周期为 pq 阶为 2^k 的 D-广义割圆序列的线性复杂度

李胜强，汪晓芬，肖国镇
(西安电子科技大学 综合业务网理论与关键技术国家重点实验室,陕西 西安 710071)

摘要：线性复杂度是度量序列随机性的一个最重要的指标. 基于 D-广义割圆,通过寻找序列的特殊的特征集,构造了一类周期为 pq 阶数为 2^k 的 D-广义割圆序列,并确定了该类序列的线性复杂度,其线性复杂度最小为 $(n-1)/2$,最大为 n. 且该类序列为平衡序列.

关键词：D-广义割圆 特征集 线性复杂度
中图分类号：TN918.1 **文献标识码**：A **文章编号**：1001-2400(2006)02-0322-05

The linear complexity of new Ding-generalized cyclotomic sequences of order 2^k of length pq

LI Sheng-qiang, *WANG Xiao-fen*, *XIAO Guo-zhen*
(State Key Lab. of Integrated Service Networks, Xidian Univ., Xi'an 710071, China)

Abstract: Linear complexity is the most important index for measuring the randomness properties of sequences. Based on the Ding-generalized cyclotomy, new generalized cyclotomic sequences of order 2^k of length pq are constructed by finding out a special characteristic set. The linear complexity of the sequences is determined. The minimum of the linear complexity is $(n-1)/2$ and the maximum of the linear complexity is n. And the sequences are balanced.

Key Words: Ding-generalized cyclotomy; characteristic set; linear complexity

割圆理论是一个古老的话题,基于割圆理论的割圆序列最早是 Ding[1] 提出来的,在文献[1]中作者给出了割圆序列的一般构造方法. 1998 年,Ding 提出了一种新的广义割圆方法,称为 D-广义割圆,这种广义割圆可看作是割圆的直接推广.

线性复杂度是度量序列随机性的一个最重要的指标. 文献[2]确定了周期为 pq 阶数为 2 的 D-广义割圆序列的线性复杂度. 笔者发现,通过找到序列的特殊的特征集,可将结果推广到 2^k 的情况,由此构造了一类周期为 pq 阶数为 2^k 的 D-广义割圆序列,简记为 D-GCS$_{2^k}$,并确定了该类序列的线性复杂度. 其线性复杂度最小为 $(n-1)/2$,最大为 n. 且该类序列为平衡序列,是密码学意义上好的序列.

1 预备知识

1.1 阶为 2^k 的 D-广义割圆及其序列

设 p,q 为奇素数,$\gcd(p-1,q-1)=2^k$,k 为正整数. 令 $n=pq$,$e=(p-1)(q-1)/2^k$. 设 g 为 GF(p) 和 GF(q) 的公共本原元,则 $\mathrm{ord}_n(g)=e$. 令整数 x 满足 $x\equiv g(\bmod p)$,$x\equiv 1(\bmod q)$. 则 Z_n 中的全部可逆元可表示为 $Z_n^*=\{g^t x^i : t=0,1,\cdots,(e-1);\ i=0,1,\cdots,(2^k-1)\}$.

阶数为 2^k 的 D-广义割圆类 $D_i^{(n)}$ 定义为

$$D_i^{(n)}=\{(g^{2^k t+i},g^{2^k t+i}x,\cdots,g^{2^k t+i}x^{2^k-1}) : t=0,1,\cdots,(e-2^k)/2^k\},\quad i=0,1,\cdots,(2^k-1).$$

设 $F\subseteq Z_n$,$a\in Z_n$,定义 $F\pm a=\{f\pm a; f\in F\}$,$a\cdot F=\{a\cdot f; f\in F\}$. 记

收稿日期：2005-05-23
基金项目：国家自然科学基金资助项目(60473028；60404290135)
作者简介：李胜强(1980-),男,西安电子科技大学博士研究生.

