一种快速构造具有最大线性复杂度 GMW 序列的方法

陈嘉兴[1], 周廷显[1], 许成谦[2]
(1. 哈尔滨工业大学通信技术研究所, 黑龙江哈尔滨 150001; 2. 燕山大学信息科学与工程学院, 河北秦皇岛 066004)

摘 要: 本文研究了计算 GMW 序列线性复杂度的算法, 在此基础上对其进行了简化, 得到了一种方法, 来快速构造给定周期长度的 GMW 序列, 使其具有最大线性复杂度. 利用此方法工程人员可以无须掌握太多数学知识而很快捷的得到理想的 GMW 序列并将之应用到扩频多址通信系统中, 从而使整个系统具有最佳性能.

关键词: Gordon-Mills-Welch (GMW) 序列; 迹函数; 线性复杂度
中图分类号: TN914 文献标识码: A 文章编号: 0372-2112 (2005) 05-0857-03

A Fast Method for Constructing GMW Sequences with Largest Linear Spans

CHEN Jia-xing[1], ZHOU Ting-xian[1], XU Cheng-qian[2]
(1. *Communication Research Center, Harbin Institute of Technology, Harbin, Heilongjiang 150001, China;*
2. *College of Info. Sci. & Engine., Yanshan University, Qinhuangdao, Hebei 066004, China*)

Abstract: An algorithm for computing the linear spans of GMW sequences was studied and simplified in this paper. Then we get a new method which can obtain GMW sequences with largest linear spans for a certain periods. Using this method, engineers can get ideal GMW sequences in a short time without mastering much mathematic knowledge. These sequences can make the spread spectrum multiple access communication systems have optimal performance.

Key words: Gordon-Mills-Welch (GMW) sequences; trace function; linear span

1 引言

扩频通信由于其具有保密性和抗干扰能力, 所以不仅在军事通信中获得了成功应用, 而且越来越广泛的应用到民用通信中去. 在扩频多址通信中扩频码的性能占着举足轻重的作用, 它的好坏将直接影响整个系统性能的优劣, 所以如何构造出好的扩频序列就成为人们研究的热点[1,2]. 而在扩频码的特性中, 线性复杂度又是一个重要的指标, 因为只有大线性复杂度的序列才可以不会被别人轻易截获和破译, 因此构造出具有大线性复杂度的扩频序列也成了人们研究的焦点之一[3]. 1984 年, Scholtz 和 Welch 提出了用迹函数生成 GMW 序列的一种方法[4], 人们发现此序列不仅和 m 序列一样具有理想自相关性能, 而且对于相同周期的两种序列, GMW 序列的线性复杂度要大于 m 序列. 从此, 人们开始了对 GMW 序列线性复杂度的研究[5,6]. 我们知道迹函数的形式是多变的, 对于相同周期长度的序列改变其迹函数的参数, 就会得到不同的 GMW 序列, 但是这些 GMW 序列的线性复杂度是不同的, 甚至是相差很大的, 所以说拿任意的 GMW 序列来进行扩频序列的构造肯定会有比 m 序列好的效果, 但并不一定是最好的效果, 因此要想达到最好的效果就要对 GMW 序列进行筛选, 取出其中具有最大线性复杂度的 GMW 序列来进行扩频序列的构造. 1993 年, Klapper 等人针对特殊情况讨论了 GMW 序列的线性复杂度[5]; 1999 年, Chung 等人也只是研究了 GMW 序列线性复杂度的求法[6], 均没有涉及到最值问题, 且计算公式较繁琐, 不易理解.

针对以上情况本文对 GMW 序列线性复杂度进行了更进一步的研究, 用数学的方法简化了算法, 给出了针对固定长度构造具有最大线性复杂度的 GMW 序列的快速方法. 应用此法只需进行简单的计算就可以快速构造出具有最大线性复杂度的 GMW 序列.

2 理论基础

设 q 为 2 的某个阶数次幂, $GF(q)$ 表示含有 q 个元素的 Galois 域.

定义 **1**[7] 迹函数 $y=tr_q^{q^n}(x)$ 表示由 $GF(q^n)$ 到 $GF(q)$ 的一个映射, 即对任意的 $x\in GF(q)$ 有

$$tr_q^{q^n}(x)=\sum_{i=0}^{n-1}x^{q^i} \tag{1}$$

定义 **2**[4] 设 $q_0=2$ 且 $q_i=q_{i-1}^{n_i}$, $n_i>1(i=1,2)$ 且为正整数, α 为 $GF(q_2)$ 的一个本原元. 设 k_1 为正整数, $k_1<q_1$ 且 $\gcd(k_1, q_1-1)=1$. 则 GMW 序列 T 其第 j 项定义为

$$T_j=tr_{q_0}^{q_1}(\{tr_{q_1}^{q_2}(\alpha^j)\}^{k_1}) \tag{2}$$

收稿日期: 2004-06-13; 修回日期: 2005-01-10
基金项目: 国家自然科学基金(No. 60272026)

