m 序列扩展及一类 M 序列快速生成*

林须端　　蔡长年

(北京邮电学院电信工程系,北京 100088)

关键词　伪随机序列、线性复杂度、序列密码、信息技术

由于m序列数量少、线性复杂度小[1],不能满足保密通信等需要. M 序列虽已得到了深入研究[1-6],但许多产生M序列的算法因需要大量存储空间或计算时间而不实用,对 $k>2$,仅有两个产生 k 进M序列的有效算法[1,6]. 设U为 $GF(q^m)$ 上周期为 $q^{mn}-1$ 的序列全体, PN 是U中的m序列集. U的子集 R、S、C 分别满足游程特性、窗特性和二值自相关特性. 本文扩展了 $GF(q^m)$ 上的m序列[7], 在$q>2$或$m>2$时得出了 $S\cap C\neq PN$ 及 $R\cap C\neq PN$ 的结论, 因而 Golomb 在 $GF(2)$ 上 $S\cap C=PN$ 和 $R\cap C=PN$ 的猜想[8]在 $GF(q^m)$ 上不成立.本文还提出产生一类M序列快速算法.

一、m 序列的扩展

设 $Tr_m^{mn}(x)=\sum_{j=0}^{n-1}x^{q^{mj}}$ 为从有限域 $GF(q^{mn})$ 到 $GF(q^m)$ 上的迹映射,$\{a_i\}$为 $GF(q^m)$ 上 n 次多项式 $f(x)$ 产生的m序列, γ 为 $f(x)$ 的根,则有 $\theta\in GF(q^{mn})^*$ 使 $a_i=Tr_m^{mn}(\theta\gamma^i)$, $i=0,1,2,\cdots$. 令 $e_0,e_1,\cdots,e_{m-1}$ 为 $GF(q^m)$ 在 $GF(q)$ 上的一组基, $a_i=\sum_{j=0}^{m-1}b_{ij}e_j$, $i=0,1,2,\cdots$, $b_{ij}\in GF(q)$, 设 $h_0,h_1,\cdots,h_{m-1}$ 为 $e_0,e_1,\cdots,e_{m-1}$ 的对偶基[7], 则有 $b_{ij}=Tr_1^{mn}(\theta h_j\gamma^i)$, $i=0,1,2,\cdots,j=0,1,\cdots,m-1$. 对 $GF(q^m)$ 在 $GF(q)$ 上的基 $e'_0,e'_1,\cdots,e'_{m-1}$, 构造序列 $\{a'_i\}$: $a'_i=\sum_{j=0}^{m-1}b_{ij}e'_j$, $i=0,1,2,\cdots$.

定理 1　序列 $\{a'_i\}$ 的周期为 $q^{mn}-1$, 在 $\{a'_i\}$ 的一个周期中 $GF(q^m)$ 上每个 n 长非零状态恰好出现一次.

证　在m序列 $\{a_i\}$ 的一个周期中, $GF(q^m)$ 上每个 n 长非零状态出现一次, 故阵列 $(b_{ij})_{i=0,1,\cdots,q^{mn}-2;j=0,1,\cdots,m-1}$ 具有 $n\times m$ 纵向窗特性, 在基 $e'_0,e'_1,\cdots,e'_{m-1}$ 表示下, 每个 $n\times m$ 窗对应一个 n 长状态,由此证得定理.

称满足定理 1 的序列具有窗特性,并以 S 记U中具有窗特性的序列集. 由定理 1 易得:

推论 1　在 $\{a'_i\}$ 的一个周期中, $GF(q^m)^*$ 中每个ω元出现 $q^{m(n-1)}$ 次, 0 元出现 $q^{m(n-1)}-1$ 次.

推论 2　在 $\{a'_i\}$ 的一个周期中, $1\leqslant i\leqslant n-2$ 时, 对 $\omega\in GF(q^m)$, i 长ω游程有 $q^{m(n-i-2)}(q^m-1)^2$ 个, $n-1$ 长 0 游程 q^m-1 个, $n-1$ 长非零ω游程 q^m-2 个, n长非零ω游程 1 个. U中满足推论 2 游程特性的序列类记为 R. 当 $q=p$ 为素数时,设 $e''_0,e''_1,\cdots,e''_{m-1}$ 为 $GF(q^m)$ 在 $GF(q)$ 上的一组基, $a'_i=\sum_{j=0}^{m-1}b'_{ij}e''_j$, $b'_{ij}\in GF(q)$, 令 $d_i=(b'_{i0},b'_{i1},$

本文 1989 年 11 月 21 日收到. 1990 年 2 月 10 日收到修改稿.

* 国家教育委员会高等学校科学技术基金资助项目.

$\cdots, b'_{i_{m-1}}), \theta_m(d_i) = (\theta_1(b'_{i_0}), \theta_1(b'_{i_1}), \cdots, \theta_1(b'_{i_{m-1}}))$，其中 $\theta_1(b'_{i_k}) = \exp(2\pi j b'_{i_k}/p)$，$\{a'_i\}$ 的复共轭 θ_m 的自相关函数定义为 $R_{\{a'_i\}}(\tau) = \sum_{i=0}^{q^{mn}-2} \theta_m(d_i)([\theta_m(d_{i+\tau})]^*)^T$，其中 $[V]^*$ 为 V 关于映射，$(V)^T$ 为 V 的转置.

