doi:10.16104/j.issn.1673-1891.2019.03.007

F_p上一类周期倒序序列稳定性分析

梁 静,李红菊
(安徽新华学院通识教育部,合肥 230088)

摘要:流密码稳定性的重要度量指标是序列的线性复杂度。通过生成多项式和极小多项式研究了F_p上一类周期为$2N$的倒序新序列的稳定性,给出了其极小多项式及线性复杂度,并讨论了F_p上由这类倒序新序列构成的多维周期序列的联合极小多项式及联合线性复杂度,这些结论对周期序列的研究有一定的应用价值。

关键词:周期序列;极小多项式;线性复杂度;联合线性复杂度
中图分类号:O29:TN918.4 **文献标志码**:A **文章编号**:1673-1891(2019)03-0032-03

Analysis of the Stability of Periodic Reverse Sequence Over

LIANG Jing, LI Hongju
(Department of General Education, Anhui Xinhua University, Hefei 230088, China)

Abstract: The linear complexity of the sequence is an important measure of stream cipher stability. In this paper, the stability of the new reverse sequence with a period of over is studied by generating polynomials and minimum polynomials, and its minimal polynomial and linear complexity are given. The joint minimal polynomials and joint linear complexity of the multidimensional periodic sequences composed of these new sequences over are discussed. These conclusions are somewhat applicably valuable to the study of periodic sequences.

Keywords: periodic sequence; minimal polynomial; linear complexity; joint linear complexity

0 引言

习总书记指出:网络安全和信息化对一个国家很多领域都是牵一发而动全身的,增强网络安全的防御能力和威慑能力迫在眉睫。信息是否安全取决于加密技术是否可靠,对密码技术的研究始于古罗马时期,1949年《保密系统的通信理论》[1]的发表,将数学与密码学联系在一起,从此密码学就成为一门独立学科。密码就要保障信息的安全,而衡量密钥流序列安全性的度量指标一般有:游程分布、自相关值、周期等。评价密钥流序列稳定性的又一重要指标产生于六十年代末的B-M综合算法[3],重量复杂度、k-错线性复杂度等度量指标随之而产生[4,5]。在序列稳定性研究的过程中,学者们研究了涉及序列稳定性的快速算法[6-8]。除了研究周期单序列的稳定性,还研究了多维周期序列的稳定性[9]。文献[10]研究了二元周期倒序序列的稳定性,给出了极小多项式及其线性复杂度,文献[11]研究了由序列及其对偶序列构造的一类新序列的稳定性,文献[12-13]构造了多维序列,由已有结论研究了多维周期序列的稳定性。

对于周期序列S及其对偶序列$\bar{S}$构造成周期新序列,其倒序序列的稳定性如何?并由这类周期倒序新序列构成的多维序列的联合极小多项式及联合线性复杂度是何形式,本文下面将展开研究。

1 预备知识

设F_p上的一条无穷序列为$s^\infty=(s_0,s_1,s_2,\cdots)$,$s^N=(s_0,s_1,s_2,\cdots,s_{N-1})$是$F_p$上周期为$N$的有限序列。定义$s^\infty$和$s^N$的生成多项式如下:

$$s^\infty(x)=s_0+s_1x+\cdots+s_nx^n+\cdots=\sum_{i=0}^{\infty}s_ix^i,\ s^N(x)=s_0+s_1x+\cdots+s_{N-1}x^{N-1}$$

若无穷序列是周期为N的周期序列,则s^N即为第一周期,有

$$s^\infty(x)=s^N(x)(1+x^N+x^{2N}+\cdots)=\frac{s^N(x)}{1-x^N}$$

收稿日期:2019-04-26
基金项目:安徽省高校自然科学研究项目(KJ2017A623);安徽省高校自然科学研究项目(KJ2018A0584);安徽新华学院自然科学重点项目(2018zr001)
作者简介:梁静(1986—),女,安徽蒙城人,讲师,硕士,研究方向:代数编码与密码。

$$=\frac{s^N(x)/\gcd\left(s^N(x),1-x^N\right)}{\left(1-x^N\right)/\gcd\left(s^N(x),1-x^N\right)}=\frac{r_s(x)}{f_s(x)}$$

