Sequence with Period $2p^n$ over GF(q). *IEEE Transactions on Information Theory*, 2002, 48(10): 2754-2758

[15] Zhou J Q. On the k-error Linear Complexity of Sequences with Period 2 $p^n$ over GF(q). *Des. Codes Cryptogr.*, 2011, 58(3): 279-296

[1] 胡磊. 达到极大线性复杂度的前馈阵列[J]. 应用数学学报, 2000, 23(3): 377-384.