$$D_0^{(p)} = \left\{g^{2^k t} : t = 0,1,\cdots,\frac{p-2^k-1}{2^k}\right\},\quad D_0^{(q)} = \left\{g^{2^k t} : t = 0,1,\cdots,\frac{q-2^k-1}{2^k}\right\},$$

$$D_1^{(p)} = g\,D_0^{(p)}, D_2^{(p)} = g^2 D_0^{(p)},\cdots,D_{2^k-1}^{(p)} = g^{2^k-1} D_0^{(p)},$$

$$D_1^{(q)} = g\,D_0^{(q)}, D_2^{(q)} = g^2 D_0^{(q)},\cdots,D_{2^k-1}^{(q)} = g^{2^k-1} D_0^{(q)},\quad R = \{0\},$$

$$C_0 = R \cup \left[q \bigcup_{i=0}^{2^{k-1}-1} D_{2i}^{(p)}\right] \cup \left[p \bigcup_{i=0}^{2^{k-1}-1} D_{2i}^{(q)}\right] \cup \left[\bigcup_{i=0}^{2^{k-1}-1} D_{2i}^{(n)}\right]$$

$$C_1 = \left[q \bigcup_{i=0}^{2^{k-1}-1} D_{2i+1}^{(p)}\right] \cup \left[p \bigcup_{i=0}^{2^{k-1}-1} D_{2i+1}^{(q)}\right] \cup \left[\bigcup_{i=0}^{2^{k-1}-1} D_{2i+1}^{(n)}\right],$$

则 $C_0 \cup C_1 = Z_n, C_0 \cap C_1 = \varnothing$. D-GCS$_{2^k}$ 定义为:对所有的 $i, s_i = \begin{cases} 0, & (i \bmod n) \in C_0; \\ 1, & (i \bmod n) \in C_1. \end{cases}$ 把 C_1 称为序列 S 的特征集.

在序列 D-GCS$_{2^k}$ 的一个周期段中有 $(n-1)/2$ 个 1,$(n+1)/2$ 个 0,又 n 为奇数,因此该序列为平衡序列.

1.2　阶数为 2^k 的 D-广义割圆序列的线性复杂度

设 $S = (s_0, s_1, \cdots, s_{n-1})$ 为 GF(q) 上周期为 n 的序列,S 的线性复杂度 LC(S) 定义为满足 $c_0 s_i + c_1 s_{i-1} + \cdots + c_l s_{i-l} = 0$ ($l \leqslant i \leqslant n$) 的最小正整数 l,其中 $c_0 = 1, c_1, c_2, \cdots, c_l \in \mathrm{GF}(q)$,多项式 $c(x) = 1 + c_1 x + \cdots + c_l x^l$ 称为 S 的极小多项式.

记 $s(x) = s_0 + s_1 x + \cdots + s_{n-1} x^{n-1}$,则序列 S 的线性复杂度可简单地表示为[3,4]

$$\mathrm{LC}(S) = n - \deg[\gcd(x^n - 1, s(x))]. \tag{1}$$

记 $P_0 = pD_0^{(q)}, P_1 = pD_1^{(q)},\cdots,P_{2^k-1} = pD_{2^k-1}^{(q)}, Q_0 = qD_0^{(p)}, Q_1 = qD_1^{(p)},\cdots,Q_{2^k-1} = qD_{2^k-1}^{(p)}, D_0 = D_0^{(n)}, D_1 = D_1^{(n)},\cdots,D_{2^k-1} = D_{2^k-1}^{(n)}, P = \bigcup_{i=0}^{2^k-1} P_i, Q = \bigcup_{i=0}^{2^k-1} Q_i$.

根据 D-GCS$_{2^k}$ 的构造方式:$s(x) = \sum_{i \in C_1} x^i = \sum_{j=0}^{2^{k-1}-1} \left(\sum_{i \in P_{2j+1}} + \sum_{i \in Q_{2j+1}} + \sum_{i \in D_{2j+1}}\right) x^i \in \mathrm{GF}(2)[x]$.

设 m 为 2 的模 n 阶,即 $2^m \equiv 1 \pmod n$. 由于 $\gcd(n,2) = 1$,故在 $x^n - 1 \in \mathrm{GF}(2)[x]$ 的分裂域 GF(2^m) 上存在 n 次单位原根 α,由式(1)有

$$\mathrm{LC}(s) = n - |\{j : s(\alpha^j) = 0,\ 0 \leqslant j \leqslant n-1\}|. \tag{2}$$

由于 $0 = \alpha^n - 1 = (\alpha^p)^q - 1 = (\alpha^p - 1)(1 + \alpha^p + \cdots + \alpha^{(q-1)p})$,因此 $\sum_{i \in P} \alpha^i = \sum_{j=0}^{2^k-1} \sum_{i \in P_j} \alpha^i = 1$.

