广义 Jacobi 序列的自相关函数

周　璇*　　李　超*,**,***

*(国防科技大学理学院数学与系统科学系　长沙　410073)

**(国防科技大学计算机学院网络与信息安全研究所　长沙　410073)

***(中国科学院软件研究所计算机科学重点实验室　北京　100080)

摘　要：相关函数是衡量序列密码安全性的重要指标。该文讨论了两类广义 Jacobi 序列的自相关特性，给出了它们的自相关函数的取值，结论表明：两类广义 Jacobi 序列都具有良好的自相关特性。

关键词：广义 Jacobi 序列，自相关性

中图分类号：TN918.2　　**文献标识码**：A　　**文章编号**：1009-5896(2005)04-0625-04

Auto-correlation Function of Generalized Jacobi Sequences

Zhou Xuan*　　Li Chao*,**,***

*(*Dept. of Mathematics and System Science, School of Science, NUDT, Changsha* 410073, *China*)

**(*Inst. of Network and Information Security, School of Compute, NUDT, Changsha* 410073, *China*)

***(*Lab. of Computer Science, Inst. of Software, Chinese Academy of Sciences, Beijing* 100080, *China*)

Abstract　Correlation function is the important parameter for studying the security of sequence cipher. This paper discusses the auto-correlation of two classes of generalized Jacobi sequences and gives their values of auto-correlation. The results show that two classes of generalized Jacobi sequences have good auto-correlation properties.

Key words　Generalized Jacobi sequence, Auto-correlation

1　引言

设计性能良好的密钥序列始终是序列密码研究中的热点问题，而性能好的主要标志是序列具有良好的伪随机性、大的周期与高的线性复杂度。文献[1]提出了 Legendre 序列的概念并证明了 Legendre 序列具有良好的伪随机特性；文献[2]进一步研究了 Legendre 序列的线性复杂度特性，求出了 Legendre 序列的线性复杂度与反馈多项式；在文献[1]与文献[2]的基础上，文献[3]定义了广义 Legendre 序列和两类广义 Jacobi 序列，并讨论了它们的线性复杂度；本文计算了当 R=2 时两类广义 Jacobi 序列的自相关函数；结果表明，两类广义 Jacobi 序列都具有良好的自相关特性。

2　定义及性质

定义 1[3]　设奇素数 p，q，$p\neq q$，素数 r 和正整数 e 满足：$r^e\mid(p-1,q-1)$。令 $R=r^e$，在 GF(p) 和 GF(q) 上分别取定本原元 g_1,g_2，令 $h_1=g_1^{(p-1)/R}(\bmod p)$，$h_2=g_2^{(q-1)/R}(\bmod q)$。定义 $\log_p x=j$，若 $(p,x)=1$，$\left(\frac{x}{p}\right)_R=h_1^j(\bmod p)$，$j=0,1,\cdots,R-1$；同理，当 $(q,x)=1$ 时，可以定义 $\log_q x$。令 $n=pq$，当 $(n,x)=1$，定义 $\log_n x=\log_p x+\log_q x(\bmod R)$，其中 $\left(\frac{x}{p}\right)_R$ 表示 x 关于 p 的 R 阶剩余符号：$\left(\frac{x}{p}\right)_R=x^{(p-1)/R}(\bmod p)$。

定义 2[3]　任意取定 GF(R) 上全体元素的一个排列 $\{b_0,b_1,\cdots,b_{R-1}\}$，则 GF($R$) 上的序列 $a=a_0a_1a_2\cdots$ 称为第一类广义 Jacobi 序列，如果序列 $a=a_0a_1a_2\cdots$ 满足：$a_i=0$，当 $(n,i)>1$；$a_i=b_j$，当 $(n,i)=1$ 且 $\log_n i=j$；

