吉首大学学报自然科学版 » 2012, Vol. 33 » Issue (2): 28-34 DOI: 10.3969/j.issn.1007-2985.2012.02.008



# $2^n$周期平衡二元序列的8错线性复杂度

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

# 8-Error Linear Complexity of $2^n$-Periodic Balanced Binary Sequences

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





**摘要** 线性复杂度和k错线性复杂度分别是流密码密钥流序列强度和稳定性的重要度量指标.通过研究周期为2n的二元序列线性复杂度，基于Games-Chan算法，讨论了线性复杂度小于$2n$的$2^n$-周期二元序列的8错线性复杂度的分布，给出其对应8错线性复杂度为$2^{n-2}$，$2^{n-3}$，$2^{n-4}$和$2^{n-3}-2^{n-j}$的原始二元序列计数公式.

**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 the important measurement of keystream sequence strength.By studying linear complexity of binary sequences with period 2n,based on Games-Chan algorithm,8-error linear complexity distribution of 2n-periodic binary sequences with linear complexity less than 2n is discussed.The complete counting functions on 2n-periodic balanced binary sequences with 8-error linear complexity 2n-2,2n-3,2n-4 and 2n-3-2n-j are derived respectively.

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



**基金资助:**

安徽省自然科学基金资助项目(1208085MF106)

**作者简介**: 周建钦（1963-），男，山东巨野人，安徽工业大学计算机学院教授，硕士，主要从事通信、密码学与理论计算机科学研究.

**引用本文:**

周建钦,赵起,崔洪成. $2^n$周期平衡二元序列的8错线性复杂度[J]. 吉首大学学报自然科学版, 2012, 33(2): 28-34.

ZHOU Jian-Qin,ZHAO Qi,CUI Hong-Cheng. 8-Error Linear Complexity of $2^n$-Periodic Balanced Binary Sequences[J]. Journal of Jishou University(Natural Sciences Edit, 2012, 33(2): 28-34.

[1] DING Cun-sheng,XIAO Guo-zhen,SHAN Wei-juan.The Stability Theory of Stream Ciphers [M].LNCS 561.Berlin:Springer-Verlag,1991:85-88.

[2] STAMP M,MARTIN C F.An Algorithm for Thek-Error Linear Complexity of Binary Sequences with Period 2n [J].IEEE Transactions on Information Theory,1993,39(4):1 389-1 401.

[3] 苏明.周期序列复杂度的分布 [D].天津:南开大学博士论文，2004.

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

[5] MEIDL W.On the Stability of 2n-Periodic Binary Sequences [J].IEEE Transactions on Information Theory,2005,51(3):1 151-1 155.

[6] ZHU Feng-xiang,QI Wen-feng.The 2-Error Linear Complexity of 2n-Periodic Binary Sequences with Linear Complexity 2n-1 [J].Journal of

Electronics (China),2007,24(3):390-395.

[7] 谭林,戚文峰.F2上2n周期序列的k错误序列 [J].电子与信息学报,2008,30(11):2 592-2 595.

[8] GAMES R A,CHAN A H.A Fast Algorithm for Determining the Complexity of a Binary Sequence with Period 2n[J].IEEE Transactions on Information Theory,1983,29(1):144-146.

[1] 周建钦, 刘军. **周期二元序列的部分4-错误序列计数公式**[J]. 吉首大学学报自然科学版, 2012, 33(3): 32-35.

[2] 周建钦, 上官成. **周期为2pn的q元序列m紧错线性复杂度**[J]. 吉首大学学报自然科学版, 2011, 32(6): 27-32.