同样的根据对称性有 $$\sum_{i \in Q} \alpha^i = \sum_{j=0}^{2^k-1} \sum_{i \in Q_j} \alpha^i = 1. \tag{3}$$

引理 1　设 $a \in D_j$,则 $aD_i = D_{(i+1) \pmod{2^k}}$,　$i, j = 0, 1, 2, \cdots, (2^k - 1)$[5].

引理 2　在 p 特征域中,恒有 $x^p - a^p = (x - a)^p$,其中 a 为域中的任意元素[3].

引理 3　设 p 为奇素数,$\gcd(p,n) = 1$,则 $(n/p) = n^{(p-1)/2} \pmod p$. 特别地[6]

$$(2/p) = (-1)^{(p^2-1)/8} = \begin{cases} 1, & p \equiv \pm 1 \pmod 8, \\ -1, & p \equiv \pm 3 \pmod 8. \end{cases}$$

2　主要结果

下面出现的数学符号定义和上相同. 现在给出本文中构造的 D-广义割圆序列(D-GCS$_{2^k}$)的线索性复杂度的主要结果. 用 LC(S) 表示该类序列的线性复杂度.

定理 1

(1) 若 $p \equiv 1 \pmod 8$,$q \equiv 3 \pmod 8$ 或者 $p \equiv 7 \pmod 8$,$q \equiv 5 \pmod 8$,则 $\mathrm{LC}(S) = \dfrac{(p+1)q}{2}$.

(2) 若 $p \equiv 5 \pmod 8$,$q \equiv 5 \pmod 8$ 或者 $p \equiv 3 \pmod 8$,$q \equiv 3 \pmod 8$,则 $\mathrm{LC}(S) = pq - 1$.

(3) 若 $p \equiv 5 \pmod 8$,$q \equiv 7 \pmod 8$ 或者 $p \equiv 3 \pmod 8$,$q \equiv 1 \pmod 8$,则 $\mathrm{LC}(S) = pq - \dfrac{(q-1)}{2}$.

(4) 若 $p \equiv 3 \pmod 8$, $q \equiv 7 \pmod 8$ 或者 $p \equiv 5 \pmod 8$, $q \equiv 1 \pmod 8$, 则 $\mathrm{LC}(S) = pq - \dfrac{(q-1)}{2} - 1$.

(5) 若 $p \equiv 5 \pmod 8$, $q \equiv 3 \pmod 8$ 或者 $p \equiv 3 \pmod 8$, $q \equiv 5 \pmod 8$, 则 $\mathrm{LC}(S) = pq$.

(6) 若 $p \equiv 7 \pmod 8$, $q \equiv 3 \pmod 8$ 或者 $p \equiv 1 \pmod 8$, $q \equiv 5 \pmod 8$, 则 $\mathrm{LC}(S) = \dfrac{(p+1)q}{2} - 1$.

(7) 若 $p \equiv 7 \pmod 8$, $q \equiv 1 \pmod 8$ 或者 $p \equiv 1 \pmod 8$, $q \equiv 7 \pmod 8$, 则 $\mathrm{LC}(S) = \dfrac{(pq+1)}{2}$.

(8) 若 $p \equiv 7 \pmod 8$, $q \equiv 7 \pmod 8$ 或者 $p \equiv 1 \pmod 8$, $q \equiv 1 \pmod 8$, 则 $\mathrm{LC}(S) = \dfrac{(pq-1)}{2}$.

为了证明定理 1, 首先证明下面的 4 个引理.

引理 4 $\sum\limits_{i \in D_i} \alpha^{mi} = \begin{cases} 0, & m \in P \\ ((q-1)/2^k) \pmod 2, & m \in Q \end{cases}$, 其中 $i = 1,3,5,\cdots,(2^k-1)$.