上式中$f_s(x)=(1-x^N)/\gcd(s^N(x),1-x^N)$，$r_s(x)=x^N(x)/\gcd(s^N(x),1-x^N)$，可见$\gcd(f_s(x),r_s(x))=1$，$\deg(r_s(x))<\deg(f_s(x))$，称$f_s(x)$为序列$s^\infty$的极小多项式。则$s^\infty$的线性复杂度为$LC(s)=\deg(f_s(x))=N-\deg(\gcd(1-x^N,s^N(x)))$，式中$\deg(f_s(x))$表示$f_s(x)$的次数。

定义1[10] 设$s^N=(s_0,s_1,s_2,\cdots,s_{N-1})$为$F_p$上周期为$N$的序列，其倒序$N$-周期序列记为$\hat{s}^N=(s_{N-1},s_{N-2},\cdots,s_1,s_0)$，对偶$N$-周期序列记为$\bar{s}^N=(\bar{s}_0,\bar{s}_1,\bar{s}_2,\cdots,\bar{s}_{N-1})$，对偶倒序序列记为$\hat{\bar{s}}^N=(\bar{s}_{N-1},\bar{s}_{N-2},\cdots,\bar{s}_1,\bar{s}_0)$　其中$\bar{s}_i=p-1-s_i,i=0,1,\cdots,N-1$。且记

$$s^N(x)=s_0+s_1x+s_2x^2+\cdots+s_{N-1}x^{N-1},\ \hat{s}^N(x)=s_{N-1}+s_{N-2}x+\cdots+s_1x^{N-2}+s_0x^{N-1}$$

$$\bar{s}^N(x)=\bar{s}_0+\bar{s}_1x+\bar{s}_2x^2+\cdots+\bar{s}_{N-1}x^{N-1},\ \hat{\bar{s}}^N(x)=\bar{s}_{N-1}+\bar{s}_{N-2}x+\cdots+\bar{s}_1x^{N-2}+\bar{s}_0x^{N-1}$$

则无穷序列$\hat{s}^\infty$与$\hat{\bar{s}}^\infty$的生成多项式分别为：

$$\hat{s}^\infty(x)=\frac{\hat{s}^N(x)}{1-x^N},\quad \hat{\bar{s}}^\infty(x)=\frac{\hat{\bar{s}}^N(x)}{1-x^N}。$$

定义2[11] 将s^N和$\bar{s}^N$组合为一类新的序列$A^\infty=(s_0,s_1,\cdots s_{N-1},\bar{s}_0,\bar{s}_1,\cdots\bar{s}_{N-1})^\infty$，则该序列是周期为$2N$的新序列。

引理1[13] 设F_p上N-周期倒序序列为$\hat{s}^\infty=(s_{N-1},s_{N-2},\cdots,s_1,s_2)^\infty$，其生成函数为$\hat{s}^\infty(x)=s_{N-1}+s_{N-2}x+\cdots+s_1x^{N-2}+s_0x^{N-1}+\cdots=\frac{r_{\hat{s}}(x)}{f_{\hat{s}}(x)}$，且$\gcd(r_{\hat{s}}(x),f_{\hat{s}}(x))=1$，则$f_{\hat{s}}(x)$为$\hat{s}^\infty$的极小生成多项式。若记$f_{\hat{s}}(x)=\sum_{i=0}^{m}a_ix^i,a_0=a_m=1$令$l$为$f_{\hat{s}}(x)$在$x=1$时根的次数($l\geqslant0$)，有$f_{\hat{s}}(x)=(1-x)^lf_1(x)$，其中$f_1(1)\neq0$，则$\hat{s}^\infty$的对偶周期序列$\hat{\bar{s}}^\infty$的生成函数为：

$$\hat{\bar{s}}^\infty(x)=\frac{(p-1)f_{\hat{s}}(x)-r_{\hat{s}}(x)(1-x)}{(1-x)f_{\hat{s}}(x)}$$

$$=\begin{cases}\dfrac{(p-1)f_1(x)-r_{\hat{s}}(x)(1-x)}{(1-x)f_1(x)},l=0\\ \dfrac{(p-1)(1-x)f_1(x)-r_{\hat{s}}(x)(1-x)}{(1-x)^2f_1(x)},\quad l=1\\ \dfrac{(p-1)(1-x)^lf_1(x)-r_{\hat{s}}(x)(1-x)}{(1-x)^{l+1}f_1(x)},l\geqslant2\end{cases}$$

