一种由移位数列生成 GMW 序列和级联 GMW 序列的新算法 [1]

严春林 周 亮 李少谦

(电子科技大学通信抗干扰国防重点实验室 成都 610054)

摘 要 该文提出了一种新的根据移位数列生成 GMW 序列和级联 GMW 序列的构造方法，该方法简化了传统的 GMW 序列和级联 GMW 序列的构造方法，大大提高了生成效率，且验证了其可行性。

关键词 移位数列，m 序列，GMW 序列，级联 GMW 序列

中图号 TN914.4

1 引 言

具有两值自相关的伪随机序列广泛用于通信和密码系统，如用于通信信号同步、信号检测、雷达测距，及用于无线通信网络和流密码中。m 序列，GMW 序列 [1] 和级联 GMW[2,3] 序列都满足两值自相关，故有重要的使用价值。但 m 序列因为是线性序列，其线性复杂度很小，很难满足实际系统安全性的要求。GMW 序列和级联 GMW 是非线性伪随机序列，它们的线性复杂度和移位不等价序列个数比相同长度的 m 序列大得多，故研究 GMW 序列和级联 GMW 的简洁、快速生成算法有重要的应用价值。

在几乎所有文献中，GMW 序列和级联 GMW 序列都是用迹函数来定义和生成的，生成过程复杂，需进行不低于两次的迹函数映射且需非线性变换。我们发现可通过先生成 m 序列以生成所需的移位数列 [4]，再通过移位数列来生成 GMW 序列和级联 GMW 序列算法，其生成方法简洁，无需迹函数和复杂的迹函数映射计算。利用此算法，我们只需生成一个 m 序列，就可以生成所有这种长度的移位不等价的 GMW 序列和级联 GMW 序列。

2 移位数列的定义

设 α 为 GF(2^m) 上的本原元，整数 $n|m$, $T=(2^m-1)/(2^n-1)$, $0\le k<2^n$, $0\le j<T$，则 m 序列 $a(i)$ 在 2 元域上的迹函数 [5] 描述为

$$a(i)=\mathrm{tr}_1^m(\alpha^i)=\sum_{t=0}^{m-1}(\alpha^i)^{2^t},\ i=1,2,3,\cdots,2^m-1 \tag{1}$$

$$a(i)=\mathrm{tr}_1^m(\alpha^i)=\mathrm{tr}_1^m(\alpha^{kT+j})=\mathrm{tr}_1^n[\mathrm{tr}_n^m(\alpha^{kT+j})] \tag{2}$$

上式中，$\mathrm{tr}_1^m(\cdot)$ 是 $\mathrm{tr}_{2^1}^{2^m}(\cdot)$ 的简写，$\mathrm{tr}_n^m(\cdot)$ 是 $\mathrm{tr}_{2^n}^{2^m}(\cdot)$ 的简写。由于 α^T 的级为 $(2^m-1)/(T,2^m-1)=2^n-1$，故 $\alpha^T\in$ GF(2^n) 且为其上的本原元 [5]。利用迹函数性质有

$$a(i)=\mathrm{tr}_1^n[\mathrm{tr}_n^m(\alpha^{kT+j})]=\mathrm{tr}_1^n[\alpha^{kT}\mathrm{tr}_n^m(\alpha^j)] \tag{3}$$

定义 m 序列的移位数列 e_j, $0\le j<T$ 为

$$e_j=\begin{cases}\infty, & \mathrm{tr}_n^m(\alpha^j)=0\\ k, & \mathrm{tr}_n^m(\alpha^j)=\beta^k\end{cases} \tag{4}$$

[1] 2001-11-30 收到，2002-10-18 改回

其中 $\beta=\alpha^T$, 于是 m 序列 $a(i)$ 可用移位数列表示为

$$a(i)=\mathrm{tr}_1^n[\mathrm{tr}_n^m(\alpha^{kT+j})]=\mathrm{tr}_1^n[\alpha^{kT}\mathrm{tr}_n^m(\alpha^j)]=\mathrm{tr}_1^n(\beta^{k+e_j}) \tag{5}$$

其中 $0\le k<2^n-1$ 。

由于迹函数 $\mathrm{tr}_1^n(\beta^i)$, $0\le i<2^n-1$, 表示一长为 2^n-1 的 m 序列，故将长为 2^m-1 的 m 序列排成 2^n-1 行 T 列的阵列，除 $e_j=\infty$ 的那一列为全零列外，其余各列为不同初始相位的同一 m 序列。