证明 设 $m \in P$, 由于 g 是 $\mathrm{GF}(p)$ 和 $\mathrm{GF}(q)$ 的公共本原元. 并且 $\mathrm{ord}_n(g) = e$, 由 x 的定义, $D_i \pmod q = \{(g^{2^{kt+i}}, g^{2^{kt+i}}x, \cdots, g^{2^{kt+i}}x^{2^k-1}) \pmod q : t = 0,1,\cdots,((e-2^k)/2^k)\} = D_i^{(q)}$ $(i = 1,3,5,\cdots 2^k-1))$. 因此, 当 t 遍历 $\{0,1,\cdots,((e-2^k)/2^k)\}$ 时, $D_i \pmod q = D_i^{(q)}$ $(i = 1,3,5,\cdots,(2^k-1))$. 且每个值都被取 $(p-1)$ 次, 则

$$\sum_{i \in D_j} \alpha^{mi} = [(p-1) \bmod 2] \sum_{i \in D_j^{(q)}} \alpha^{mi} = 0, \quad j = 1,3,5,\cdots,(2^k-1).$$

同理, 当 $m \in Q$ 时, 有

$$\sum_{i \in D_j} \alpha^{mi} = \left[\frac{(q-1)}{2^k} \bmod 2\right] \sum_{i \in Q} \alpha^i = \frac{(q-1)}{2^k} \pmod 2, \quad j = 1,3,5,\cdots,(2^k-1). \qquad \text{证毕.}$$

引理 5
$$s(\alpha^m) = \begin{cases} s(\alpha), & m \in Z_n^*, \ m \pmod p \in \bigcup\limits_{i=0}^{2^{k-1}-1} D_{2i}^{(p)}, \\ s(\alpha)+1, & m \in Z_n^*, \ m \pmod p \in \bigcup\limits_{i=0}^{2^{k-1}-1} D_{2i+1}^{(p)}, \\ \left(\dfrac{(p-1)}{2} \bmod 2\right) + \sum\limits_{j=0}^{2^{k-1}-1} \sum\limits_{i \in P_{2j+1}} \alpha^{mi}, & m \in P, \\ \sum\limits_{j=0}^{2^{k-1}-1} \sum\limits_{i \in Q_{2j+1}} \alpha^{mi}, & m \in Q. \end{cases}$$

证明 显然有 $D_j \pmod p = \bigcup\limits_{i=0}^{2^k-1} D_i^{(p)}$ $(j = 0,1,2,\cdots,(2^k-1))$, $D_i \pmod q = D_i^{(q)}$ $(i = 0,1,2,\cdots,(2^k-1))$. 由引理 1, 若 $m \in D_0$, 则 $mD_1 = D_1$, $mD_3 = D_3, \cdots, mD_{2^k-1} = D_{2^k-1}$. 若 $m \pmod p \in D_0^{(p)}$, 则 $mQ_1 = qmD_1^{(p)} = Q_1, mQ_3 = Q_3, \cdots, mQ_{2^k-1} = Q_{2^k-1}$; $mP_1 = pmD_1^{(q)} = P_1, mP_3 = P_3, \cdots, mP_{2^k-1} = P_{2^k-1}$. 因此,

$$s(\alpha^m) = \sum_{j=0}^{2^{k-1}-1} \left(\sum_{j \in P_{2j+1}} + \sum_{i \in Q_{2j+1}} + \sum_{i \in D_{2j+1}} \right) \alpha^{mi} = s(\alpha).$$

若 $m \pmod p \in D_1^{(p)}$, 则 $mQ_1 = qmD_1^{(p)} = Q_2$, $mQ_3 = Q_4, \cdots, mQ_{2^k-1} = Q_{2^k} = Q_0$; $mP_1 = pmD_1^{(q)} = P_1$, $mP_3 = P_3, \cdots, mP_{2^k-1} = P_{2^k-1}$. 由(3),

$$s(\alpha^m) = \sum_{j=0}^{2^{k-1}-1} \left(\sum_{i \in P_{2j+1}} + \sum_{i \in Q_{2j+1}} + \sum_{i \in D_{2j+1}} \right) \alpha^{mi} = 1 + s(\alpha).$$

依此类推, 若 $m \pmod p \in D_{2^k-1}^{(p)}$, 则 $s(\alpha^m) = \sum\limits_{j=0}^{2^{k-1}-1} \left(\sum\limits_{i \in P_{2j+1}} + \sum\limits_{i \in Q_{2j+1}} + \sum\limits_{i \in D_{2j+1}} \right) \alpha^{mi} = 1 + s(\alpha)$.