定理 2 序列 $\{a'_i\}$ 关于映射 θ_m 的自相关函数为二值：$R_{\{a'_i\}}(\tau) = -m$，当 $\tau \neq 0 \bmod(q^{mn}-1)$；$R_{\{a'_i\}}(\tau) = m(q^{mn}-1)$，当 $\tau \equiv 0 \bmod(q^{mn}-1)$.

证 设 $e'_i = \sum_{k=0}^{m-1} y_{ik} e''_k$，$h''_k = \sum_{j=0}^{m-1} y_{ik} h_j$，则 $a'_i = \sum_{k=0}^{m-1} Tr_1^{mn}(\theta h''_k \gamma^i) e''_k$，故 $b'_{ik} = Tr_1^{mn}(\theta h''_k \gamma^i)$，$i = 0, 1, 2, \cdots, k = 0, 1, \cdots, m-1$，$R_{\{a'_i\}}(\tau) = \sum_{k=0}^{m-1} \sum_{i=0}^{q^{mn}-2} \exp\{2\pi j Tr_1^{mn}[\theta h''_k \gamma^i (1-\gamma_\tau)]/p\}$，由此证得定理 2.

对 q 不是素数时，用分量序列表示可得类似的二值自相关函数. U 中满足自相关函数为二值的序列类记为 C，令 $T = \dfrac{q^{mn}-1}{q^m-1}$，$\eta = \gamma^T$.

定理 3 由 $GF(q^m)$ 在 $GF(q)$ 上不同基 $e'_0, e'_1, \cdots, e'_{m-1}$ 及 $GF(q^{mn})$ 的不同本原元 γ 构造的序列 $a'_i = \sum_{j=0}^{m-1} Tr_1^{mn}(\theta h_j \gamma^i) e'_{ij}$，$i = 0, 1, 2, \cdots$，中，平移不等价序列数目为 $\dfrac{1}{mn}\varphi(q^{mn}-1)\prod_{j=1}^{m-1}(q^m - q^j)$，其中 φ 为欧拉函数.

证 设 $e'_0, \cdots, e'_{m-1}$ 与 $e''_0, \cdots, e''_{m-1}$ 为两组基，$e''_j = \sum_{k=0}^{m-1} z_{jk} e'_k$，$j = 0, 1, \cdots, m-1$，令 $h''_k = \sum_{j=0}^{m-1} z_{jk} h_j, k = 0, 1, \cdots, m-1, \gamma, \gamma^s$ 为两本原元，$a'_i = \sum_{j=0}^{m-1} Tr_1^{mn}(\theta h_j \gamma^i) e'_j$，$a''_i = \sum_{j=0}^{m-1} Tr_1^{mn}(\theta h_j \gamma^{si}) e''_j$，$i = 0, 1, 2, \cdots$. 若有 $\tau \in Z_{q^{mn}-1}$，使 $a'_i = a''_{i+\tau}$，$i = 0, 1, 2, \cdots$，取 $\theta = 1$，由 $a''_i = \sum_{k=0}^{m-1} Tr_1^{mn}(h''_k \gamma^{si}) e'_k$ 得 $Tr_1^{mn}(h_j \gamma^i) = Tr_1^{mn}(h''_i \gamma^{s(i+\tau)})$，$i = 0, 1, 2, \cdots, j = 0, 1, \cdots, m-1$. 因此 $s \equiv q^r \bmod(q^{mn}-1)$，$r \in Z_{mn}$ 且 $h''_i = h_i^{q^r} \gamma^{-s\tau}$，故 $\{a'_i\}$ 与 $\{a''_i\}$ 平移等价当且仅当 $s \equiv q^r \bmod(q^{mn}-1)$ 且 $h''_i = \eta^l h_i^{q^r}, j = 0, 1, \cdots, m-1, l, r$ 为整数. 对 $l \in Z_{q^m-1}$，$r \in Z_m$，形式基 $\eta^l h_0^{q^r}, \eta^l h_1^{q^r}, \cdots, \eta^l h_{m-1}^{q^r}$ 均不同，而 $GF(q^m)$ 在 $GF(q)$ 上不同基数目为 $\prod_{j=0}^{m-1}(q^m - q^j)$，由此得平移不等价序列数目.

新序列类是 m 序列的扩展. Golomb 在 $m = 1$，$q = 2$ 时提出猜想[8]：(1) $R \cap C = PN$；(2) $S \cap C = PN$. 随后 Cheng 和 Golomb 得出在 $GF(2)$ 上 $R \cap C \neq PN$[9]. 上述结果可得出：当 $q > 2$ 或 $m > 2$ 时，(1) $R \cap C \neq PN$；(2) $S \cap C \neq PN$. $\{a'_i\}$ 满足移位相加特性.