2 主要内容

定义3 若F_p上周期为$2N$的新序列为$A^\infty=(s_0,s_1,\cdots,s_{N-1},\bar{s}_0,\bar{s}_1,\cdots,\bar{s}_{N-1})^\infty$，则称$\hat{A}^\infty=(\bar{s}_{N-1},\bar{s}_{N-2},\cdots,\bar{s}_1,\bar{s}_0,s_{N-1},s_{N-2},\cdots,s_1,s_0)^\infty$是$F_p$上$2N$-周期的倒序新序列。

定理1 F_p上$2N$-周期倒序新序列$\hat{A}^\infty=(\bar{s}_{N-1},\cdots,\bar{s}_1,\bar{s}_0,s_{N-1},\cdots,s_1,s_0)^\infty$的极小生成多项式为$f_{\hat{A}}(x)=(1-x)(1+x^N)$。

证明：设$\hat{A}^{2N}=(\bar{s}_{N-1},\bar{s}_{N-2}\cdots,\bar{s}_1,\bar{s}_0,s_{N-1},s_{N-2}\cdots,s_1,s_0)$为$F_p$上倒序新序列第一个$2N$周期。则有

$$\hat{A}^{2N}(x)=\bar{s}_{N-1}+\bar{s}_{N-2}x+\cdots+\bar{s}_1x^{N-2}+\bar{s}_0x^{N-1}+s_{N-1}x^N+\cdots+s_1x^{2N-2}+s_0x^{2N-1}=$$

$$\hat{\bar{s}}^N(x)+x^N\hat{s}^N(x)$$

$$\hat{A}^\infty(x)=\hat{A}^{2N}(x)\left(1+x^{2N}+x^{4N}+x^{6N}+\cdots\right)=\frac{\hat{A}^{2N}(x)}{1-x^{2N}}=\frac{\hat{\bar{s}}^N(x)+x^N\hat{s}^N(x)}{1-x^{2N}}=$$

$$\frac{1}{1+x^N}\left[\frac{\hat{\bar{s}}^N(x)}{1-x^N}+\frac{x^N\hat{s}^N(x)}{1-x^N}\right]=\frac{1}{1+x^N}\left(\hat{\bar{s}}^\infty(x)+x^N\hat{s}^\infty(x)\right)$$

由引理1，1）$l=0$，$f_{\hat{s}}(x)=f_1(x),f_1(1)\neq0$

$$\hat{A}^\infty(x)=\frac{\hat{\bar{s}}^\infty(x)+\hat{s}^\infty(x)}{1+x^N}=\frac{1}{1+x^N}\left[\frac{(p-1)f_1(x)-r_{\hat{s}}(x)(1-x)}{(1-x)f_1(x)}+\frac{r_{\hat{s}}(x)}{f_{\hat{s}}(x)}\right]=$$

$$\frac{1}{1+x^N}\left[\frac{(p-1)f_1(x)-r_{\hat{s}}(x)(1-x)+(1-x)r_{\hat{s}}(x)}{(1-x)f_1(x)}\right]=\frac{p-1}{(1+x^N)(1-x)}$$

可见，$\gcd(p-1,(1-x)(1+x^N))=1$，有$f_{\hat{A}}(x)=(1-x)(1+x^N)$。

2）$l=1$时，$f_{\hat{s}}(x)=(1-x)f_1(x),f_1(1)\neq0$

$$\hat{A}^\infty(x)=\frac{\hat{\bar{s}}^\infty(x)+\hat{s}^\infty(x)}{1+x^N}=\frac{1}{1+x^N}\left[\frac{(p-1)(1-x)f_1(x)-r_{\hat{s}}(x)(1-x)}{(1-x)^2f_1(x)}+\frac{r_{\hat{s}}(x)}{f_{\hat{s}}(x)}\right]=$$

$$\frac{1}{1+x^N}\left[\frac{(p-1)(1-x)f_1(x)-r_{\hat{s}}(x)(1-x)+(1-x)r_{\hat{s}}(x)}{(1-x)^2f_1(x)}\right]=\frac{p-1}{(1-x)(1+x^N)}$$