由此得出一般结论, 若 $m \in D_0$, 且满足 $m \pmod p \in D_t^{(p)}$, $t \in \{0,1,2,\cdots,(2^k-1)\}$, 当 t 为偶数时, $s(\alpha^m) = s(\alpha)$; 当 t 为奇数时, $s(\alpha^m) = 1 + s(\alpha)$.

类似可证明, $m \in D_i, i \in \{0,1,2,\cdots,(2^k-1)\}$, 且满足 $m \pmod p \in D_t^{(p)}, t \in \{0,1,2,\cdots,(2^k-1)\}$, 当 t 为偶数时, $s(\alpha^m) = s(\alpha)$; 当 t 为奇数时, $s(\alpha^m) = 1 + s(\alpha)$. 当 $m \in P$, 由引理 4:

$$s(\alpha^m)=\sum_{j=0}^{2^{k-1}-1}\Big(\sum_{i\in P_{2j+1}}+\sum_{i\in Q_{2j+1}}+\sum_{i\in D_{2j+1}}\Big)\alpha^{mi}=\left(\frac{p-1}{2}\right)\pmod 2+\sum_{j=0}^{2^{k-1}-1}\sum_{i\in P_{2j+1}}\alpha^{mi}\quad .$$

当 $m\in Q$,由引理 4:

$$s(\alpha^m)=\sum_{j=0}^{2^{k-1}-1}\Big(\sum_{i\in P_{2j+1}}+\sum_{i\in Q_{2j+1}}+\sum_{i\in D_{2j+1}}\Big)\alpha^{mi}=\sum_{j=0}^{2^{k-1}-1}\sum_{i\in pD_{2j+1}^{(q)}}\alpha^{mi}+$$

$$\sum_{j=0}^{2^{k-1}-1}\sum_{i\in Q_{2j+1}}\alpha^{mi}+\left(\frac{q-1}{2}\right)\pmod 2=\sum_{j=0}^{2^{k-1}-1}\sum_{i\in Q_{2j+1}}\alpha^{mi}\quad .$$

证毕

引理 6　$s(\alpha)\in\{0,1\}$ 当且仅当 $p\equiv\pm1\pmod 8$.

证明　因为域 GF(2) 的特征为 2,由引理 2 知 $[s(\alpha)]^2=s(\alpha^2)$,由引理 5,$s(\alpha^2)=s(\alpha)\Leftrightarrow 2\in\bigcup_{i=0}^{2^{k-1}-1}D_{2i}^{(p)}$. 因此,$s(\alpha)\in\{0,1\}\Leftrightarrow 2\in\bigcup_{i=0}^{2^{k-1}-1}D_{2i}^{(p)}$. 注意到 $\bigcup_{i=0}^{2^{k-1}-1}D_{2i}^{(p)}$ 就是模 p 的全部二次剩余,因此由引理 3 有:$2\in\bigcup_{i=0}^{2^{k-1}-1}D_{2i}^{(p)}\Leftrightarrow p\equiv\pm1\pmod 8$. 证毕

引理 7　(1) 若 $m\in P$,$\sum_{j=0}^{2^{k-1}-1}\sum_{i\in P_{2j+1}}\alpha^{mi}\in\{0,1\}$,当且仅当 $q\equiv\pm1\pmod 8$;(2) 若 $m\in Q$,$\sum_{j=0}^{2^{k-1}-1}\sum_{i\in Q_{2j+1}}\alpha^{mi}\in\{0,1\}$,当且仅当 $p\equiv\pm1\pmod 8$.

