二元周期倒序序列及其对偶序列的复杂性分析*

王菊香
(安徽建筑工业学院 数理系, 合肥 230601)

摘 要: 讨论了有限域 F_2 上周期倒序序列 $\hat{S}^\infty$ 与原序列 S^∞ 之间的极小多项式以及生成函数的关系;同时研究了 $\hat{S}^\infty$ 按位取反后得到的对偶序列 $\overline{\hat{S}}^\infty$ 与原序列 S^∞ 之间的极小多项式和线性复杂度的关系。这些结果对研究流密码密钥流序列的线性复杂度有一定的应用价值.

关键词: 极小多项式; 线性复杂度; 倒序序列; 对偶序列
中图分类号: TN918.4 **文献标志码**: A **文章编号**: 1001-3695(2012)12-4654-02
doi:10.3969/j.issn.1001-3695.2012.12.064

Complexity of binary periodic inverse sequence and its generalized bit-wise negative sequence

WANG Ju-xiang
(*Dept. of Mathematics & Physics, Anhui University of Architecture, Hefei* 230601, *China*)

Abstract: This paper presented the relation between the inverse sequence $\hat{S}^\infty$ and periodic sequence S^∞ about the minimal polynomial. At the same time, it discussed the same problems between the generalized bit-wise negative periodic sequence $\overline{\hat{S}}^\infty$ and periodic sequence S^∞ too. The results can be used to analyze the complexity of periodic sequences of stream ciphers.
Key words: minimal polynomial; linear complexity; inverse sequence; generalized bit-wise negative sequence

在全球信息化的时代中,序列密码体制以简捷、快速的生成算法,使其成为移动通信的主流加密算法。序列密码的安全性取决于密钥流序列的伪随机性。周期和线性复杂度是度量密钥流序列安全性的两个重要指标。有限域上周期单序列的线性复杂度分析是流密码学的基本内容[1]。很多学者研究了单序列线性复杂度以及序列的复杂度测量[2]。文献[3]讨论了周期序列 S^∞ 的极小多项式 $f_s(x)$ 与 S^∞ 的倒序序列 $\hat{S}^\infty$ 的极小多项式 $f_{\hat{S}}(x)$ 之间的关系,并对它们之间的线性复杂度进行了分析。由于周期序列及其对偶序列之间有着密切的联系,所以讨论对偶序列的相关性质有着一定的应用价值。文献[4]提出了 F_P 上周期序列 S^∞ 与其对偶序列 $\overline{S}^\infty$ 之间的线性复杂度分析。随着流密码学的发展,流密码学的理论要求对多序列的联合线性复杂度进行分析。文献[5]中介绍了多序列的联合线性复杂度的综述。文献[6]对 F_2 上周期序列及其广义对偶多序列的复杂性进行了讨论。文献[7]则对 F_P 上周期多序列及其广义对偶多序列的联合线性复杂度进行了综合分析。文献[1,8]提出了广义欧几里德算法和迭代算法,近年来许多学者也应用 Gröbner 基理论来解决这个问题[9,10]。鉴于周期序列及其倒序序列之间的特殊关系,本文将探讨 F_2 上周期倒序序列 $\hat{S}^\infty$ 及其对偶序列 $\overline{\hat{S}}^\infty$ 与原周期序列 S^∞ 的线性复杂度之间的关系。

1 基本知识

设 S^T 表示有限域 F_2 上有限序列 $S=(S_0,S_1,S_2,\cdots,S_{T-1})$,$S$ 表示有限域 F_2 上无限序列 $S=(S_0,S_1,S_2,\cdots)$。设有整数 L 和 F_2 上一组数 $C_1,C_2,\cdots,C_L$,使 S^T(或 S)满足

$$S_j+C_1S_{j-1}+C_2S_{j-2}+\cdots+C_LS_{j-L}=0 \quad j\geqslant L$$

则称 S^T(或 S)是一个 L 阶齐次线性递归序列;L 是 S^T(或 S)所满足的齐次线性递归关系的最小阶数,称为 S^T(或 S)的线性复杂度,记为 $LC(S^T)$(或 $LC(S)$)。对于序列 S 和 S^T,它们的生成函数定义为