如果取定 j_1,j_2，$0\le j_1\le R-1$，$0\le j_2\le R-1$，并定义 $\log_p x=j_1$，当 $p\mid x$；$\log_q x=j_2$，当 $q\mid x$；则 GF(R) 上的序列 $a=a_0a_1a_2\cdots$ 称为第二类广义 Jacobi 序列，是指当 $\log_n i=j$ 时，$a_i=b_j$。

显然，两类广义 Jacobi 序列的最小周期均为 $n=pq$[3]。

2003-12-10 收到，2004-06-02 改回
中国科学院软件研究所计算机科学重点实验室开放基金(syskf0402)和国防科技大学基础研究基金(JC02-02-007)资助课题

本文仅考虑当 $R=2$ 时广义 Jacobi 序列的自相关特性，在下文中，我们都假定 $R=2$ 。

引理 1[4] (Euler 判别条件)设 p 为奇素数，$(p,n)=1$，则 $n^{\frac{p-1}{2}} \equiv \left(\frac{n}{p}\right) (\mathrm{mod}\, p)$ 。

引理 2[4] 设 p 为素数，$n \geq 0$，$f(x)=a_n x^n + a_{n-1}x^{n-1} + \cdots + a_0$，则当 $(p,a_n)=1$，同余方程 $f(x) \equiv 0 (\mathrm{mod}\, p)$ 的解数 k 满足： $k \leq \min(n,p)$ 。

引理 3 当 $R=2$ 时，在定义 1 中所定义的 $\log_p x$ 有如下表达式： $\log_p x = \frac{1}{2}\left[1-\left(\frac{x}{p}\right)\right]$，当 $(p,x)=1$; 其中 $\left(\frac{x}{p}\right)$ 表示 Legendre 符号。相应地，当 $(n,x)=1$ 时，

$$\log_n x = \log_p x + \log_q x \equiv \frac{1}{2}\left[1-\left(\frac{x}{p}\right)\right] + \frac{1}{2}\left[1-\left(\frac{x}{q}\right)\right] \equiv 1 + \frac{1}{2}\left[\left(\frac{x}{p}\right) + \left(\frac{x}{q}\right)\right] (\mathrm{mod}\, 2)。$$

注：在上式中，$1+\frac{1}{2}\left[\left(\frac{x}{p}\right)+\left(\frac{x}{q}\right)\right] (\mathrm{mod}\, 2)$ 仅表示 $1+\frac{1}{2}\left[\left(\frac{x}{p}\right)+\left(\frac{x}{q}\right)\right]$ 的值模 2 的结果，以下同。

证明 由定义及 Legendre 符号的性质，易知结论成立。

引理 4 设 $a(t)$，$a(t+u)$ 如定义 2 中所述，$\{b_0,b_1\}$ 为 GF (2) 中元的任意一个排列，则当 $(t,n)=1$，$(t+u,n)=1$ 时，如下结论成立：

$a(t)=a(t+u)$，当且仅当 $\log_n t + \log_n (t+u) \equiv 0 (\mathrm{mod}\, 2)$

$a(t)+a(t+u)=1$，当且仅当 $\log_n t + \log_n (t+u) \equiv 1 (\mathrm{mod}\, 2)$

证明 仅证明第一个式子，第二个式子可类似证明。

$$\begin{aligned} a(t)=a(t+u) &\Leftrightarrow a(t)=a(t+u)=b_0 \text{ 或 } a(t)=a(t+u)=b_1 \\ &\Leftrightarrow \log_n t = \log_n (t+u) = 0 \text{ 或 } \log_n t = \log_n (t+u) = 1 \\ &\Leftrightarrow \log_n t + \log_n (t+u) \equiv 0 (\mathrm{mod}\, 2)。 \end{aligned}$$