证明　若 $m\in P$,$\sum_{j=0}^{2^{k-1}-1}\sum_{i\in P_{2j+1}}\alpha^{mi}=\sum_{j=0}^{2^{k-1}-1}\sum_{i\in D_{2j+1}^{(q)}}\alpha^{mpi}=\sum_{i\in D_1^{(q)}}(\alpha^{p^2})^{vi}+\cdots+\sum_{i\in D_{2^k+1}^{(q)}}(\alpha^{p^2})^{wi}$. 这里 $u,v,\cdots,w\in\{1,2,3,\cdots,(q-1)\}$,设 $\alpha^{p^2}=\beta$,则 β 为 x^q-1 的 q 次单位原根. 注意到 $D_i^{(q)}$ $(i=1,3,5,\cdots,(2^k-1))$ 为模 q 的二次非剩余集合. 因此,由文献[7] 中定理 1 的证明可知:$\sum_{j=0}^{2^{k-1}-1}\sum_{i\in P_{2j+1}}\alpha^{mi}\in\{0,1\}$,当且仅当 $q\equiv\pm1\pmod 8$. 同理可证明引理第二部分. 证毕

显然有下式成立:

$$s(1)=\left[\frac{(p-1)}{2}+\frac{(q-1)}{2}+\frac{(p-1)(q-1)}{2}\right]\pmod 2=\left(\frac{(p-1)}{2}+\frac{(q-1)}{2}\right)\pmod 2\quad .\quad (4)$$

下面给出定理 1 的证明.

结论(1)　若 $p\equiv1\pmod 8$,$q\equiv3\pmod 8$ 或者 $p\equiv7\pmod 8$,$q\equiv5\pmod 8$,则 $\mathrm{LC}(s)=\dfrac{(p+1)q}{2}$.

证明　当 $p\equiv1\pmod 8$,$q\equiv3\pmod 8$ 或者 $p\equiv7\pmod 8$,$q\equiv5\pmod 8$ 时,由式(4)

$$s(\alpha^0)=s(1)=((p-1)/2+(q-1)/2)\pmod 2=1\quad .$$

由引理 3 和引理 6,当 $m\in Z_n^*$ 时,$s(\alpha^m)=\begin{cases}0, & m\in Z_n^*,\ m\pmod p\in\bigcup_{i=0}^{2^{k-1}-1}D_{2i}^{(p)},\\ 1, & m\in Z_n^*,\ m\pmod p\in\bigcup_{i=0}^{2^{k-1}-1}D_{2i+1}^{(p)},\end{cases}$

则使得 $s(\alpha^m)=1$ 的 m 的个数为 $(p-1)(q-1)/2$.

由引理 3 和引理 7,当 $m\in P$ 时,$s(\alpha^m)=0$,即:使得 $s(\alpha)=1$ 的 m 的个数为 0. 当 $m\in Q$ 时,

$$s(\alpha^m)=\begin{cases}0, & m\in\bigcup_{i=0}^{2^{k-1}-1}Q_{2i},\\ 1, & m\in\bigcup_{i=0}^{2^{k-1}-1}Q_{2i+1},\end{cases}$$

则使得 $s(\alpha^m)=1$ 的 m 的个数为 $\left|\bigcup_{i=0}^{2^{k-1}-1}Q_{2i+1}\right|=(p-1)/2$,由式(2)

$$\mathrm{LC}(S)=n-|\{j:s(\alpha^j)=0,\ 0\leqslant j\leqslant n-1\}|=pq-\frac{(p-1)(q-1)}{2}-\frac{(p-1)}{2}=\frac{(p+1)q}{2}\quad .$$

故结论(1)得证. 同理,利用定理 1 中结论(1)的证明方法,容易证明定理 1 的结论(2)~(8)也是成立的. 证毕

3 结 论

构造了一类周期为 pq 阶数为 2^k 的 D-广义割圆序列,确定了该类序列的线性复杂度,构造该类序列时把 Z_n 划分为 C_0 和 C_1 两个子集时必须满足下面的条件:C_0 的子集 $qD_i^{(p)}, pD_i^{(q)}, D_i^{(n)}, i \in \{0,1,\cdots,2^k-1\}$ 的下标 i 全为偶数;C_1 的子集 $qD_i^{(p)}, pD_i^{(q)}, D_i^{(n)}, i \in \{0,1,\cdots,2^k-1\}$ 的下标 i 全为奇数. 由定理1的结论可知:该类序列的线性复杂度最小值为 $(n-1)/2$,最大可达到 n,且该类序列为平衡序列. 除了 $p \equiv 7 \pmod 8$, $q \equiv 7 \pmod 8$ 和 $p \equiv 1 \pmod 8$, $q \equiv 1 \pmod 8$ 外,序列的线性复杂度均大于 $(n+1)/2$,因此,按 B-M 算法,获取该序列的任何一段子序列都不能用该算法恢复出全部序列.