$$S(x)=S_0+S_1x+S_2x^2+\cdots+S_{T-1}x^{T-1}+\cdots=\sum_{i=0}^{\infty}S_ix^i$$

$$S^T(x)=S_0+S_1x+S_2x^2+\cdots+S_{T-1}x^{T-1}$$

若 S 是周期为 T 的序列,S^T 是它的第一个周期:

$$S(x)=S^T(x)(1+x^T+x^{2T}+\cdots)=\frac{S^T(x)}{1-x^T}=$$

$$[S^T(x)/\gcd(S^T(x),1-x^T)]/[(1-x^T)/\gcd(S^T(x),$$

$$1-x^T)]=\frac{r_s(x)}{f_s(x)}$$

其中:$f_s(x)=(1-x^T)/\gcd(S^T(x),1-x^T)$,$r_s(x)=S^T(x)/\gcd(S^T(x),1-x^T)$。

显然 $r_s(x)/f_s(x)$ 是既约的,$\deg(r_s(x))<\deg(f_s(x))$,$f_s(x)$ 为 S 的极小多项式,$\deg(f_s(x))=LC(S)$ 为 S 的线性复杂度[11]。

2 主要结果

定义 1 设 $S=(S_0,S_1,S_2,\cdots)$ 是 F_2 上周期序列,称 $\overline{S}=(\overline{S_0},\overline{S_1},\overline{S_2},\cdots)$ 为 S 的对偶序列,其中 $\overline{S_i}=1+S_i(i=0,1,2,\cdots)$。

收稿日期: 2012-05-14; **修回日期**: 2012-06-21 **基金项目**: 安徽建筑工业学院青年科学研究专项经费资助项目(2011183-16)
作者简介: 王菊香(1976-),女,安徽东至人,助教,主要研究方向为序列密码和纠错码(jnqz05@163.com).

定义 2　设 $S=(S_0,S_1,\cdots,S_{T-1})^\infty$ 表示 F_2 上周期为 T 的无限序列,称 $\hat{S}=(S_{T-1},S_{T-2},\cdots,S_1,S_0)^\infty$ 为 S 的倒序序列,且记

$$S^T(x)=S_0+S_1x+\cdots+S_{T-1}x^{T-1}=\sum_{i=0}^{T-1}S_ix^i$$

$$\hat{S}^T(x)=S_{T-1}+S_{T-2}x+\cdots+S_1x^{T-2}+S_0x^{T-1}=\sum_{i=0}^{T-1}S_{T-1-i}x^i$$

引理 1[3]　设周期为 T 的序列 $S=(S_0,S_1,\cdots,S_{T-1})^\infty$,$S$ 的生成函数 $S^T(x)=S_0+S_1x+\cdots+S_{T-1}x^{T-1}$,则 S 的极小多项式 $f_S(x)=(1-x^T)/\gcd(1-x^T,S^T(x))$;$S$ 的倒序序列 $\hat{S}=(S_{T-1},S_{T-2},\cdots,S_1,S_0)^\infty$,则 $\hat{S}$ 的极小多项式 $f_{\hat{S}}(x)=(1-x^T)/\gcd(1-x^T,\hat{S}^T(x))$,$\hat{S}$ 的生成函数

$$\hat{S}^T(x)=S_{T-1}+S_{T-2}x+\cdots+S_1x^{T-2}+S_0x^{T-1}=x^{T-1}S^T\left(\frac{1}{x}\right)$$

令 $g(x)=\gcd(1-x^T,S^T(x))$,$\hat{g}(x)=\gcd(1-x^T,\hat{S}^T(x))$,则 $\hat{g}(x)=x^{\deg(g(x))}g\left(\frac{1}{x}\right)$,故 $\deg(f(x))=\deg(\hat{f}(x))$,且 $LC(S)=LC(\hat{S})$。