3 广义 Jacobi 序列的自相关特性

对于周期为 n 的二元序列 $a=a_0a_1a_2\cdots$，其自相关函数定义为

$$C_a(u)=\sum_{t=0}^{n-1}(-1)^{a(t)+a(t+u)}, \qquad u=0,1,\cdots,n-1$$

定理 1 设序列 $a=a_0a_1a_2\cdots$ 是周期为 n 的第一类广义 Jacobi 序列，则

$$C_a(u)=\begin{cases} n, & u=0 \\ q-p+1, & u=lp, 1\leq l\leq q-1 \\ p-q+1, & u=lq, 1\leq l\leq p-1 \\ 3-\left[(-1)^{a(u)}+(-1)^{a(-u)}\right], & u\text{为其它} \end{cases}$$

注：在公式中出现的 $-u$ 表示为模 n 下的值，以下同。

证明

$$\begin{aligned} C_a(u) &= \sum_{t=0}^{n-1}(-1)^{a(t)+a(t+u)} \\ &= \sum_{(t,n)\neq 1 \text{或} (t+u,n)\neq 1}(-1)^{a(t)+a(t+u)} + \sum_{(t,n)=1,(t+u,n)=1}(-1)^{a(t)+a(t+u)} \end{aligned} \tag{1}$$

证毕

下面我们分 3 种情况讨论。

情形 1 $u=lp$，$1\leq l\leq q-1$

首先说明满足 $p|t$ 或 $q|t$ 或 $p|t+lp$ 或 $q|t+lp$，$0\leq t\leq n-1$ 的 t 值的个数共有 $2p+q-2$ 个，其中 $t+lp$ 表示模 n 的结果，以下同。

分别设满足上面 4 个条件的 t 值的集合为 U_1，U_2，U_3，U_4，则可知 $|U_1|=|U_3|=q$，$|U_2|=|U_4|=p$。又由 p,q 为奇素数且不相等，$1\leq l\leq q-1$ 知：$U_1\cap U_2=\{0\}$，$U_1=U_3$，$U_2\cap U_4=\phi$，$U_1\cap U_4=\{(q-l)p\}$，故得 $|U_1\cup U_2\cup U_3\cup U_4| = 2p+q-2$。

下面计算式(1)的第 1 部分的值：

$$\sum_{(t,n)\neq 1 \text{或} (t+lp,n)\neq 1}(-1)^{a(t)+a(t+u)} = q + \sum_{i=1}^{p-1}(-1)^{a(iq+lp)} + \sum_{i=1}^{p-1}(-1)^{a(iq-lp)}$$

由引理 3 得

$$\log_n (iq+lp) = 1 + \frac{1}{2}\left(\frac{q}{p}\right)\left[\left(\frac{i}{p}\right)+\left(\frac{l}{q}\right)(-1)^{(p-1)(q-1)/4}\right] (\mathrm{mod}\, 2) \tag{2}$$

由式(2)可知：在模 2 的意义下，$\log_n (iq+lp)=0$ 与 $\log_n (iq+lp)=1$, $1\leq i\leq p-1$ 的个数相等，即 $\sum_{i=1}^{p-1}(-1)^{a(iq+lp)}=0$。

同理，我们可以计算出：$\sum_{i=1}^{p-1}(-1)^{a(iq-lp)}=0$ 。因此

$$\sum_{(t,n)\neq 1 \text{或} (t+lp,n)\neq 1}(-1)^{a(t)+a(t+lp)} = q。$$

再计算式(1)中第 2 部分的值。

由引理 3 可得

$$\log_n t + \log_n (t+lp) = 1 + \frac{1}{2}\left[\left(\frac{t}{q}\right)+\left(\frac{t+lp}{q}\right)\right] (\mathrm{mod}\, 2)$$

由引理 4 知

$$a(t)=a(t+u) \Leftrightarrow \left(\frac{t}{q}\right)=\left(\frac{t+lp}{q}\right)$$

又由引理 1 知

$$\left(\frac{t}{q}\right)=\left(\frac{t+lp}{q}\right) \Leftrightarrow t^{(q-1)/2}-(t+lp)^{(q-1)/2}\equiv 0 (\mathrm{mod}\, q) \tag{3}$$

