文章编号:1671 - 6833(2007)02 - 0110 - 04

Jennings 复合序列的一些补注

王锦玲,雷玉印,杨 娜,王 静

(郑州大学 数学系,河南 郑州 450001)

摘 要:引入了一组向量,用真值描述的方法对 Jennings 复合序列的定义进行了新的推导,并对该序列的有关周期、线性复杂度的定理的证明作了简化和补充. 为了度量序列的稳定性,引入了重量复杂度 $WC_k(u^\infty)$,给出了它的 1 - 重量复杂度和 2 - 重量复杂度下限;当 $1 = k < m$ 时,下限为 $(2^m - 1)(2^n - 1) - n(m + 1)$;当 $2 \le k < m$ 时,下限为 $(2^m - 1)(2^n - 1) - n\sum_{i=0}^{k} C_m^i$;当 $k = m$ 时,下限为 $(2^m - 1)(2^n - 1) - n(2^m - 1)$. 分析了该序列线性复杂度的稳定性.

关键词:周期;线性复杂度;特征多项式;复合序列;重量复杂度

中图分类号:O 157.4 **文献标识码**:A

0 引言

线性复杂度是衡量密钥流序列稳定性的指标之一. 一般而言,其数值越大,对应的序列密码性能越好,但在实际应用上,我们希望线性复杂度大且易于控制. Jennings 给出控制线性复杂度的方法,他把得到的序列称作 Jennings 复合序列. 本文对 Jennings 复合序列[1] 的定义、周期、线性复杂度有关定理进一步作了简化证明的补充. 并给出了它的 1,2 - 重量复杂度[2] 下界.

1 Jennings 复合序列的结构

设 GF(2) 上的 m 级 m 序列 a^∞ 的模型为 LFSR1,其状态为 $A_i, i = 0 \sim m - 1$,极小多项式为 $f(x)$;GF(2) 上的 n 级 m 序列 b^∞ 的模型为 LFSR2,其状态为 $B_j, j = 0 \sim n - 1$,极小多项式为 $g(x)$. 设 $2^m - 1 < n, \gcd(m,n) = 1$. 选择 $k \in Z^+$, $1 \le k \le m; \tau_i \in Z^+, i = 0,1,\cdots,k-1$,使 $0 = \tau_0 < \tau_1 < \tau_2 < \cdots < \tau_{k-1} < m$.

引理 1 对 $\forall x \in 0 \sim 2^n - 1, x \in Z^+$;$GF(2)^n$ 表示二次元域上的 n 维向量空间,则有二进制表示 $x = x_1 \cdot 2^{n-1} + x_2 \cdot 2^{n-2} + \cdots + x_n$. 从而 $\{0,1,\cdots, 2^n - 1\}$. 与向量 $\boldsymbol{X} = (x_1, x_2, \cdots, x_n) \in GF(2)^n$ 存在一一对应关系.

因此,$N(t) = A_0(t) + A_{\tau 1}(t) \cdot 2 + \cdots + A_{\tau_{k-1}}(t) \cdot 2^{k-1} = a_{t+\tau 0} + a_{t+\tau 1} \cdot 2 + \cdots + a_{t+\tau_{k-1}} \cdot 2^{k-1}$. $N(t) \in \{0,1,\cdots 2^k - 1\}$ 与向量 $\boldsymbol{a} = (a_{t+\tau 0}, a_{t+\tau 1}, \cdots, a_{t+\tau_{k-1}})$ 对应. 分两种情形:

$k < m$,选单射 $\gamma: \{0,1,\cdots 2^k - 1\} \to \{0,1,\cdots n - 1\}$;

$k = m$,选 $\gamma: \{1,2,\cdots 2^m - 1\} \to \{0,1,\cdots n - 1\}$.

定义 1 将以上两条序列 a^∞, b^∞ 复合得 u^∞: $u_t = B_{\gamma(N(t))}(t)$.