二、一类 M 序列的快速产生

令 $nq > 2$ 或 $m > 3$，$a^T = a_0, a_1, \cdots, a_{T-1}$，则 $\{a_i\}$ 可表示为 $\eta^0 a^T, \eta^1 a^T, \cdots \eta^{q^{m-2}} a^T, \cdots$，故 $\{a_i\}$ 的 0 元分布与 $\{a_i\}$ 一样且 $n-1$ 长 0 游程等间隔分布. 令 $a'(k) = a'_{kT}, a'_{kT+1},$

$\cdots, a_{kT+T-1}$，取θ使 $a'_0 = a'_1 = \cdots = a'_{n-2} = 0$，由 $\{a'_i\}$ 的窗特性得

定理4 设P为 Z_{q^m-1} 上的置换，则周期序列 $\{c_i\} = a'(P(0)), a'(P(1)), \cdots, a'(P(q^m - 2)), \cdots$，具有窗特性。

定理5 当P为非循环置换时，$\{a'_i\}$ 经P置换所得序列 $\{c_i\}$ 的线性复杂度不小于 $T + n - mn > mn$。

证 由广义移位相加特性[10]知：$\{a'_i\}$的线性复杂度不大于 mn，因存在k，使 $a'(P(k))\cdot a'(P(k+1))$ 不出现在 $\{a'_i\}$ 中，由复杂度改变特性[10]，$\{c_i\}$ 的线性复杂度不小于 $T + n - mn > mn$。令 $e_0, e_1, \cdots, e_{m-1}$ 与 $1, \eta, \cdots, \eta^{m-1}$ 为共轭基，X为 $GF(q)$ 上m阶非奇异矩阵，$f(x)$为 $GF(q^m)$ 上n次本原多项式，我们的算法如下：

1) 初值：$X, f(x), I_0 \in Z_{q^m-1}$，置换 P。

2) 计算 $(e'_0, e'_1, \cdots, e'_{m-1}) = (e_0, e_1, \cdots, e_{m-1})X$。

3) 对 $I = 0, 1, \cdots, q^m - 2$，进行下列步骤：i) 当 $I = I_0$ 时，插入一个输出值 0；ii) 将 $f(x)$ 对应的移存器赋初态 $(0, 0, \cdots, \eta^{P(I)})$；iii) 对 $i = 0, 1, \cdots, T-1$，移存器产生 a_i 并计算 $a'_i = \sum_{j=0}^{m-1} Tr_1^m(a_i\eta^j)e'_j$，输出 a'_i。

4) 输出序列为 $\{c'_i\}$。

$\{c'_i\}$ 是 $GF(q^m)$ 上周期为 q^{mn} 的M序列，迹映射是向量空间的线性变换，由移存器的递归运算及前面分析知，上述算法是一个产生一类M序列的有效快速算法。

定理6 上述算法能产生 $\frac{1}{mn}\varphi(q^{mn}-1)(q^m-1)!\prod_{j=1}^{m-1}(q^m - q^j)$ 个 $GF(q^m)$ 上周期为 q^{mn} 的不平移等价M序列。

证 $\{a'_i\}$ 经 P_1 置换和经 P_2 置换的序列平移等价当且仅当 $P_1 = P_2P$，其中P为循环置换。对两不同序列 $\{a'_i\}$、$\{a''_i\}$，若有 $a'(P_1(i)) = a''(P_2(i+k))$，$i \in Z_{q^m-1}$，则有置换$P$使 $a'(P(i)) = a''(i+k)$，$i \in Z_{q^m-1}$，由 $\{a'_i\}$、$\}a''_i\}$ 不平移等价及定理5知这是不可能的，所以 $\{a'_i\}$ 经 P_1 置换与 $\{a''_i\}$ 经 P_2 置换所得序列不平移等价。因而上述算法产生

$$\frac{1}{mn}\varphi(q^{mn}-1)\left[\prod_{j=1}^{m-1}(q^m - q^j)\right](q^m-1)(q^m-1)!/(q^m-1)$$

个不同M序列。

设 P' 为 $GF(q^m)$ 的置换，则 $\{P'(c'_i)\}$ 仍是M序列。在序列密码中，适当选择 P' 及算法中的初值作种子密钥，则序列 $\{P'(c'_i)\}$ 可作为加密的序列密钥。

参 考 文 献

[1] Fredricksen, H. M., *SIAM Review*, 24(1982), 195—221.
[2] 高鸿勋，应用数学学报，2(1979)，316—324.
[3] 高鸿勋，科学通报，27(1982)，1226- 1228.
[4] 万哲先、戴宗铎、刘木兰、冯绪宁，非线性移位寄存器，科学出版社，1978.
[5] 康庆德，应用数学学报，7(1984)，78—85.
[6] Etzion, T., *J. Algorithms*, 7(1986), 331—340.
[7] Lidl, R. and Niedereiter, H., *Finite Fields*, Addson-Wesley Publishing Company, 1983.
[8] Golomb, S. W., *IEEE Trans.*, IT-26(1980), 730—732.
[9] Cheng, U. and Golomb, S. W., *IEEE Trans.*, IT-29(1983), 600.
[10] Massey, J. L. and Schaub, T., *Lecture Notes in Computer Sciences*, No. 311, Springer-Verlag, 1988. 19 -32.