同理可知

$$a(t)+a(t+lp)=1 \Leftrightarrow t^{(q-1)/2}+(t+lp)^{(q-1)/2}\equiv 0(\mathrm{mod}\,q) \quad (4)$$

因为对 $\forall t$， $t\neq q-1$， $0<t<q$ 均满足同余方程：

$$[t^{(q-1)/2}-(t+lp)^{(q-1)/2}][t^{(q-1)/2}+(t+lp)^{(q-1)/2}]$$

$$=t^{q-1}-(t+lp)^{q-1}\equiv 0(\mathrm{mod}\,q) \quad (5)$$

即同余方程式(3)与同余方程式(4)的解都是同余方程式(5)的解，又易知，同余方程式(5)的解是且仅是同余方程式(3)与同余方程式(4)中的一个同余方程的解。设同余方程式(3)的解的个数为 k_1，同余方程式(4)解的个数为 k_2，则有 $k_1+k_2=q-2$。

由引理 2 知

$$k_1\le \min((q-3)/2,q)=(q-3)/2$$

$$k_2\le \min((q-1)/2,q)=(q-1)/2$$

因此，可得 $k_1=(q-3)/2$， $k_2=(q-1)/2$。

所以，在 $0<t<n$，同余方程式(3)解的个数为 $(q-3)p/2$，同余方程式(4)解的个数为 $(q-1)p/2$。

又因为 $t\neq ip$， $0<i<q$， $i\in N$，由下面两式：$(ip)^{(q-1)/2}-(ip+lp)^{(q-1)/2}\equiv 0(\mathrm{mod}\,q)$，有 $(q-3)/2$ 个解；$(ip)^{(q-1)/2}+(ip+lp)^{(q-1)/2}\equiv 0(\mathrm{mod}\,q)$，有 $(q-1)/2$ 个解；因此，满足式(3)的 t 值共有 $(q-3)(p-1)/2$ 个，而满足式(4)的 t 值共有 $(q-1)(p-1)/2$ 个，所以得到

$$\sum_{(t,n)=1,(t+lp,n)=1}(-1)^{a(t)+a(t+u)}=1-p$$

综合可得到

$$\sum_{t=0}^{n-1}(-1)^{a(t)+a(t+lp)}=q-p+1$$

情形 2　$u=lq$，$1\le l\le p-1$

由上面的计算，同理可得 $\sum_{t=0}^{n-1}(-1)^{a(t)+a(t+lq)}=p-q+1$。

情形 3　u 为其它的情况，且 $u\neq 0$ 时，由情形 1 中的证明可类似证明，此时满足 $p|t$ 或 $q|t$ 或 $p|t+u$ 或 $q|t+u$ 的 t 值 $(0\le t\le n-1)$ 共有 $2p+2q-4$ 个。

下面我们依然先计算式（1）的第 1 部分。

由引理 3：

$$\sum_{(t,n)\neq 1\text{或}(t+u,n)\neq 1}(-1)^{a(t)+a(t+u)}=\sum_{i=0}^{q-1}(-1)^{a(ip+u)}+\sum_{i=0}^{q-1}(-1)^{a(ip-u)}$$

$$+\sum_{i=1}^{p-1}(-1)^{a(iq+u)}+\sum_{i=1}^{p-1}(-1)^{a(iq-u)}-2 \quad (6)$$

因为 $\log_n(ip+u)=\frac{1}{2}\left[\left(\frac{u}{p}\right)+\left(\frac{ip+u}{q}\right)\right](\mathrm{mod}\,2)$，则易知：对 $\forall i$，$i\neq i_0$，$0\le i\le q-1$ 都有 $\log_n(ip+u)=0$，或 $\log_n(ip+u)=1$，且个数相等，其中 i_0 满足 $0\le i_0\le q-1$，$q|(i_0p+u)$，故可得到 $\sum_{i=0}^{q-1}(-1)^{a(ip)+a(ip+u)}=1$。