因 $B_j(t) = B_0(t + j) = b_{t+j}$,故 $u_t = b_{t+\gamma(N(t))}$. 设 $k < m$,$\{A(j)\ j = 0,\cdots,2^k - 1\}$ 为 $\{0,\cdots,k-1\}$ 的幂集. $A(j)$ 以 Hamming 重量排列:$A(0) = \varnothing, A(2^k - 1) = \{0,1,\cdots,k-1\}$,若 $i < j$,则 $|A(i)| < |A(j)|$. 定义:

$$P_j(t) = \prod_{l \in A(j)} a_{t+\tau_l} (j = 0,1,\cdots,2^k - 1).$$

引理 2 GF(2) 上 n 级 m 序列 t^∞ 的 r 个平移序列 t_i^∞,任取 r 个 m_i 属于 GF(2),则 $\sum_{i=1}^{r} m_i t_i^\infty$ 为 0 序列或 t^∞ 的一个平移序列.

定理 1 若 $k < m$,则 $u_t = \sum_{j=0}^{2k-1} P_j(t) b_{t+v_j}$. 其中 $(v_0,\cdots,v_{2k-1})$ 取决于 $(\gamma(0),\cdots,\gamma(2^k - 1))$,且 2^k 个序列 $b_{vj}^\infty = b_{vj} b_{vj+1} \cdots (j = 0 \sim 2^k - 1)$ 在 GF(2) 上线性独立.

证 $N(t)$ 与 $\boldsymbol{a} = (a_{t+\tau_0}, a_{t+\tau_1}, \cdots, a_{t+\tau_{k-1}})$ 对应,故取向量一组特值,其余由它线性表出. 向量中 1 对应的序号在 $A(j)$ 中时,令 $N(t) = \rho(j)$. 于

收稿日期:2006 - 12 - 15 **修订日期**:2007 - 03 - 20

基金项目:河南省教育厅自然科学研究项目(200510459003)

作者简介:王锦玲(1963 -),女,河北安国人,郑州大学副教授,主要从事代数与密码学方面的研究.

是有以下对应：

$$\begin{array}{llll}(a_{t+\tau_0} & a_{t+\tau_1} & \cdots & a_t+\tau_{k-1}) \quad N(t)\to u_t\\ (0 & 0 & \cdots & 0) \quad b_{t+\rho_0}\\ (1 & 0 & \cdots & 0) \quad b_{t+\rho_1}\\ (0 & 1 & \cdots & 0) \quad b_{t+\rho_2}\\ & & \vdots & \\ (0 & 0 & \cdots & 1) \quad b_{t+\rho_k}\\ (1 & 1 & \cdots & 1) \quad b_{t+\rho_{2k-1}}\end{array}$$

于是，我们得到

$$\begin{aligned}u_t &= b_{t+\gamma(N(t))}\\ &= (1+a_t)\cdot(1+a_{t+\tau 1})\cdots(1+a_{t+\tau_{k-1}})\cdot b_{t+\rho_0}\\ &\quad + a_t(1+a_{t+\tau 1})\cdots(1+a_{t+\tau_{k-1}})\cdot b_{t+\rho_1}\\ &\quad + \cdots + a_t\cdot a_{t+\tau 1}\cdots a_{t+\tau_{k-1}}\cdot b_{t+\rho_k}\\ &\quad + a_t\cdot a_{t+\tau 1}\cdots a_{t+\tau_{k-1}}\cdot b_{t+\rho_{2k-1}}\\ &= \{P_0(t)+P_1(t)+\cdots+P_{2^{k-1}}(t)\}b_{t+\rho_0}\\ &\quad + \{P_1(t)+P_2(t)+\cdots+P_{2^{k-1}}(t)\}b_{t+\rho_1}+\cdots\\ &\quad + P_{2^{k-1}}(t)b_{t+\rho_{2k-1}}\\ &= \sum_{j=0}^{2^k-1}\{\prod_{l\in A(j)}a_{t+\tau_l}\prod_{e\in\overline{A(j)}}(1+a_{t+\tau_e})\}b_{t+\rho(j)}\\ &= \sum_{j=0}^{2^k-1}\{\sum_{A(i)\supseteq A(j)}\prod_{l\in A(j)}a_{t+\tau_l}\}b_{t+\rho(j)}\\ &= \sum_{j=0}^{2^k-1}\{\sum_{A(i)\supseteq A(j)}P_i(t)\}b_{t+\rho(j)}\\ &= \sum_{i=0}^{2^k-1}P_i(t)(\sum_{A(j)\subseteq A(i)}b_{t+\rho(j)}).\end{aligned}\tag{1}$$