有$f_{\hat{A}}(x)=(1-x)(1+x^N)$。

3）$l\geqslant2$时，$f_{\hat{s}}(x)=(1-x)^lf_1(x),f_1(1)\neq0$

$$\hat{A}^\infty(x)=\frac{\hat{\bar{s}}^\infty(x)+\hat{s}^\infty(x)}{1+x^N}=\frac{1}{1+x^N}\left[\frac{(p-1)(1-x)^lf_1(x)-r_{\hat{s}}(x)(1-x)}{(1-x)^{l+1}f_1(x)}+\frac{r_{\hat{s}}(x)}{f_{\hat{s}}(x)}\right]=$$

$$\frac{1}{1+x^N}\left[\frac{(p-1)(1-x)^lf_1(x)-r_{\hat{s}}(x)(1-x)+(1-x)r_{\hat{s}}(x)}{(1-x)^{l+1}f_1(x)}\right]=\frac{p-1}{(1-x)(1+x^N)}$$

亦有$f_{\hat{A}}(x)=(1-x)(1+x^N)$。

综上，F_p上$2N$-周期的倒序新序列$\hat{A}^\infty=(\bar{s}_{N-1},\cdots,\bar{s}_1,\bar{s}_0,s_{N-1},\cdots,s_1,s_0)^\infty$的极小多项式为$f_{\hat{A}}(x)=(1-x)(1+x^N)$。

推论1 F_p上$2N$-周期倒序新序列$\hat{A}^\infty=(\bar{s}_{N-1},\cdots,\bar{s}_1,\bar{s}_0,s_{N-1},\cdots,s_1,s_0)^\infty$的线性复杂度为$LC\left(\hat{A}^\infty\right)=N+1$。

证明：由定理1直接可得。

例1 设$s^3=(2,0,1)$是F_3上周期为$N=3$的序列，可知其对偶序列为$\bar{s}^3=(2,0,1)$，由s^3和$\bar{s}$组合的周期为$2N=6$的倒序新序列为$\hat{A}^6=(1,2,0,1,0,2)$，求$LC(\hat{A}^\infty)$。

解：$\hat{A}^\infty(x)=\frac{1+2x+x^3+2x^5}{1-x^6}=\frac{1-x+x^3-x^5}{(1-x^3)(1+x^3)}=\frac{(1-x)+x^3(1-x)(1+x)}{(1-x)^3(1+x)^3}=$

$$\frac{1+x^3+x^4}{(1-x)^2(1+x)^3}=\frac{1-2x^3+x^4}{(1-x)^2(1+x)^3}=$$

$$\frac{(1-x)^3-x^3(1-x)}{(1-x)^2(1+x)^3}=\frac{(1-x)^2-x^3}{(1-x)(1+x)^3}。$$

设$r_{\hat{A}}(x)=(1-x)^2-x^3$，则$r_{\hat{A}}(1)=(1-1)^2-1^3=-1=2\neq0$，故$(1-x)\nmid(1-x)^2-x^3$，又因$r_{\hat{A}}(-1)=(1-(-1))^2-(-1)^3=5=2\neq0$，则有$(1-x)\nmid(1-x)^2-x^3$。

综上$\gcd((1-x)^2-x^3,(1-x)(1+x)^3)=1$，$\hat{A}^\infty$的极小多项式为$f_{\hat{A}}(x)=(1-x)(1+x)^3$，$\hat{A}^\infty$的线性复杂度$LC\left(\hat{A}^\infty\right)=\deg\left(f_{\hat{A}}(x)\right)=3+1=4$

例2 设F_5上周期为N=5的序列为s^5=(1,0,2,0,3),则其对偶序列s^5=(3,4,2,4,1),由s^5和$\bar{s}^5$组成的周期为10的倒序新序列为$\hat{A}^{10}$=(1,4,2,4,3,3,0,2,0,1),求$LC(\hat{A}^{\infty})$。