引理 1[9] 设 $q_0=2$ 且 $q_i=q_{i-1}^{n_i}$, $n_i>1(i=1,2)$ 且为正整数. α 为 $GF(q_2)$ 的一个本原元, 且设 $\beta=\alpha^K$, 其中 $K=(q_2-1)/(q_1-1)$. 对一个指标集 $J=\{d_1,d_2,\cdots,d_Q\}$, 周期为 q_1-1 的序列 S, 其第 j 项$(j=1,2,\cdots,q_1-1)$表示如下

$$S_j=\sum_{d\in J}tr_{q_0}^{q_1}(\beta^{dj})=\sum_{i=1}^{Q}tr_{q_0}^{q_1}(\beta^{d_ij}) \tag{3}$$

设此序列有理想自相关性能, 则对一个整数 r, $1\leqslant r\leqslant q_1-2$, 且 r 和 q_1-1 相对互素, 周期为 q_2-1 的序列 T', 其第 j 项$(j=1,2,\cdots,q_2-1)$定义为

$$T'_j=\sum_{d\in J}tr_{q_0}^{q_1}(tr_{q_1}^{q_2}(\alpha^t))^{dr}=\sum_{i=1}^{Q}\sum_{\alpha\in I(n_1n_2,\,n_1;\,\langle d_ir\rangle_{q_1-1})}tr_{q_0}^{q_2}(\alpha^{tj}) \tag{4}$$

也有理想自相关性能. 如果 2^jd_i, $0\leqslant j\leqslant n_1-1$, 对每个 i 模 q_1-1 都不同. 则 T' 的线性复杂度为

$$L=n_1\sum_{i=1}^{Q}(n_2)^{wt\langle d_ir\rangle_{q_1-1}} \tag{5}$$

其中 $wt\langle d_ir\rangle_{q_1-1}$ 表示 d_ir 模 q_1-1 的二进制表达式中的项数.

3 GMW 序列最大线性复杂度快速求法

在这里我们分两种情况来讨论 GMW 序列最大线性复杂度的求取问题: (1) 当参数 n_1, n_2 均已取定时, 怎样选择 k_1 不同的值使得 GMW 序列的线性复杂度最大; (2) 当 n_1n_2 取定时, 怎样选择 n_1, n_2 和 k_1 值从而使得 GMW 序列的线性复杂度达到最大.

定理 1 设周期为 $M=q_2-1$ 的 GMW 序列 T 其第 j 项为

$$T_j=tr_{q_0}^{q_1}(\{tr_{q_1}^{q_2}(\alpha^j)\}^{k_1}) \tag{6}$$

其中 $q_0=2$, $q_i=q_{i-1}^{n_i}$, $n_i>1(i=1,2)$ 且为正整数, α 为 $GF(q_2)$ 的一个本原元, k_1 为正整数满足 $k_1<q_1$ 且 $\gcd(k_1,q_1-1)=1$, 则 T 具有理想自相关性能且其线性复杂度为

$$L=n_1(n_2)^{wt\langle k_1\rangle_{q_1-1}} \tag{7}$$

如果参数 n_1, n_2 均已取定, 则当 $k_1=2^{n_1}-k_2-1(k_2=2^0,2^1,2^2,\cdots,2^{n_1-1})$ 时, T 的线性复杂度取得最大值

$$L_{max}=n_1(n_2)^{n_1-1} \tag{8}$$

证明 在引理 1 中取指标集 $J=\{1\}$, 则 $S_j=tr_{q_0}^{q_1}(\beta^j)$ 为 m 序列, 又知 m 序列有理想自相关性能, 则周期为 $M=q_2-1$ 的 GMW 序列 $T_j=tr_{q_0}^{q_1}(\{tr_{q_0}^{q_2}(\alpha^j)\}^{k_1})$ 也有理想自相关性能. 又由引理 1 可见当取指标集 $J=\{1\}$ 时, GMW 序列的线性复杂度为 $L=n_1(n_2)^{wt\langle k_1\rangle_{q_1-1}}$.

由公式(7)知 $L=n_1(n_2)^{wt\langle k_1\rangle_{q_1-1}}$, 因为 k_1 为正整数且 $k_1<q_1$, $\gcd(k_1,q_1-1)$, 所以 $k_1\leqslant q_1-2$. 又因为 $q_1-1=2^0+2^1+\cdots+2^{n_1-1}$, 所以我们可以得到 $q_1-2=2^1+2^2+\cdots+2^{n_1-1}$, 因此 $wt\langle k_1\rangle_{q_1-1}\leqslant n_1-1$, 这样设 $k_2=2^0,2^1,2^2,\cdots,2^{n_1-1}$, 当 $k_1=2^{n_1}-k_2-1$ 时, $wt\langle k_1\rangle_{q_1-1}=n_1-1$ 且能满足 $\gcd(k_1,q_1-1)=1$, GMW 序列 T 的线性复杂度取得最大值 $L_{max}=n_1(n_2)^{n_1-1}$.