进一步地，我们又得到 $\{\sum_{A(j)\subseteq A(i)}b_{t+\rho_j}|j=0\sim 2^k-1\}$ 与 $\{b_{t+\rho j}|j=0\sim 2^k-1\}$ 对应矩阵的行列式非零. 故矩阵可逆，故对应的变换可逆. 由引理 2，$\{b_{t+\rho j}|j=0\sim 2^k-1\}$ 在 GF(2) 上线性独立，故 $\{\sum_{A(j)\subseteq A(i)}b_{t+\rho_j}|j=0\sim 2^k-1\}$ 在 GF 上线性独立.

2　Jennings 复合序列的周期及线性复杂度

定义 2　设 C 是代数封闭域[3]，K,E,F 均是 C 的子域，$K\subset E\cap F$，E 和 F 在 K 上线性无缘指 E 的每个集合若在 K 上线性无关，则在 F 也线性无关.

引理 3　E 的子集 X 在 C 的某个子域上线性无关 $\Leftrightarrow X$ 的每个有限子集在此子域上线性无关. 可见，若 $K\subset E$，则 E 和 K 在 K 上线性无缘.

设 $f(x)$ 在 GF(2^m) 一根为 α，$g(x)$ 在 GF(2^n) 一根为 β，则有 $f(x)=\prod_{i=0}^{m-1}(x+\alpha^{2^i})$，$g(x)=\prod_{j=0}^{n-1}(x+\beta^{2^j})$. $w_H(i)$ 为 i 的汉明重量. 对 $1\le s\le m$，定义多项式 $F_s(x)=\prod_{\substack{1\le i\le 2^m-1\\ 1\le w_H(i)\le s}}(x+\alpha^i)$. 由于 $\alpha,\alpha^2,\cdots,\alpha^{2^{m-1}}$ 为 $f(x)$ 在 GF(2^n) 上互异的单根，所以 $F_s(x)$ 为 GF(2) 上的多项式. 下证 $F_s(x)$ 的次数为：$\sum_{j=1}^{s}C_m^i$. 考虑分裂域 $K^{(n)}$ 上的分圆多项式[4]. 令 $E^{(n)}=\{\xi\mid\xi^n=1,\xi\in K^{(n)}\}=\langle\xi\rangle$. ξ^s 为 n 次本原单位根，则有 n 次本原多项式：

$$Q_n(x)=\prod_{s=1}^{n}(x-\xi^s),\text{其中 }\gcd(s,n)=1\tag{2}$$

根据前馈序列的知识有

$$Q_r=\{q\mid 1\le q\le 2^n-1,w_H(q)\le r\}\tag{3}$$

其中 $|Q_r|=\sum_{i=1}^{r}C_n^i$. Q_r 是 mod(2^n-1) 的若干分圆陪集的并集. α 为 $f(x)$ 在 GF(2^m) 上的本原根，所以 $F_s(x)$ 的表达式就是分圆多项式，故 $Q_s=\{i\mid 1\le i\le 2^m-1,w_H(i)\le s\}$，其中 $|Q_s|=\sum_{j=1}^{s}C_m^j$. Q_s 是 mod(2^m-1) 的若干分圆陪集的并集，而所有分圆陪集含有无素的个数恰好就是分圆多项式的次数. 所以 $\deg(F_s(x))=\sum_{j=1}^{s}C_m^i$. 记 $F(x)=(x+1)\prod_{\substack{1\le i\le 2^m-1\\ 1\le w_H(i)\le k}}(x+\alpha^i)=\prod_{\substack{0\le i\le 2^m-1\\ 0\le w_H(i)\le k}}(x+\alpha^i)$. 因 $1,\alpha,\alpha^2,\cdots,\alpha^{2^k-1}$ 为 $F(x)$ 互异的单根，$1,\beta,\beta^2,\cdots,b^{2^n-1}$ 为 $g(x)$ 互异的单根，所以有