引理 2[12]　设有限域 F_2 上周期序列 S 的生成函数 $S(x)=\sum_{i=0}^{\infty}S_ix^i=r_s(x)/f_s(x)$。其中:$\gcd(r_s(x),f_s(x))=1$,且 $f_s(x)$ 为 S 的极小多项式,记 $f_S(x)=\sum_{j=0}^{m}C_jx^j(C_0=C_m=1)$,以 l 记 $x=1$ 为 $f_S(x)$ 根的次数($l\geqslant 0$),即 $f_S(x)=(1+x)^lf_1(x)$,其中 $f_1(1)\neq 0$,则 S 的对偶序列 $\bar{S}$ 的生成函数为

$$\bar{S}(x)=[f_S(x)+r_S(x)(1+x)]/(1+x)f_S(x)=\begin{cases}[f_S(x)+r_S(x)(1+x)]/(1+x)f_S(x) & l=0\\ [r_S(x)+f_1(x)]/(1+x)f_1(x) & l=1\\ [r_S(x)+f_1(x)]/f_S(x) & l\geqslant 2\end{cases}$$

$\bar{S}$ 的极小多项式为

$$f_{\bar{S}}(x)=\begin{cases}(1+x)f_S(x) & l=0\\ f_1(x) & l=1\\ f_S(x) & l\geqslant 2\end{cases}$$

推论 1　设 F_2 上周期序列 $\hat{S}=(S_{T-1},S_{T-2},\cdots,S_1,S_0)^\infty$ 的生成函数 $\hat{S}=\frac{r_{\hat{S}}(x)}{f_{\hat{S}}(x)}$。其中:$\gcd(r_{\hat{S}}(x),f_{\hat{S}}(x))=1$,且 $f_{\hat{S}}(x)$ 是 $\hat{S}$ 的极小多项式,记 $f_{\hat{S}}(x)=\sum_{j=0}^{q}s_jx^j(s_0=s_q=1)$,以 n 记 $x=1$ 为 $f_{\hat{S}}(x)$ 根的次数($n\geqslant 0$),即 $f_{\hat{S}}(x)=(1+x)^nf_2(x)$,其中 $f_2(1)\neq 0$,则 $\hat{S}$ 的对偶序列 $\bar{\hat{S}}$ 的生成函数

$$\bar{\hat{S}}(x)=[f_{\hat{S}}(x)+r_{\hat{S}}(x)(1+x)]/(1+x)f_{\hat{S}}(x)=\begin{cases}[f_{\hat{S}}(x)+r_{\hat{S}}(x)(1+x)]/(1+x)f_{\hat{S}}(x) & n=0\\ [r_{\hat{S}}(x)+f_2(x)]/(1+x)f_2(x) & n=1\\ [r_{\hat{S}}(x)+f_2(x)]/f_{\hat{S}}(x) & n\geqslant 2\end{cases}$$

$\bar{\hat{S}}$ 的极小多项式为

$$f_{\bar{\hat{S}}}(x)=\begin{cases}(1+x)f_{\hat{S}}(x) & n=0\\ f_2(x) & n=1\\ f_{\hat{S}}(x) & n\geqslant 2\end{cases}$$

证明由引理 2 直接得证。

定理 1　设 F_2 上周期为 T 的序列 $S=(S_0,S_1,\cdots,S_{T-1})^\infty$ 的极小多项式为 $f_S(x)$,$\hat{S}=(S_{T-1},S_{T-2},\cdots,S_1,S_0)^\infty$ 的极小多项式为 $f_{\hat{S}}(x)$,即