GMW 序列 $b(i)$ 可用迹函数描述为

$$b(i)=\mathrm{tr}_1^n\{[\mathrm{tr}_n^m(\alpha^i)]^I\} \tag{6}$$

其中 $0<I<2^n-1$, $\gcd(I,2^n-1)=1$, $\alpha\in\mathrm{GF}(2^m)$ 且为其上的本原元。定义 $\gamma=\alpha^{TI}$, $T=(2^m-1)/(2^n-1)$, 则 $\gamma\in\mathrm{GF}(2^n)$ 且为其上的本原元。GMW 序列的移位数列 e_j, $0\le j<T$ 为

$$e_j=\begin{cases}\infty, & [\mathrm{tr}_n^m(\alpha^j)]^I=0\\ k, & [\mathrm{tr}_n^m(\alpha^j)]^I=\gamma^k\end{cases} \tag{7}$$

上式中 $0\le k<2^n-1$ 。

对 (4) 式进行变形，等式两边取 I 的幂，有

$$e_j=\begin{cases}\infty, & [\mathrm{tr}_n^m(\alpha^j)]^I=0\\ k, & [\mathrm{tr}_n^m(\alpha^j)]^I=\beta^{Ik}=\alpha^{TIk}=\gamma^k\end{cases} \tag{8}$$

由于 $0<I<2^n-1$, $\gcd(I,2^n-1)=1$, 故在域 $\mathrm{GF}(2^n)$ 上存在元素 I 的逆，设 I 的逆为 I^{-1}, 对 (7) 式两边取 I^{-1} 的幂，有

$$e_j=\begin{cases}\infty, & ([\mathrm{tr}_n^m(\alpha^j)]^I)^{I^{-1}}=\mathrm{tr}_n^m(\alpha^j)=0\\ k, & ([\mathrm{tr}_n^m(\alpha^j)]^I)^{I^{-1}}=\mathrm{tr}_n^m(\alpha^j)=(\gamma^k)^{I^{-1}}=(\alpha^{ITk})^{I^{-1}}=\alpha^{Tk}=\beta^k\end{cases} \tag{9}$$

将 (8) 式和 (7) 式进行比较，(9) 式和 (4) 式进行比较。可知，若生成 m 序列和 GMW 序列的扩域 $\mathrm{GF}(2^m)$ 由同一本原多项式在基域 $\mathrm{GF}(2)$ 上构造，则由 m 序列所得到的移位数列 $\{e_j\}$ 与 GMW 序列所得到的移位数列 $\{e_j\}$ 相同。此结论是本文的理论基础。

GMW 序列也可用移位数列表示为

$$\begin{aligned}b(i)&=\mathrm{tr}_1^n\{[\mathrm{tr}_n^m(\alpha^i)]^I\}=\mathrm{tr}_1^n\{[\mathrm{tr}_n^m(\alpha^{kT+j})]^I\}\\&=\mathrm{tr}_1^n\{[\alpha^{kT}\mathrm{tr}_n^m(\alpha^j)]^I\}=\mathrm{tr}_1^n(\gamma^{k+e_j})\end{aligned} \tag{10}$$

3 使用移位数列生成 GMW 序列和级联 GMW 序列的算法

由以上 GMW 序列和 m 序列的移位数列的表示形式可得如下结果：

(1) 设 $\alpha\in\mathrm{GF}(2^m)$ 且为其上的本原元，$\beta=\alpha^T$, $\beta\in\mathrm{GF}(2^n)$ 且为其上的本原元。则 $a_1(l)=\mathrm{tr}_1^n(\beta^l)$, $0\le l<2^n-1$, 表示长为 2^n-1 的 m 序列；而 $a_2(i)=\mathrm{tr}_1^n(\beta^{k+e_j})$, $0\le k<2^n-1$, $0\le j<T$, $i=j+kT$, 表示长为 2^m-1 的 m 序列。将 $a_2(i)$ 排成 2^n-1 行 T 列的阵列，可以发现，除 $e_j=\infty$ 的那一列外，其余列都为长为 2^n-1 的不同初始相位的同一 m 序列 $a_1(l)$ ；

(2) $b(i)=\mathrm{tr}_1^n[(\gamma)^{k+e_j}]$, $0\le k<2^n-1$, $0\le j<T$, $i=j+kT$, 表示长为 2^m-1 的 GMW 序列，且其结果等价根据迹函数 $\mathrm{tr}_1^n\{[\mathrm{tr}_n^m(\alpha^i)]^I\}$ 求得的结果。这里 $\alpha\in\mathrm{GF}(2^m)$ 且为其上的本

原元，$\gamma=\alpha^{TI}$。将 $b(i)$ 排成 2^n-1 行 T 列的阵列，可以发现，除 $e_j=\infty$ 的那一列外，其余列都为一长为 2^n-1 的 m 序列。当 $I=1$ 时，$b(i)$ 等同于 (1) 中的 $a_2(i)$，为一长为 2^m-1 的 m 序列；当 $I\neq 1$ 时，且 $0<I<2^n-1$, $\gcd(I,2^n-1)=1$, $b(i)$ 为一长为 2^m-1 的 GMW 序列；