解:$\hat{A}^{\infty}(x)=\frac{1+4x+2x^2+4x^3+3x^4+3x^5+2x^7+x^9}{1-x^{10}}=$

$\frac{(1-x)+(2x^2-2x^4)-(x^3-x^9)-(2x^5-2x^7)}{(1-x)^5(1+x)^5}=$

$\frac{1+2x^2(1+x)-x^3(1+x+x^2)(1+x^3)-2x^5(1+x)}{(1-x)^4(1+x)^5}=$

$\frac{1+2x^2+x^3-x^4-3x^5-3x^6-x^7-x^8}{(1-x)^4(1+x)^5}=$

$\frac{(1-x^4)+(x^3-x^8)+(2x^2-2x^5)-(x^5-x^6)+(x^6-x^7)}{(1-x)^4(1+x)^5}=$

$\frac{(1+x)(1+x^2)+x^3(1-x)^4+2x^2(1+x+x^2)-x^5+x^6}{(1-x)^3(1+x)^5}=$

$\frac{1+x-2x^2-2x^3+2x^4+x^3(1-x)^4-x^5(1-x)}{(1-x)^3(1+x)^5}=$

$\frac{(1-x^2)+(x-x^2)-2x^3(1-x)+x^3(1-x)^4-x^5(1-x)}{(1-x)^3(1+x)^5}=$

$\frac{(1+x)+x-2x^3+x^3(1-x)^3-x^5}{(1-x)^2(1+x)^5}=$

$\frac{2x(1-x^2)+x^3(1-x)^3+(1-x^5)}{(1-x)^2(1+x)^5}=$

$\frac{2x(1+x)+x^3(1-x)^2+(1-x)^4}{(1-x)(1+x)^5}$

设$r_{\hat{A}}(x)=2x(1+x)+x^3(1+x)^2+(1-x)^4$,则$r_{\hat{A}}(1)=4\neq 0$,故$(1-x)\nmid r_{\hat{A}}(x)$

又$r_{\hat{A}}(-1)=12=2\neq 0$,有$(1+x)\nmid r_{\hat{A}}(x)$。

综上$\gcd(r_{\hat{A}}(x),(1-x)(1+x)^5)$,故$\hat{A}^{\infty}$的极小生成多项式为$f_{\hat{A}}(x)=(1-x)(1+x)^5$,$\hat{A}^{\infty}$的线性复杂度$LC(\hat{A}^{\infty})=\deg(f_{\hat{A}}(x))=5+1=6$。

定义4 设$\hat{A}_j^{\infty}=(\bar{s}_{j,N-1},\cdots,\bar{s}_{j,1},\bar{s}_{j,0},s_{j,N-1},\cdots,s_{j,1},s_{j,0})$,$\bar{s}_{ji}=p-1-s_{ji}$,$i=0,1,2,\cdots,N-1$,$j=1,2,\cdots,m$是$F_p$上周期为$2N$倒序新序列,则由$\hat{A}_1,\hat{A}_2,\cdots,\hat{A}_m$构成的多维序列$\tilde{A}=(\hat{A}_1,\hat{A}_2,\cdots,\hat{A}_m)$称为$F_p$上$m$-维周期多序列。

m-维多序列$\tilde{A}=(\hat{A}_1,\hat{A}_2,\cdots,\hat{A}_m)$中,序列$\hat{A}_1,\hat{A}_2,\cdots,\hat{A}_m$的共同特征多项式中次数最低的多项式称为多维周期序列$\tilde{A}$的联合极小多项式,记为$f_A(x)$。易见$f_{\tilde{A}}(x)=lcm\left(\hat{f}_1(x),\hat{f}_2(x),\cdots,\hat{f}_m(x)\right)$,其中$\hat{f}_A(x)$表示$\hat{A}_j$,$1\leqslant j\leqslant m$的极小多项式。称$LC\left(\tilde{A}\right)=\deg\left(f_{\tilde{A}}(x)\right)$为多维周期序列$\tilde{A}$的联合线性复杂度。

定理2 设$\tilde{A}=\hat{A}_1,\hat{A}_2,\cdots,\hat{A}_m$为$F_p$上$p$元$2N$-周期多维序列,若$\hat{A}_j$的极小多项式为$f_j(x)$,$1\leqslant j\leqslant m$,则$\tilde{A}$的联合极小多项式为$f_{\tilde{A}}(x)=(1-x)\left(1+x^N\right)$。

证明:由定理1 $\hat{f}_j(x)=(1-x)\left(1+x^N\right)$,$j=1,2,\cdots,m$,则有

$f_{\tilde{A}}(x)=lcm\left(\hat{f}_1(x),\hat{f}_2(x),\cdots,\hat{f}_m(x)\right)=$

$lcm\left((1-x)\left(1+x^N\right),(1-x)\left(1+x^N\right),\cdots,(1-x)\left(1+x^N\right)\right)=$

$(1-x)\left(1+x^N\right)$。

推论2 设F_p上,p元$2N$-周期多维序列$\tilde{A}=(\hat{A}_1,\hat{A}_2,\cdots,\hat{A}_m)$,$\hat{f}_j(x)$,$1\leqslant j\leqslant m$为$\hat{A}_j$的极小多项式,则$\tilde{A}$的联合线性复杂度为$LC(\tilde{A})=N+1$。