$$H(x)=\prod_{\substack{0\le i\le 2^m-1\\ 0\le w_H(i)\le k}}\prod_{j=0}^{n-1}(1+\frac{x}{\alpha^i\beta^{2^j}})\tag{4}$$

为 GF(2) 上的多项式.

引理 4　GF(q) 上一周期序列 s^∞，GF(q) 上的多项式 $f(x)$ 有 m 个单根 $\{x_1,\cdots,x_m\}$，其中 $f(0)=1$. 若 $s_n=\sum_{i=1}^{m}b_ix_i^{-n}(n=0,1,2,\cdots)$，则某个 x_i 是 s^∞ 的极小多项式的根 $\Leftrightarrow b_i\neq 0$.

引理 5　设 2^k 个序列[5] $b_{vj}^\infty=b_{vj}b_{vj+1}\cdots(j=0,1,\cdots 2^k-1)$. 令 $\xi_j=\beta^{vj}$，则 ①$b_{vj+t}=\sum_{r=0}^{n-1}\xi_j^{2r}\beta^{2^r\cdot t}$；②$\{\xi_j\mid j=0\sim 2^k-1\}$ 在 GF(2) 线性无关；③满足(1)，(2) 的 $\{\xi_j\mid j=0\sim 2^k-1\}$ 唯一.

定理 2　若 $k<m$，则在 GF(2^{mn}) 上存在唯一的一组元素 $\{\eta_{ij}\}$，使得

$$u_t=\sum_{\substack{0\le i\le 2^m-1\\ 0\le w_H(i)\le k}}\sum_{j=0}^{n-1}\{\eta_{ij}\}(\alpha^i\beta^{2j})^t\tag{5}$$

对 $\forall (i,j), \eta_{ij} \neq 0 \Leftrightarrow \{P_j(t) \mid j = 0,1,2,\cdots,2^k - 1\}$ 中至少有一函数,其 α^t 的多项式表示中 α^{it} 的系数非零.

证 $u_t = \sum_{j=0}^{2^k-1} P_j(t) b_{t+v_j}, b_{v_j+t} = \sum_{r=0}^{n-1} \xi_j^{2r} \beta^{2^r \cdot t}$,再由 $P_j(t)$ 的表达式可得定理中的式子. 其中 $\eta_{ij} = \sum_{l=0}^{2^k-1} \delta_l \xi_l^{2j}$,$\delta_l$ 是 $P_l(t)$ 作为 α^t 的多项式时 α^{it} 的系数. 由于 $H(x) = \prod_{\substack{1 \le i \le 2^m-1 \\ 1 \le w_H(i) \le k}} \prod_{j=0}^{n-1} (1 + \frac{x}{\alpha^i \beta^{2^j}})$ 为 GF(2) 上的多项式,根据引理4,要在 $GF(2^{mn})$ 上存在一组元素 η_{ij},使它对应的序列为

$$u_t = \sum_{\substack{1 \le i \le 2^m-1 \\ 1 \le w_H(i) \le k}} \sum_{j=0}^{n-1} \{\eta_{ij}\} (\alpha^i \beta^{2^j})^t. \qquad (6)$$

$H(x)$ 为 u^∞ 的特征多项式,为极小多项式等价于 $\eta_{ij} \neq 0$. $H(x)$ 的根是 $F(x)$ 与 $g(x)$ 根的乘积,故 $\alpha^i \beta^{2^j}$ 是 $H(x)$ 的根 $\Leftrightarrow \eta_{ij} \neq 0$. ①$\delta_l$ 属于 $GF(2^{mn})$;②$\{\xi_l^{2^j} \mid l = 0 \sim 2^k - 1\}$ 在 $GF(2^n)$ 上线性无关,所以 $\{\delta_l \mid l = 0 \sim 2^k - 1\}$ 不全为零 $\Leftrightarrow \eta_{ij} \neq 0$.