参考文献:

[1] Ding C. Binary Cyclotomic Generators[A]. Fast Software Encryption:LNCS 1 008[C]. Berlin:Springer-Veralg, 1995. 20-60.

[2] 白恩健. 伪随机序列构造及其随机性分析研究[D]. 西安:西安电子科技大学,2004. 43-52.

[3] Lidl R, Niederreiter H. Finite Fields[M]. Reading:Addison-Wesley, 1983.

[4] Xu Chunxiang, Wei Shimin, Xiao Guozhen. On the Linear Complexity of Periodic Sequences[J]. Journal of Xidian University, 2001, 28(4):434-437.

[5] Ding C. New Generalized Cyclotomy and Its Applications[J]. Finite Fields and Their Applications, 1998, 4(2):140-166.

[6] 柯 召,孙 琦. 数论讲义[M]. 北京:高等教育出版社,1987.

[7] Ding C, Helleseth T, Shan W J. On the Linear Complexity of Legendre Sequences[J]. IEEE Trans of Information Theory, 1998, 44(3):1 276-1 278.

(编辑:李维东)

(上接第 294 页)

step 3 由式(3)计算得:$\omega_1 = 0.2129$, $\omega_2 = 0.2128$, $\omega_3 = 0.1992$, $\omega_4 = 0.3750$. 从而相应方案的排序为:$x_3 \prec x_2 \prec x_1 \prec x_4$,即最佳方案为 x_4.

4 结 束 语

给出了区间数一致性互补判断矩阵的概念及其判断定理,提出了区间数互补判断矩阵权重向量确定的目标规划法,操作简单、易于上机实现,为解决区间数互补判断矩阵排序问题开辟了一条新的途径,利用信息集结算子,文中的排序方法在区间数群决策中也有良好的应用前景.

参考文献:

[1] Hwang C L, Yoon K. Multiple Attribute Decision Making[M]. Berlin:Springer-Verlag, 1981.

[2] Orlorski S A. Decision-making with a Fuzzy Preference Relation[J]. Fuzzy Sets and Systems, 1978, 1(2):155-167.

[3] Van Laarboven P J M, Pedrycz W. A Fuzzy Extension of Saaty's Priority Theory[J]. Fuzzy Sets and Systems, 1983, 11(2):229-241.

[4] 徐泽水. 模糊互补判断矩阵的排序方法研究[J]. 系统工程与电子技术,2002, 24(11):73-75.

[5] 樊治平,姜艳萍,肖四汉. 模糊判断矩阵的一致性及其性质[J]. 控制与决策,2001, 16(1):69-71.

[6] 宋光兴,杨德礼. 模糊判断矩阵排序向量的确定方法研究[J]. 模糊系统与数学,2004, 18(2):74-83.

[7] 徐泽水. 不确定多属性决策方法及应用[M]. 北京:清华大学出版社,2004.

[8] 张吉军. 区间数的排序方法研究[J]. 运筹与管理,2003, 12(3):18-22.

[9] Feng Xiaohui, Yu Xijian, Zhang Yueling. A New Algorithm-RD for Linear Programming[J]. Journal of Xidian University, 2000, 27(5):627-629.

[10] Sengupta A, Pal T K. On Comparing Interval Numbers[J]. European Journal of Operational Research, 2000, 127(1):28-43.

[11] 刘进生,王绪柱,张宝玉. 区间数排序[J]. 工程数学学报,2001, 18(4):103-109.

[12] 吴 江,黄登仕. 区间数排序方法研究综述[J]. 系统工程,2004, 20(8):1-4.

[13] Nakahara Y, Sasaki M, Gen M. On the Linear Programming Problems with Interval Coefficients[J]. Journal of Computer Industrial Engineering, 1992, 23(2):301-304.

(编辑:齐淑娟)