证明:因$LC\left(\tilde{A}\right)=\deg\left(f_{\tilde{A}}(x)\right)$,由定理2即得。

例3 设在F_3上,三元3-周期序列s_1^3=(1,1,2),s_2^3=(0,2,1),s_3^3=(2,2,1),则其对偶周期序列分别为$\bar{s}_1^3$=(1,1,0),$\bar{s}_2^3$=(2,0,1),$\bar{s}_3^3$=(0,0,1),将$s_1^3,s_2^3s_3^3$与$\bar{s}_1^3,\bar{s}_2^3\bar{s}_3^3$对应组成周期倒序新序列$\hat{A}_1^6$=(0,1,1,2,1,1),$\hat{A}_2^6$=(1,0,2,1,2,0),$\hat{A}_3^6$=(1,0,0,1,2,2)。并由$\hat{A}_1^6,\hat{A}_2^6,\hat{A}_3^6$构成多维周期新序列为$\tilde{A}^{\infty}=\left(\hat{A}_1^{\infty},\hat{A}_2^{\infty},\hat{A}_3^{\infty}\right)$,求$\tilde{A}^{\infty}$的联合线性复杂度$LC(\tilde{A}^{\infty})$。

解:$\hat{A}_1^{\infty}(x)=\frac{\hat{A}_1^6(x)}{1-x^6}=\frac{x+x^2+2x^3+x^4+x^5}{1-x^6}=\frac{x+x^2-x^3-2x^4+x^5}{(1-x)^3(1+x)^3}=$

$\frac{(x+x^2)(1-x^2)-x^4(1-x)}{(1-x)^3(1+x)^3}\ \frac{(x+x^2)(1+x)-x^4}{(1-x)^2(1+x)^3}=$

$\frac{x+2x^2+x^3-x^4}{(1-x)^2(1+x)^3}=\frac{(x-x^2)+x^3(1-x)}{(1-x)^2(1+x)^3}=\frac{x+x^3}{(1-x)(1+x)^3}$

设$r_{\hat{A}}(x)=x+x^3$,则$r_{\hat{A}}(1)=2\neq 0$,有$(1-x)\nmid r_{\hat{A}}(x)$,又$r_{\hat{A}}(-1)=-2=1\neq 0$,即有$(1+x)\nmid r_{\hat{A}}(x)$,故$\gcd(x+x^3,(1-x)(1+x)^3)=1$,则$\hat{A}_1^{\infty}$的极小多项式为$\hat{f}_1(x)=(1-x)(1+x)^3$,同理有$\hat{f}_2(x)=(1-x)(1+x)^3$,$\hat{f}_3(x)=(1-x)(1+x)^3$,$\tilde{A}$的联合极小多项式$f_{\tilde{A}}(x)=lcm\left(\hat{f}_1(x),\hat{f}_2(x),\hat{f}_3(x)\right)=(1-x)(1+x)^3$,故$\tilde{A}$的联合线性复杂度$LC(\tilde{A})=3+1=4$。

3 结语

由序列S及其对偶序列$\bar{S}$构造出了一类新周期序列的相关思想,本文研究了F_p上这类新周期序列的倒序序列的稳定性。给出了这类倒序新序列的极小多项式和线性复杂度,并利用F_3及F_5上的序列验证了所得结论的正确性。最后用这类倒序新序列构造了多维序列,给出多维序列的联合极小多项式和联合线性复杂度,亦通过F_3上的多维序列验证了结论。这些研究成果为序列稳定性的研究提供了理论支撑,为后续研究序列期望方差的界提供了便利。

参考文献:

[1] SHANNON C E. Communication theory of secret system [J]. Bell.Syst.Tech. 1949(28):656-715.