定理3 复合序列 u^∞ 的极小多项式 $h(x)$ 满足 ① 若 $1 = k < m$,则 $h(x) = H(x)$,其次数为 $n(m+1)$,② 若 $2 \le k < m$ 且 $(\tau_0, \tau_1, \cdots, \tau_{k-1})$ 之间等距,则 $h(x) = H(x)$,其次数为 $n(\sum_{i=0}^{k} C_m^i)$.

证 ①因 $P_1(t) = a_t = \sum_{r=0}^{m-1} \alpha^{2^r \cdot t}$,故对 $\forall i = 2^r$, $r \in \{(0 \sim m-1)\}$,有 α^{it} 的系数非零,故 $\eta_{2^i,j} \neq 0$,从而 $h(x) = H(x)$,故 $\deg(h(x)) = \deg(H(x))$. 又 ①$F(x), g(x)$ 的根全为单根,②$F(x), g(x)$ 根的乘积互不相同,故 $\deg(H(x)) = \deg(F(x)) \times \deg(g(x)) = n(C_m^0 + C_m^1) = n(m+1)$,③ 设 $2 \le k < m, \tau_1 = d, \tau_2 = 2d, \cdots, \tau_{k-1} = (k-1)d$. 下证 $\eta_{ij} \neq 0$. 选择 $P_l(t) = a_t a_{t+d} \cdots a_{t+(s-1)d}$,令 $i = 2^{i_1} + 2^{i_2} + \cdots + 2^{i_s}$,其中 $2 \le s \le k, 0 \le i_1 < \cdots < i_s \le m-1$. 故 $P_l(t) = \sum_{r_0=0}^{m-1} \sum_{r_1=0}^{m-1} \cdots \sum_{r_s-1=0}^{m-1} \alpha^u \alpha^{wt}$. 其中,$u = 2^{r_1 d} + 2^{r_2 2d} + \cdots + 2^{r_{s-1}(s-1)d}, w = 2^{r_0} + 2^{r_1} + \cdots + 2^{r_{s-1}}$. 来证对于 $w = i = 2^{i_1} + 2^{i_2} + \cdots + 2^{i_s}$,$\alpha^{wt}$ 的系数非零. 事实上 α^{it} 的系数为:

$$\begin{vmatrix} 1 & 1 & \cdots & 1 \\ (\alpha^{d2^{i_1}}) & (\alpha^{d2^{i_2}}) & \cdots & (\alpha^{d2^{i_s}}) \\ (\alpha^{d2^{i_1}})^2 & (\alpha^{d2^{i_2}})^2 & \cdots & (\alpha^{d2^{i_s}})^2 \\ \vdots & \vdots & \ddots & \vdots \\ (\alpha^{d2^{i_1}})^{s-1} & (\alpha^{d2^{i_2}})^{s-1} & \cdots & (\alpha^{d2^{i_s}})^{s-1} \end{vmatrix}$$

记该行列式为 Δ,则 $\Delta = \prod_{u<v} \{(\alpha^d)^{2^{iu}} - (\alpha^d)^{2^{iv}}\}$. 又 $\alpha^d, (\alpha^d)^2, \cdots, (\alpha^d)^{2^{is}}$ 两两互异,故 $\Delta \neq 0$. 故 $h(x) = H(x)$ 是极小多项式,从而

$$\deg(h(x)) = \deg(H(x)) = n \times \sum_{i=0}^{k} C_m^i.$$

定理4 设 Jennings 复合序列的最小周期为 N,则 $N = (2^m - 1)(2^n - 1)$.