推论 1 对于定理 1 中的 GMW 序列 T, 如果参数 n_1, n_2 均已取定, 则当 $k_1=2,2^2,2^3,\cdots,n^{n_1-1}$ 时, T 的线性复杂度取得最小值

$$L_{min}=n_1n_2 \tag{9}$$

证明 当 $k_1=2,2^2,2^3,\cdots,2^{n_1-1}$ 时, $wt\langle k_1\rangle_{q_1-1}=1$, 由公式(7)可见此时线性复杂度取得最小值 $L_{min}=n_1n_2$.

推论 2 设GMW 序列 T 如定义 2 中所定义, 参数 n_1, n_2 均已取定, 则选择不同的 k_1 值, T 的线性复杂度可以取 n_1n_2, $n_2n_2^2$, $\cdots$, $n_1(n_2)^{(n_1-1)}$ 中不同的值.

定理 2 设周期为 $M=q_2-1$ 的 GMW 序列 T 如定义 2 中所定义, 则当 $n_2=2$, $n_1=\frac{\log_2(M+1)}{2}$, $k_1=2^{\frac{\log_2(M+1)}{2}-1}-k_2-1$ $(k_2=2^0,2^1,2^2,\cdots,2^{n_1-2})$ 时, 序列 T 的线性复杂度取得最大值

$$L_{max}=\frac{\log_2(M+1)}{2}(2)^{\frac{\log_2(M+1)}{2}-1} \tag{10}$$

证明 由定理 1 知

$$L_{max}=n_1(n_2)^{n_1-1} \tag{11}$$

因为 $q_0=2$ 且 $q_i=q_{i-1}^{n_i}$ $(i=1,2)$, 所以 $q_1=q_0^{n_1}=2^{n_1}$, $q_2=q_1^{n_2}=2^{n_1\cdot n_2}$, 又因为 $M=q_2-1$, 所以 $2^{n_1\cdot n_2}=M+1$, 即 $n_1\cdot n_2=\log_2(M+1)$. 由于参数 n_1, n_2 为不定值, 所以上式可以化为以下形式

$$L_{max}=\frac{\log_2(M+1)}{n_2}(n_2)^{\frac{\log_2(M+1)}{n_2}-1} \tag{12}$$

因为 n_2 必须大于 1, 即 $n_2\geqslant 2$ 且为正整数, 这是因为如果 $n_2=1$, 那么序列就会退变成 m 序列, 不符合我们的前提条件, 所以 n_2 必为大于或者等于 2 的正整数, 又指数函数的增长要远远大于幂函数的增长速度, 所以要想使式(12)取得最大值就必须使 n_2 项越小越好, $\frac{\log_2(M+1)}{n_2}-1$ 项越大越好, 从此式我们可以看出当 $n_2=2$, $n_1=\frac{1}{2}\log_2(M+1)$, $k_1=2^{\frac{\log_2(M+1)}{n_2}-1}-k_2-1(k_2=2^0,2^1,2^2,\cdots,2^{n_1-2})$ 时, L 取得最大值

$$L'_{max}=\frac{\log_2(M+1)}{2}(2)^{\frac{\log_2(M+1)}{2}-1} \tag{13}$$

推论 3 设周期为 $M=q_2-1$ 的 GMW 序列 T 如定义 2 中所定义, 则当 $n_1=2$, $n_2=\frac{1}{2}\log_2(M+1)$, $k_1=2$ 时, 序列 T 的线性复杂度取得最小值 $\log_2(M+1)$.

证明 由式(7)和定理 2 的证明可见, 当 $n_1=2$, $n_2=\frac{1}{2}\log_2(M+1)$ 时, 因为 k_1 为正整数, $k_1<q_1=2^{n_1}=4$ 且 $\gcd(k_1,3)=1$, 所以 $k_1=2$, L 取得最小值

$$L'_{min}=n_1n_2=\log_2(M+1) \tag{14}$$

4 实例

为了说明定理 1 和定理 2, 下面我们举两个实际的例子.

例 1 设 GMW 序列 T 的第 j 项为

$$T_j=tr_2^6(\{tr_{2^6}^{2^{24}}(\alpha^j)\}^{k_1})$$

求 T 的线性复杂度 L 的取值范围.