(下转第113页)

[4] 马卫,刘蓉.旅游行业从业人员计算机应用技能需求调查分析与思考[J].中小企业管理与科技,2012,21(1):193-194.
[5] 秦兆祥.旅游管理专业本科学生核心竞争力培养机制实证研究[J].内蒙古师范大学学报(教育科学版),2012,25(5):95-98.
[6] 胡伏湘,方玲玉.基于大数据思维的教育教学模式探析[J].湖南行政学院学报,2018,18(5):25-29.
[7] 刘蓉.突出行业需求特色的计算机应用技能培养研究[J].电脑知识与技术,2012,8(24):5845-5847.
[8] 刘金岭."数据库原理及应用"教学中的项目教学法[J].计算机教育,2009,7(24):96-98.
[9] 李俊.基于 OBE 的"数据库理论与技术"课程教学改革研究[J].宁波工程学院学报,2018,30(1):90-94.
[10] 钱进.项目驱动案例情景为辅的数据库课程教学模式探讨[J].软件工程,2016,19(12):47-49.

(责任编辑:蒋召雪)

(上接第34页)

[2] DIFFIE W, HELLMAN M E. New directions in cryptography [J]. IEEE Trans. Inform.Theory,1976,22(6):644-654.
[3] BERLEKAMP S R.Algebraic coding theory [M].New York: McGraw-Hill,1968.
[4] DING C, XIAO G, SHAN W.The stability theory of stream ciphers[M].Lecture Notes in Computer Science, Springer-Verlag,1991,561:85-88.
[5] 冯登国,肖国镇.序列周期稳定性新度量指标[J].电子学报,1994,22(1):86-90.
[6] 王磊,张玉清,肖国镇.确定周期为p^n的二元序列的k-错线性复杂度的一个快速算法[J].通信学报,2001,22(4):91-95.
[7] 魏仕民.确定周期序列k-错线性复杂度的一个快速算法[J].电子学报,2004,32(5):705-708.
[8] 牛志华,孔得宇.计算有限域$GF(q)$上$2p^n$-周期序列的k-错线性复杂度及其错误序列的算法[J].电子与信息学报,2018,40(7):204-211.
[9] MEIDL W, WINTERHOF A. On the joint linear complexity profile of explicit inversive multisequences[J]. Journal of Complexity, 2005,21(3):324-336.
[10] 王菊香.二元周期倒序序列及其对偶序列的复杂性分析[J].计算机应用研究,2012,29(12):4654-4655.
[11] 王军,朱士信.F_p上周期序列s^∞与$s^{*\infty}$的线性复杂度分析*[J].计算机应用研究,2010,27(6):2297-2298.
[12] 王菊香,马锦锦,王鑫.二元周期多维序列的联合复杂度分析[J].安徽建筑大学学报,2017,25(2):47-49.
[13] 王菊香,唐森.p元周期倒序广义对偶多维序列的复杂性分析[J].井冈山大学学报(自然科学版),2017,38(6):43-47.

(责任编辑:曲继鹏)

(上接第83页)

参考文献:

[1] 张强峰,孙洪涛.我国学生体质健康测试制度的演变[J].体育学刊,2016,23(2):29-33.
[2] 李艳红.浅谈高中学生体质健康测试[J].教育教学论坛,2017(34):217-218.
[3] 庄希琛,任平社,付锦锐.《国家学生体质健康标准》测试指标科学性的完善研究[J].内蒙古体育科技,2010(3):111-112.
[4] 李爱国.对大学生"国家学生体质健康标准"实施时策的研究[J].吉林师范大学学报(自然)科学版,2016(1):46-52.
[5] 李桐.吉林省城市高中《国家学生体质健康标准》实施的研究[D].长春:东北师范大学,2011.
[6] 中国大学生体质与健康研究组.2008年中国学生体质与健康调研报告[R].北京:高等教育出版社,2008.
[7] 王军利.关于学生体质健康测试中存在问题的思考[J].体育学刊,2015(1):70-74.
[8] 冯海.西南地区大学生体质现状调查与分析[J].成都体育学院学报,2014,35(8):66-69.
[9] 骆繁荣.论青少年学生体质健康下降的教育成因及其健康促进[J].青少年体育,2013(6)12-18.
[10] 丁小虎,徐大成.我国中小学体育教学改革的发展趋势[J].体育科技文献通报,2012,20(3):51-54.
[11] 张昕,王怡然.大连市高中生近五年体质健康水平分析研究[J].教育教学论坛,2013(15):171-173.
[12] 中共中央、国务院.中共中央国务院关于加强青少年体育增进青少年体质健康的意见[N].人民日报,2013-01-05:25.
[13] 刘海元.学生体质健康水平下降原因及解决对策[J].体育学刊,2016(1):12-20.

(责任编辑:曲继鹏)