证 由 u_t 表达式,则 N 整除 $(2^m - 1)(2^n - 1)$,从而 $N \le (2^m - 1)(2^n - 1)$. $\alpha\beta$ 是 $h(x)$ 一根,$o(\alpha\beta) = (2^m - 1)(2^n - 1)$,所以 $N \ge (2^m - 1)(2^n - 1)$,由此定理成立.

定理5 若 $k = m$,则 Jennings 复合序列的线性复杂度为 $L(u^\infty) = \deg(u^\infty) = n(2^m - 1)$.

证 $L(u^\infty) = \deg(u^\infty) = n \times \sum_{i=1}^{m} C_m^i = n(2^m - 1)$.

3 Jennings 复合序列的 1 - 重量复杂度下界

定理6 设 Jennings 复合序列的极小多项式的次数为 $\deg(u^\infty)$,它的最小周期为 N,则 Jennings 复合序列的 1 - 重量复杂度下界为

$$WC_1(u^\infty) \ge N - \deg(u^\infty).$$

当 $1 = k < m$ 时,$WC_1(u^\infty) \ge (2^m - 1)(2^n - 1) - n(m+1)$;当 $2 \le k < m$ 时,$WC_1(u^\infty) \ge (2^m - 1)(2^n - 1) - n\sum_{i=0}^{k} C_m^i$;当 $k = m$ 时,$WC_1(u^\infty) \ge (2^m - 1)(2^n - 1) - n(2^m - 1)$.

证 设 w^∞ 时周期为 N 的二元序列,其既约式为 $w^\infty = \frac{r_w}{f_w}$;复合序列 u^∞ 的既约式为 $u^\infty = \frac{r_u}{f_u}$,这里 $f_u = h(x) = H(x)$ 为 u^∞ 的极小多项式. 根据定义[3]有

$$WC_1(u^\infty) = \min_{0 \le i \le N-1} \deg\{\frac{1 - x^N}{\gcd(1 - x^N, x^i + \frac{r_u(1 - x^N)}{f_u})}\}.$$

设 $h(x) = \gcd(1 - x^N, x^i + \frac{r_u(1 - x^N)}{f_u})$,则 $h(x)$ 整除 $1 - x^N$;$h(x)$ 整除 $x^i + \frac{r_u(1 - x^N)}{f_u}$. 因 $f_u(x)$ 不可约,若 $h(x)$ 不为 $f_u(x)$ 的因式,则 $h(x)$ 整除 $\frac{r_u(1 - x^N)}{f_u}$,从而 $h(x)$ 整除 x^i,这与 $h(x)$ 整除 $1 - x^N$ 矛盾,所以 $h(x) = 1$ 或 $h(x) = f_u(x)$. 故 $WC_1(u^\infty) \ge \min_{0 \le i \le N-1} \deg\{\frac{1 - x^N}{f_u(x)}\}$.

定理7 Jennings 复合序列的 2 - 重量复杂度为 $WC_2(u^\infty) \ge N - G - \deg(u^\infty)$,其中 G 为 N 的

最大真因子. 当 $1 = k < m$ 时，$WC_2(u^\infty) \geq (2^m - 1)(2^n - 1) - G - n(m+1)$；当 $2 \leq k < m$ 时，$WC_2(u^\infty) \geq (2^m - 1)(2^n - 1) - G - n\sum_{i=0}^{k} C_m^i$；当 $k = m$ 时，$WC_2(u^\infty) \geq (2^m - 1)(2^n - 1) - G - n(2^m - 1)$.

证 $w^\infty(x) = \dfrac{x^i + x^j}{1 + x^N} = \dfrac{x^i(1 + x^{j-i})}{1 + x^N} = \dfrac{\dfrac{x^i + x^j}{1 + x^G}}{\dfrac{1 + x^N}{1 + x^G}}$

$= \dfrac{r_w}{f_w}$，$G = \gcd(j - i, N)$. $r_w = \dfrac{x^i + x^j}{1 + x^G}$；$f_w = \dfrac{1 + x^N}{1 + x^G}$.