解 由已知可见 $q_1=2^6$, $q_2=2^{24}$, T 的周期为 $q_2-1=2^{24}-1$, $n_1=6$, $n_2=4$. 由公式(7)知 $L=n_1(n_2)^{wt\langle k_1\rangle_{q_1-1}}$, 根据定

理1 知, 当 $k_1= 2^{n_1}- k_2- 1$, 其中$(k_2= 2^0, 2^1, 2^2, \cdots, 2^{n_1-1})$, 即 $k_1= 62, 61, 59, 55, 47, 31$ 时, T 的线性复杂度 L 取得最大值 $L_{max}= 6\times (4)^{6-1}= 6144$. 当 $k_1= 2, 2^2, \cdots, 2^5$ 时, L 取得最小值 $L_{min}= 6\times 4= 24$.

从这个例子我们可以看出, 对 GMW 序列来说, 当 n_1n_2 给定时, 选择不同的 k_1 值, 可以得到具有不同线性复杂度的 GMW 序列, 也就是说可以通过改变参数 k_1 的值来改变序列的线性复杂度, 从而寻找出具有更大线性复杂度的 GMW 序列.

例 **2**　设 GMW 序列 T 的第 j 项为

$$T_j= tr_{q_0}^{q_1}(\{tr_{q_1}^{2^4}(\alpha^j)\}^{k_1})$$

求 T 的线性复杂度 L 的取值范围.

解　已知GMW 序列 T 的周期为 $M= q_2- 1= 2^{24}- 1$, 由定理 2 知, 当 $n_2= 2$, $n_1= \frac{1}{2}\log_2(M+ 1)= 12$, $k_1= 2^{\frac{\log_2(M+1)}{2}-1}- k_2- 1$ $(k_2= 2^0, 2^1, 2^2, \cdots, 2^{n_1-2})$, 即 $k_1= 2046, 2045, 2043, 2039, 2031, 2015, 1983, 1919, 1791, 1535, 1023$ 时, T 的线性复杂度 L 取得最大值 $n_1(n_2)^{n_1-1}= 12\cdot(2)^{12-1}= 24566$. 当 $n_1= 2$, $n_2= 12$, $k_1= 2$ 时, L 取得最小值 $n_1n_2= 2(12)= 24$.

从例 2 我们可以看出, 对 GMW 序列来说, 当只给定其周期, 即 n_1n_2 给定时, 我们可以选择 n_1, n_2 和 k_1 的值, 从而改变序列的线性复杂度, 使得序列的线性复杂度取得最大值, 且此方法具有普遍意义. 如果需要用 GMW 序列构造扩频族, 就可以很快捷的通过带入 n_1, n_2 和 k_1 值而得到一些具有较大线性复杂度的 GMW 序列来进行构造.

5　结论

综上所述, 本文研究了 GMW 序列线性复杂度的最值问题, 给出了对于相同周期长度的 GMW 序列怎样选择其参数从而使得序列的线性复杂度取得最大值的快速求法, 以此来构造新的 GMW 序列, 由实例可见用此方法来构造扩频序列族简单易行、便于理解, 应该是更好的选择.

参考文献:

[1] A Klapper. Spectral method for cross correlations of geometric sequences[J]. IEEE Trans Inform Theory, 2004, 50(1): 229– 232.

[2] W Sun, A Klapper, Y Yang. On correlations of a family generalized geometric sequences[J]. IEEE Trans Inform Theory, 2001, 47(9): 2609 – 2618.

[3] P V Kumar. Frequency hopping code sequences designs having large linear span[J]. IEEE Trans Inform Theory, 1988, 34(1): 146– 151.

[4] R A Scholtz, L R Welch. GMW sequence[J]. IEEE Trans Inform Theory, 1984, 30(3): 548– 553.

[5] A Klapper, A H Chan, M Goresky. Cascaded GMW sequences[J]. IEEE Trans Inform Theory, 1993, 39(1): 177– 183.

[6] H Chung, J S No. Linear span of extended sequences and cascaded GMW sequences[J]. IEEE Trans Inform Theory, 1999, 45(6): 2060– 2065.

[7] 梅文华, 杨义先. 基于GMW 序列构造最佳跳频序列族[J]. 通信学报, 1997, 18(11): 20– 24.

作者简介:

陈嘉兴　男, 1977 年生于安徽阜阳, 1999 年获河北师范大学学士学位, 2002 年获燕山大学硕士学位, 现在哈尔滨工业大学攻读信号与信息处理专业博士学位, 研究方向为扩展频谱通信和信道编码, E-mail: xinghuo2815@163.com.

周廷显　男, 1937 年生于辽宁大连, 1962 年毕业于哈尔滨工业大学无线电工程系, 教授, 博士生导师, 中国电子学会三遥分会委员, 中国宇航学会遥测专业委员会委员, 长期从事扩展频谱通信及遥测遥控等方面的研究工作.