$$f_S(x)=(1-x^T)/\gcd(1-x^T,S^T(x))=(1-x^T)/g(x)$$

$$f_{\hat{S}}(x)=(1-x^T)/\gcd(1-x^T,\hat{S}^T(x))=(1-x^T)/\hat{g}(x)$$

则 $f_{\hat{S}}(x)=-xf_S\left(\frac{1}{x}\right)$。

证明　由 $f_s(x)=(1-x^T)/\gcd(1-x^T,S^T(x))=(1-x^T)/g(x)$ 得 $f_s\left(\frac{1}{x}\right)=(x^T-1)/x^T\,g\left(\frac{1}{x}\right)$,则 $g\left(\frac{1}{x}\right)=(x^T-1)/x^Tf_s\left(\frac{1}{x}\right)$,又 $f_{\hat{S}}(x)=(1-x^T)/\hat{g}(x)$,$\hat{g}(x)=x^{T-1}g(\frac{1}{x})$,可得

$$f_{\hat{S}}(x)=(1-x^T)/x^{T-1}g(\frac{1}{x})=$$

$$(1-x^T)x^Tf_S(\frac{1}{x})/x^{T-1}(x^T-1)=-xf_S\left(\frac{1}{x}\right)$$

定理 2　设 F_2 上周期序列 $\hat{S}=(S_{T-1},S_{T-2},\cdots,S_1,S_0)^\infty$ 的生成函数 $\hat{S}=\frac{r_{\hat{S}}(x)}{f_{\hat{S}}(x)}$。其中:$\gcd(r_{\hat{S}}(x),f_{\hat{S}}(x))=1$,且 $f_{\hat{S}}(x)$ 是 $\hat{S}$ 的极小多项式,记 $f_{\hat{S}}(x)=\sum_{j=0}^{m}C_jx^j(C_0=C_m=1)$,以 n 记 $x=1$ 为 $f_{\hat{S}}(x)$ 根的次数($n\geqslant 0$),即 $f_{\hat{S}}(x)=(1+x)^nf_2(x)$,其中 $f_2(1)\neq 0$,则

$$f_{\bar{\hat{S}}}(x)=\begin{cases}-x(1+x)f_S\left(\frac{1}{x}\right) & n=0\\ f_2(x) & n=1\\ -xf_S\left(\frac{1}{x}\right) & n\geqslant 2\end{cases}$$

证明　由定理 1 得 $f_{\hat{S}}(x)=-xf_S\left(\frac{1}{x}\right)$,则由引理 2 知,当 $n=0$ 时,$f_{\bar{\hat{S}}}(x)=(1+x)f_{\hat{S}}(x)=-x(1+x)f_S\left(\frac{1}{x}\right)$;当 $n=1$ 时,$f_{\bar{\hat{S}}}(x)=f_2(x)$;当 $n\geqslant 0$ 时,$f_{\bar{\hat{S}}}(x)=f_{\hat{S}}(x)=-xf_S\left(\frac{1}{x}\right)$。

推论 2　在上述记号下,$LC(\bar{\hat{S}})=\begin{cases}LC(S)+1 & n=0\\ LC(S)-1 & n=1\\ LC(S) & n\geqslant 2\end{cases}$。

证明　当 $n=0$ 时,$\deg(f_{\bar{\hat{S}}}(x))=\deg\left[-x(1+x)f_S\left(\frac{1}{x}\right)\right]=\deg(f_S(x))+1$,则 $LC(\bar{\hat{S}})=LC(S)+1$;当 $n=1$ 时,$\deg(f_{\bar{\hat{S}}}(x))=\deg[f_2(x)]$,则 $LC(\bar{\hat{S}})=LC(S)-1$;当 $n\geqslant 2$ 时,$\deg(f_{\bar{\hat{S}}}(x))=\deg\left[-xf_S\left(\frac{1}{x}\right)\right]$,则 $LC(\bar{\hat{S}})=LC(S)$。

3　结束语

本文提出了 F_2 上周期序列 S 及其倒序序列 $\hat{S}$ 的极小多项式及生成函数之间的关系;并研究了 $\hat{S}$ 的对偶序列 $\bar{\hat{S}}$ 与 S 的极小多项式之间的关系;进一步分析了它们之间的线性复杂度关系,给出了明确的关系式。这些结果对研究流密码密钥流序列的线性复杂度有一定的应用价值。在本文讨论的基础上,可以进一步讨论有限域 F_P 上相关理论,从而推进周期序列的线性复杂度的研究。

参考文献:

[1] DING Cun-sheng, XIAO Guo-zhen, SHAN Wei-juan. The stability theory of stream ciphers[C]//Lecture Notes in Computer Science. New York: Springer-Verlag, 1991: 85-100.