同理可计算得到式（6）中第 2，3，4 项的值分别为 1，$1-(-1)^{a(u)}$，$1-(-1)^{a(-u)}$，因而有

$$\sum_{(t,n)\neq 1\text{或}(t+u,n)\neq 1}(-1)^{a(t)+a(t+u)}=2-\left((-1)^{a(u)}+(-1)^{a(-u)}\right)$$

下面我们计算式(1)第 2 部分的值。

由引理 3：

$$\log_n t+\log_n(t+u)=\frac{1}{2}\left[\left(\frac{t}{p}\right)+\left(\frac{t}{q}\right)+\left(\frac{t+u}{p}\right)+\left(\frac{t+u}{q}\right)\right](\mathrm{mod}\,2)$$

由引理 4：

$$a(t)=a(t+u)\Leftrightarrow\begin{cases}\left(\frac{t}{p}\right)=\left(\frac{t+u}{p}\right)\\ \left(\frac{t}{q}\right)=\left(\frac{t+u}{q}\right)\end{cases}\text{或}\begin{cases}\left(\frac{t}{p}\right)+\left(\frac{t+u}{p}\right)=0\\ \left(\frac{t}{q}\right)+\left(\frac{t+u}{q}\right)=0\end{cases}$$

$$a(t)+a(t+u)=1\Leftrightarrow\begin{cases}\left(\frac{t}{p}\right)+\left(\frac{t+u}{p}\right)=0\\ \left(\frac{t}{q}\right)=\left(\frac{t+u}{q}\right)\end{cases}\text{或}\begin{cases}\left(\frac{t}{p}\right)=\left(\frac{t+u}{p}\right)\\ \left(\frac{t}{q}\right)+\left(\frac{t+u}{q}\right)=0\end{cases}$$

则由引理 1 可知，上面的 4 个方程组可化成下面形式：

$$\begin{cases}t^{(p-1)/2}-(t+u)^{(p-1)/2}\equiv 0(\mathrm{mod}\,p)\\ t^{(q-1)/2}-(t+u)^{(q-1)/2}\equiv 0(\mathrm{mod}\,q)\end{cases}\text{或}$$

$$\begin{cases}t^{(p-1)/2}+(t+u)^{(p-1)/2}\equiv 0(\mathrm{mod}\,p)\\ t^{(q-1)/2}+(t+u)^{(q-1)/2}\equiv 0(\mathrm{mod}\,q)\end{cases}$$

$$\text{与}\begin{cases}t^{(p-1)/2}+(t+u)^{(p-1)/2}\equiv 0(\mathrm{mod}\,p)\\ t^{(q-1)/2}-(t+u)^{(q-1)/2}\equiv 0(\mathrm{mod}\,q)\end{cases}\text{或}$$

$$\begin{cases}t^{(p-1)/2}-(t+u)^{(p-1)/2}\equiv 0(\mathrm{mod}\,p)\\ t^{(q-1)/2}+(t+u)^{(q-1)/2}\equiv 0(\mathrm{mod}\,q)\end{cases}$$

令 B_0,B_1,B_2,B_3 分别为上面 4 个同余方程组解的个数，下面以第 1 个同余方程组为例说明 $B_i(0\le i\le 3)$ 的求法。

由情形 1 的解法可得，当 $0\le t\le p-1$，同余方程 $t^{(p-1)/2}-(t+u)^{(p-1)/2}\equiv 0(\mathrm{mod}\,p)$ 有 $(p-3)/2$ 个解，设为 $t_i(0\le i\le(p-3)/2)$；当 $0\le t\le q-1$，同余方程 $t^{(q-1)/2}-(t+u)^{(q-1)/2}\equiv 0(\mathrm{mod}\,q)$ 有 $(q-3)/2$ 个解，设为 $t_j(0\le j\le(q-3)/2)$；则由中国剩余定理可知，对于每个同余方程组：

$$\left.\begin{aligned}x&\equiv t_i(\mathrm{mod}\,p)\\ x&\equiv t_j(\mathrm{mod}\,q)\end{aligned}\right\},\quad 0\le t_i\le(p-3)/2,\quad 0\le t_j\le(q-3)/2$$