由周期定义知，f_u 整除 $1 + x^N$，f_u 不整除 $1 + x^G$，所以 f_u 整除 f_w. 设 $h(x)$ 为 $\gcd(f_w, r_u + \dfrac{f_w r_u}{f_u})$ 的一不可约因子，则 $h(x)$ 整除 $f_w(x)$；$h(x)$ 整除 $r_w + \dfrac{f_w r_u}{f_u}$. 若 $h(x) \neq f_u(x)$，则 $h(x)$ 整除 $\dfrac{f_w r_u}{f_u}$，所以 $h(x)$ 整除 $r_w(x)$. 又因 $\gcd(r_w, f_w) = 1$，所以 $h(x) = 1$ 且 $\gcd(f_w, r_u + \dfrac{f_w r_u}{f_u})$ 为 $f_u(x)$ 的整数幂. 因 $\gcd(x^N, Nx^{N-1}) = 1$，故 $1 - x^N$ 无重因子，进而 $r_w(x)$ 也无重因子，所以 $\gcd(f_w, r_u + \dfrac{f_w r_u}{f_u}) = f_u(x)$.

$$WC_2(u^\infty) = \min_{0 \leq i \leq N-1} \deg\left\{\frac{f_u f_w}{\gcd(f_u f_w, f_u r_w + f_w r_u)}\right\} = \min_{0 \leq i \leq N-1} \deg\left\{\frac{f_w}{\gcd(f_w, r_w + \frac{f_w r_u}{f_u})}\right\} = \min_{0 \leq i \leq N-1} \deg\left\{\frac{1 + x^N}{f_u(1 + x^G)}\right\}$$

$\geq N - G - \deg(u^\infty)$.

4　结束语

我们得到的 Jennings 复合序列的周期是指数级[6]的，这就使得该序列很难预测，从而安全性能好. 另一方面，Jennings 复合序列的线性复杂度的数值也是较高的，但这并不能说明序列就不易猜测. 我们往往在改变序列的几个比特时，其线性复杂度变动很大，序列不稳定. 我们又求得了它的 1 - 重量复杂度和 2 - 重量复杂度的下界，从结果来看，序列有很好的稳定性，可见 Jennings 复合序列有较强的密码学意义.

参考文献：

[1] 胡玉濮，张玉清，肖国镇. 对称密码学[M]. 北京：机械工业出版社，2002.

[2] 丁存生，肖国镇. 流密码学及其应用[M]. 北京：国防工业出版社，1994.

[3] HUNGERFORD T W. 代数学[M]. 冯克勤，译. 长沙：湖南教育出版社，1986.

[4] LIDL R, NIEDERREITER H. Finite Fields[M]. Boston: Addison-Wesley Publishing Company, 1983.

[5] LIU Mu-lan, WAN Zhe-xian. Generalized multipled sequences[J]. Advance in Cryptology, LNCS, 1986: 135 - 141.

[6] 王锦玲，毕文斌. 三元树上的线性递归序列[J]. 郑州大学学报(工学版)，2006，27(2)：110 - 112.

Some Annotations about the Multipled Jennings Sequences

WANG Jin - ling, LEI Yu - yin, YANG Na, WANG Jing

(Department of Mathematics, Zhengzhou University, Zhengzhou 450001, China)

Abstract: The paper presents a series of vectors, discusses the definitions about the multipled Jennings sequences by giving the values to the vectors. Some reductions and complementaries on the period and the linear complexity of the proofs of the theory are also given. In order to measure the stability of the sequence, this paper introduces the weighty complexity $WC_k(u^\infty)$ and gets the lower limit when k is one and two, which is $(2^m - 1)(2^n - 1) - n(m+1)$ when $1 = k < m$; $(2^m - 1)(2^n - 1) - n\sum_{i=0}^{k} C_m^i$ when $2 \leq k < m$; $(2^m - 1)(2^n - 1) - n(2^m - 1)$ when $k = m$. The case is the same when k is two. The stability of the linear complexity of the sequences is analysised.

Key words: period; linear complexity; lexity; characteristic polynomial; multipled sequence; weight complexity