[2] HASSE H. Theorie der höheren differentiale in einem algebraischen funktionenk rper mit vollkommenem konstantenkörper bei beliebiger charakteristik[J]. Reine Angew Math, 1936, 175: 50-54.

(下转第 4658 页)

节点 b 的推荐信任向量定义为

$$RT_{ab} = \bigoplus_{c \in P}(\mu_c^a \otimes DT_{cb})$$

与式(1)类似,可得到节点 b 的推荐信任值计算公式为

$$rt_{ab} = RT_{ab}[1] \overset{+}{\varepsilon} (\lambda_2 \overset{\cdot}{\varepsilon} RT_{ab}[2]) \quad (3)$$

1.2.3 综合信任值

根据式(2)(3),得出综合信任值 t_{ab} 为

$$t_{ab} = \alpha \cdot dt_{ab} + \beta \cdot rt_{ab} \quad (4)$$

其中:α、β 分别表示直接信任值和推荐信任值对应的权值,且满足 $\alpha + \beta = 1$。计算得到最终的综合信任值后,节点 a 选取信任值最高节点进行交易。

2 仿真与分析

本文的仿真实验在 Windows 7 环境下用 MATLAB 7.0 实现。设定仿真网络规模为 1 000 个节点,每个节点与其他节点交易 10 ~ 50 次。在恶意节点占不同规模比例的情况下,做了本文信任模型和传统信任模型 EigenRep 的对比实验。

如图 1 所示,通过与同一实验环境下的 EigenTrust 模型进行比较,可知随着恶意节点的增多,节点间信任值倾向稳定。由于本文模型考虑了推荐信息的模糊程度,相比 EigenRep 在最终信任值计算时综合了更多信息,因此其随着恶意节点增加仍能保持较高的成功率。

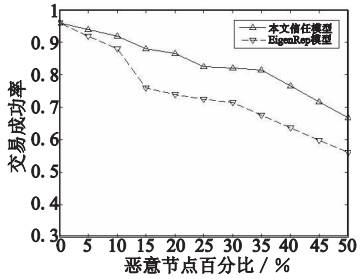

图1 交易成功率与恶意节点比率的关系

3 结束语

在开放网络中,信任具有的主观性及不确定性,使得精确的数学模型难以描述。本文结合模糊数学及 Shapley 熵的相关理论,提出一个基于 Shapley 熵的主观模型。其中直接信任值的计算都是根据节点的交易历史得到的;推荐信任值通过综合节点间评价取向相似度、节点反馈评价的不确定度、推荐节点的可信程度三个方面来计算,不仅考虑了推荐节点的参考信息,同时运用 Shapley 熵准确度量了推荐信息的确定程度。最后综合直接和推荐信任值得到节点间综合信任值。交易节点的选择根据综合信任值的大小进行,综合信任值越高的节点,交易成功的可能性越大,因此节点会倾向于和信任值高的节点进行交易,从而使本模型能利用信任值来规范节点的网络行为。实验仿真表明,该模型能有效地计算节点间信任,并且对恶意行为能起到有效的抑制作用。

参考文献:

[1] 苗光胜,冯登国. P2P 信任模型中基于行为相似度的共谋团体识别模型[J]. 通信学报,2009,30(8):9-20.

[2] 林庆国,刘宴兵. 一种基于信任的动态访问控制策略[J]. 重庆邮电大学学报,2010,22(4):478-482.