(3) 序列 $a(i)$ 和 $b(i)$ 的移位数列 $\{e_j\}(0\le j<T)$ 相同 (当生成 m 序列和 GMW 序列的扩域 $\mathrm{GF}(2^m)$ 由同一本原多项式在基域 GF(2) 上构造时)。

级联 GMW 序列可用迹函数描述为 [2]

$$c(i)=\mathrm{tr}_1^{J_1}\{\mathrm{tr}_{J_1}^{J_2}(\cdots(\mathrm{tr}_{J_{N-1}}^{m}(\alpha^i))^{r_{N-1}}\cdots)^{r_1}\} \tag{11}$$

其中 $0<r_i<2^{J_i-1}-1$, $\gcd(r_i,2^{J_i-1}-1)=1$, $m=M_1M_2\cdots M_{N-1}$, $J_i=M_1M_2\cdots M_i$, $0\le i\le N$, M_i 为正整数，$\alpha\in\mathrm{GF}(2^m)$ 且为其上的本原元。

根据迹函数公式 $\mathrm{tr}_1^n(\gamma^{i+e_j})$ 能生成 GMW 序列，GMW 序列又可写为 $\mathrm{tr}_1^n\{[\mathrm{tr}_n^m(\alpha^i)]^I\}$，其中 $0<I<2^J-1$, $\gcd(I,2^J-1)=1$。若将 $\mathrm{tr}_1^n(\gamma^{i+e_j})$ 等价表示为 $\mathrm{tr}_1^J\{[\mathrm{tr}_J^n(\gamma^{i+e_j})]^{I_1}\}$, $0<I_1<2^J-1$, $\gcd(I_1,2^J-1)=1$，则 $\mathrm{tr}_1^J\{[\mathrm{tr}_J^n(\gamma^{i+e_j})]^{I_1}\}$ 可等价表示为 $\mathrm{tr}_1^J\{[\mathrm{tr}_J^n(\mathrm{tr}_n^m(\alpha^i)^I)]^{I_1}\}$。而根据级联 GMW 序列的定义，$\mathrm{tr}_1^J\{[\mathrm{tr}_J^n(\mathrm{tr}_n^m(\alpha^i)^I)]^{I_1}\}$ 即为级联 GMW 序列。故我们可用除原始定义以外的另一种方法来生成级联 GMW 序列。

GMW 序列和级联 GMW 序列的生成算法：

(1) 根据 (4) 式求出 e_j, $0\le j<T=(2^m-1)/(2^n-1)$。e_j 也可通过将长为 2^m-1 的 m 序列排成 2^n-1 行 T 列的阵列，必有一列全零列，对应此列的 $e_j=\infty$。其余任意列为同一 m 序列的不同初始相位。任取一非零列作为参考列，对应此列的 $e_j=0$。其余各列的 e_j 值等于该列的 m 序列的初始相位值减去参考列 m 序列的初始相位值。移位数列是一个差集，它与每个元素的绝对值无关，与其相对值有关。

(2) 求出所有长为 2^n-1 的 m 序列，将其存放到数组 $a_1[l]$, $l=0,1,\cdots,2^n-2$。

(3) 根据公式 $a[k]=a_I[(i+e_j)\bmod(2^n-1)]$, $0\le i<2^n-1$, $0\le j<T$, $k=iT+j$，当 $e_j=\infty$ 时，对应的 $a(im+j)=0$，则数组 $a[k]$ 中为一长为 2^m-1 的 GMW 序列。

(4) 改变长为 2^n-1 或 2^m-1 的 m 序列可得移位不等价的另一 GMW 序列。

为避免使用迹函数理论进行计算，可使用带线性反馈的移位寄存器，通过递归计算产生 m 序列。

如果已生成一长为 2^m-1 的 m 序列，通过对此序列进行抽样，可生成所有这种长度的 m 序列 [6]。它们移位不等价，个数为 $\Phi(2^m-1)/m$, $\Phi(\cdot)$ 为欧拉函数。算法步骤 2 中所有长为 2^n-1 的 m 序列 $a_1(l)$ 的生成：在算法步骤 1 中我们已得到一个长为 2^n-1 的 m 序列，对此序列进行抽样，可生成所有 $\Phi(2^n-1)/n$ 个移位不等价的 m 序列 [6]。故共可生成 $[\Phi(2^m-1)/m]\cdot\Phi(2^n-1)/n$ 个长为 2^m-1 移位不等价的 GMW 序列。