在 $0\le x\le n-1$ 中有唯一的解，故同余方程组式(3)的解数为 $(p-3)(q-3)/4$。同理可求得 $B_1=(p-1)(q-1)/4$，

$B_2=(p-1)(q-3)/4$， $B_3=(p-3)(q-1)/4$，从而有

$$\sum_{(t,n)=1,(t+u,n)=1}(-1)^{a(t)+a(t+u)}=B_0+B_1-B_2-B_3=1$$

综合可知：

$$\sum_{t=0}^{n-1}(-1)^{a(t)+a(t+u)}=3-\left[(-1)^{a(u)}+(-1)^{a(-u)}\right]$$

定理 2 设序列 $a=a_0a_1a_2\cdots$ 为周期为 n 的第二类广义 Jacobi 序列，$\{b_0,b_1\}$ 为 GF(2) 中元素的任一排列，j_1,j_2 如定义 2 中所示，又设 $x,y\in N$，使得 $yq-xp=1$，则

当 $u=0, C_a(0)=n$；

当 $u=lp, 1\le l\le q-1$，

$C_a(lp)=-p+(-1)^{a(0)+a(lp)}+(-1)^{a(0)+a(-lp)}$；

当 $u=lq, 1\le l\le p-1$，

$C_a(lq)=-q+(-1)^{a(0)+a(lq)}+(-1)^{a(0)+a(-lq)}$；

当 u 为其它值时，

$$\begin{aligned}C_a(u)=&1+(-1)^{a(0)+a(u)}+(-1)^{a(0)+a(-u)}\\&+2(-1)^{a(xup)+a(yuq)}+2(-1)^{a(-xup)+a(-yuq)}\\&+(-1)^{x_1}+(-1)^{x_2}+(-1)^{x_3}+(-1)^{x_4}。\end{aligned}$$

其中 $x_i\ (1\le i\le 4)$ 的定义分别如下：

$$x_1=b_{j_1+\frac{1}{2}\left[1-\left(\frac{u}{p}\right)\right]},\quad x_2=b_{j_1+\frac{1}{2}\left[1-\left(\frac{-u}{p}\right)\right]}$$

$$x_3=b_{j_2+\frac{1}{2}\left[1-\left(\frac{u}{q}\right)\right]},\quad x_4=b_{j_2+\frac{1}{2}\left[1-\left(\frac{-u}{q}\right)\right]}$$

在上式中的下标的结果都表示模 2 后的值。

证明 与定理 1 类似证明，在此从略。

4 结束语

本文仅讨论了两类广义 Jacobi 序列当 $R=2$ 时的自相关特性，结论表明第一类广义 Jacobi 序列的自相关性比第二类广义 Jacobi 序列的略好，至于当 R 为其它值时的自相关特性还有待于进一步讨论。

参 考 文 献

[1] Damgaard I. On the randomness of Legendre and Jacobi sequences. Advances. in Cryptology, CRRPTO'88, Springer-Verlag, 1990: 163 – 172.

[2] Ding C, Helleseth T, Shan W. On the complexity of Legendre sequences. *IEEE Trans. on Information Theory*, 1998, 44(3): 1276 – 1278.

[3] 胡予濮，魏仕民，肖国镇. 广义 Legendre 序列和广义 Jacobi 序列的线性复杂度. 电子学报，2000，28(2)：113 – 117.

[4] 潘承洞，潘承彪. 初等数论. 北京：北京大学出版社，1991：150 – 231.

[5] 胡予濮，张玉清，肖国镇. 对称密码学. 北京：机械工业出版社，2002：96 – 107.

周 璇： 男，1979 年生，硕士生，研究方向为编码与密码.

李 超： 男，1966 年生，教授，研究方向为编码与密码.