[3] 李季,朱小勇. 基于模糊理论的 Web 服务信任评估模型[J]. 计算机工程,2010,36(15):25-30.

[4] 吕镇邦,周波. 基于 Shapley 熵和 Choquet 积分的层次化风险评估[J]. 北京邮电大学学报,2009,32(6):83-87.

[5] 李致远,王汝传. P2P 电子商务环境下的动态安全信任管理模型[J]. 通信学报,2011,32(3):50-59.

[6] 杨墨,王丽娜. 基于信任容错的 Web 服务可靠性增强方法研究[J]. 通信学报,2010,31(9):131-138.

[7] 陈深龙,张玉清. 增强 Ad hoc 网络可生存性的健壮多维信任模型[J]. 通信学报,2010,31(5):1-9.

[8] 窦文阳,王小明,张立臣. 普适环境下的动态模糊访问控制模型研究[J]. 计算机科学,2010,37(9):63-68.

[9] 朗波. 面向分布式系统访问控制的信任度量化模型[J]. 通信学报,2010,31(12):45-54.

[10] BLAZE M, FEIGENBAUM J, LACY J. Decentralized trust management[C]//Proc of the 17th Symposium on Security and Privacy. 1996.

[11] BETH T, BORCHERDING M, KLEIN B. Valuation of trust in open networks[C]//Proc of European Symposium on Research in Computer Security. 1994:3-18.

[12] J∅SANG A. Prospectives for modeling trust in information security [C]//Proc of Australian Conference on Information Security and Privacy. [S. l.]: Springer-Verlag,1997.

[13] WANG Yao, VASSILEVA J. Bayesian network-based trust model [C]//Proc of IEEE/WIC International Conference on Web Intelligence. Washington DC: IEEE Computer Society,2003.

[14] 唐文,陈钟. 基于模糊集合理论的主观信任管理模型研究[J]. 计算机研究与发展, 2005,42(10):1654-1659.

[15] 窦文,王怀民,贾焰. 构造基于推荐的 Peer-to-Peer 环境下的 Trust 模型[J]. 软件学报,2004,15(4):571-583.

(上接第 4655 页)

[3] HU Hong-gang, FENG Deng-guo. On the 2-Adic complexity and the k-Error 2-Adic complexity of periodic binary sequences[J]. IEEE Trans on Information Theory,2008,54(2):874-883.

[4] 王菊香,朱士信. F_p 上周期序列 S^∞ 与 $\overline{S}^\infty$ 的线性复杂度分析[J]. 计算机应用研究,2009,26(2):742-743.

[5] NIEDERREITER H. Linear complexity and related complexity measures for sequences[C]//Lecture Notes in Computer Science, Vol 2904. Berlin:Springer-Verlag,2003:1-17.

[6] 王菊香,朱士信. F_2 上周期多序列及其广义对偶多序列的复杂性分析[J]. 计算机应用研究,2010,27(10):3880-3882.

[7] 王菊香,朱士信. P 元周期多序列及其广义对偶多序列的复杂性分析[J]. 计算机应用研究,2011,28(10):3831-3833.

[8] ARMAND M A. Multisequence shift register synthesis over commutative rings with identity with applications to decoding cyclic codes over integer rings[J]. IEEE Trans on Information Theory, 2004, 50 (1):220-228.

[9] CHEN Po. Multisequence linear shift register synthesis and its application to BCH decoding[J]. IEEE Trans on Communication, 1976,24(4):438-440.

[10] FENG G L, TSENG K K. A generalized Euclidean algorithm for multisequence shift-register synthesis[J]. IEEE Trans on Information Theory,1989,35(3):584-594.

[11] 魏仕民,陈恺,肖国镇. 周期序列的极小多项式[J]. 西安电子科技大学学报,2000,27(6):749-751.

[12] 王尚平,高虎明,王育民. GF (2) 上伪随机序列 S^∞ 与 $\overline{S}^\infty$ 复杂性分析[J]. 西安电子科技大学学报:自然科学版,2002,29(1):67-70.