级联 GMW 序列生成方法同 GMW 序列，只需将第 (2) 步的 m 序列改为 GMW 序列即可。当级联 GMW 序列表达式为 (11) 式时，移位不等价级联 GMW 序列的个数为 $[\Phi(2^m-1)]\times[\Phi(2^{J_{N-1}}-1)]\cdots[\Phi(2^{J_1}-1)]$。

我们是在二元域中讨论 GMW 和级联 GMW 序列的生成的，实际上，以上算法可以推广到多元域，生成多元域上的 GMW 序列和级联 GMW 序列。

4 生成实例及验证

实例 1 长为 4095 的 GMW 序列的生成

生成长为 $2^{12}-1=4095$ 的 m 序列，当本原多项式为 $x^{12}+x^7+x^4+x^3+1=0$ 时，可求出移位数列 $e_j=\{\infty,1,2,8,4,29,16,52,8,46,58,49,32,17,41,22,16,18,29,44,53,27,35,13,1,4,34,51,19,23,44,3,32,1,36,15,58,55,25,9,43,41,54,14,7,34,26,12,2,1,8,28,5,21,39,49,38,1,46,11,$

$25,1,6,1,1\}$ 。

生成长为 $2^6-1=63$ 的 m 序列

011111101011100011001110110000011110010010101001101000010001011

可求出长为 4095 的一个 GMW 序列，其自相关最大值为 4095，其余值皆为 -1 。此序列线性复杂度为 24(由梅西算法 [6] 求得)，0 的个数为 2047，1 的个数为 2048，序列 0-1 平衡。

依此类推可生成其它长度为 2^m-1 的 GMW 序列。

实例 2　长为 4095 的级联 GMW 序列的生成

生成长为 $2^6-1=63$ 的 GMW 序列。

000001010010011101011101001011100011001111110010010111001110100

可求出长为 4095 的级联 GMW 序列，其自相关最大值为 4095，其余值皆为 -1 。此序列线性复杂度为 144(由梅西算法求得)，0 的个数为 2047，1 的个数为 2048，序列 0-1 平衡。

依此类推可生成其它长度为 2^m-1 的级联 GMW 序列。

5 结 束 语

本文讨论了通过生成长为 2^m-1 的 m 序列，生成所需移位数列，来生成长为 2^m-1 的 GMW 序列或级联 GMW 序列的算法。并验证了其可行性，从而提供了生成长为 2^m-1 的 GMW 序列或级联 GMW 序列的一种新算法。该算法较传统的根据迹函数定义生成 GMW 序列和级联 GMW 序列的计算方法简便，且具有相同的可靠性。

此处，我们是在二元域上讨论 GMW 序列和级联 GMW 序列的生成，该算法也可用于生成多元域上 GMW 序列和级联 GMW 序列。

参 考 文 献

[1] R. A. Scholtz, L. R. Welch, GMW sequence, IEEE Trans. on IT, 1984, IT-30(3), 548–553.

[2] 李世鹏，朱近康，一类新的性能优越的伪随机序列，电子学报，1993, 21(1), 41–51.

[3] A. Klapper, *et al.*, Cascaded GMW sequence, IEEE Trans. on IT, 1993, IT-39(1), 177–183.

[4] GongGuang, Theory and application of q-ary interleaved sequences, IEEE Trans. on IT, 1995, IT-41(2), 400–410.

[5] 王新梅，肖国镇，纠错码——原理与方法，西安，西安电子科技大学出版社，2001 年 4 月修订版，139–141, 117–117.

[6] 肖国镇，梁传甲，王育民，伪随机序列及其应用，北京，国防工业出版社，1985 年 3 月第 1 版，99–100, 102–103.

A NEW ALGORITHM TO CONSTRUCT GMW SEQUENCES AND CASCADED GMW SEQUENCES BY SHIFT SEQUENCES

Yan Chunlin　　Zhou Liang　　Li Shaoqian

(*The National Communication Lab, UEST of China, Chengdu* 610054, *China*)

Abstract　In this paper, a new algorithm to construct GMW sequences and cascaded GMW sequences by shift sequences is proposed. This algorithm simplifies the conventional algorithm to construct GMW sequences and cascaded GMW sequences, significantly improves the efficiency, and the feasibility of this algorithm is verified.

Key words　Shift sequences, m sequences, GMW sequences, Cascaded GMW sequences

严春林：　男，1976 年生，博士生，从事序列设计，OFDM 同步方面的研究.

周　亮：　男，1961 年生，副教授，从事密码学和编码理论的研究.

李少谦：　男，1957 年生，教授，博士生导师，从事移动通信、个人通信、扩频通信、抗干扰通信研究.