关于二元割圆序列的 k-错线性复杂度

陈智雄[1]，吴晨煌[1,2]
（1. 莆田学院福建省高校应用数学重点实验室，福建 莆田 351100；2. 电子科技大学计算机科学与工程学院，四川 成都 611731）

摘 要：应用伪随机序列的离散傅里叶变换，讨论了周期为素数 p 的 Legendre 序列、Ding-Helleseth-Lam 序列及 Hall 六次剩余序列的 k-错线性复杂度。具体地，首先确定了上述 3 种序列的 1-错线性复杂度，其次对 $k \geqslant 2$，以及 2 模 p 的阶的一些特殊取值，讨论了相应序列的 k-错线性复杂度。

关键词：Legendre 序列；Ding-Helleseth-Lam 序列；Hall 六次剩余序列；k-错线性复杂度；离散傅里叶变换
中图分类号：TP309
文献标识码：A
doi: 10.11959/j.issn.1000−436x.2019034

k-error linear complexity of binary cyclotomic generators

CHEN Zhixiong[1], WU Chenhuang[1,2]
1. Provincial Key Laboratory of Applied Mathematics, Putian University, Putian 351100, China
2. School of Computer Science and Engineering, University of Electronic Science and Technology of China, Chengdu 611731, China

Abstract: In terms of the discrete Fourier transforms, the k -error linear complexities over $\mathbb{F}_2$ were discussed for Legendre, Ding-Helleseth-Lam, and Hall's sextic residue sequences of odd prime period p . More precisely, the 1-error linear complexities of these sequences were determined. Then, with some special restrictions of the order of 2 modulo p , partial results on their k -error linear complexities ($k \geqslant 2$) were proved.

Key words: Legendre sequence, Ding-Helleseth-Lam sequence, Hall's sextic residue sequence, k-error linear complexity, discrete Fourier transform

1 引言

设有限域 $\mathbb{F}_p = \{0,1,\cdots,p-1\}$，其中 p 为奇素数。g 为模 p 的一个本原根。若 $r \mid (p-1)$，则 r 阶割圆类定义为

$$D_j^{(r)} = \{g^{kr+j} \pmod{p} : 0 \leqslant k < \frac{p-1}{r}\}$$

其中，$j = 0,1,\cdots,r-1$。易知，$D_j^{(r)}$ 构成 $\mathbb{F}_p \setminus \{0\}$ 的一个划分，并被广泛应用于定义伪随机序列[1]。

当 $r=2$ 时，Legendre 序列 (s_u) [2-4]定义为

$$s_u = \begin{cases} 1, & u \pmod{p} \in D_1^{(2)} \\ 0, & \text{否则} \end{cases} \tag{1}$$

其中，$u \geqslant 0$。

当 $r=4$ 时, Ding-Helleseth-Lam 序列 (s_u) [5]定义为

$$s_u = \begin{cases} 1, & u \pmod{p} \in D_0^{(4)} \cup D_1^{(4)} \\ 0, & \text{否则} \end{cases} \tag{2}$$

其中，$u \geqslant 0$。

当 $r=6$ 且 p 形如 $4x^2+27$，$x \in \mathbb{N}$ 时，Hall 六次剩余序列 (s_u) [6-7]定义为

收稿日期：2018−09−21；**修回日期**：2019−01−17
通信作者：吴晨煌，ptuwch@163.com
基金项目：国家自然科学基金资助项目(No.61772292)；国家自然科学基金国际合作交流基金资助项目（No. 6181101289）；福建省自然科学基金资助项目（No.2018J01425）；福建省高校创新团队培育计划基金资助项目（No.2018-49）
Foundation Items: The National Natural Science Foundation of China (No.61772292); Projects of International Cooperation and Exchanges NSFC (No. 6181101289), The Natural Science Foundation of Fujian Province (No.2018J01425), Program for Innovative Research Team in Science and Technology in Fujian Province University(No.2018-49)

$$s_u=\begin{cases}1, & u\ (\mathrm{mod}\ p)\in D_0^{(6)}\cup D_1^{(6)}\cup D_3^{(6)}\\ 0, & \text{其他}\end{cases} \tag{3}$$

其中，$u\geqslant 0$。

需要注意的是，在文献[6-7]中，g 的选择需满足 $3\in D_1^{(6)}$。

上述几类二元序列已受到广泛的关注和研究。研究表明，这些二元序列具有好的伪随机特性，包括一致分布性、最优相关性、高的线性复杂度等[1-3,5,6,8-12]。Xiong 等[13]证明了 Legendre、Ding-Helleseth-Lam 二元序列的 2-adic 复杂度等于周期 p。最近，Su 等[14]基于 Ding-Helleseth-Lam 二元序列使用交织的方法构造了一个周期为 $4p$ 的具有优的自相关值的二元序列。通常把上面这种 Z_p^*（p 为素数)上的割圆类称为经典割圆类，对应的序列称为经典割圆序列，而把 Z_n^*（n 为合数)上的割圆类称为广义割圆类，对应的序列称为广义割圆序列[15-22]。

文献[23-24]把上述类型序列 (s_u) 视为 p -进制序列并研究了其在有限域 $\mathbb{F}_p$ 上的 k -错线性复杂度。但是，(s_u) 在 $\mathbb{F}_2$ 上的 k -错线性复杂度还未彻底解决。文献[1, 25]证明了任意的非常数二元序列的 k -错线性复杂度的一个下界。

命题 1 ([1，Theorem 3.3.1]) 对周期为 p 的任意非常数二元序列 (s_u)，其在 $\mathbb{F}_2$ 上的 k -错线性复杂度 $\mathrm{LC}_k((s_u))$ 满足 $k<\min\{W_H((s_u)),p-W_H((s_u))\}$ 时，$\mathrm{LC}_k((s_u))\geqslant \mathrm{ord}_p(2)$。其中，$\mathrm{ord}_p(2)$ 表示 2 在模 p 的阶，$W_H((s_u))$ 表示序列 (s_u) 的一个周期中所含 1 的个数。

本文工作主要是考虑由经典割圆类定义的序列 (s_u) 的 k -错线性复杂度。本文计算了 Legendre 序列、Ding-Helleseth-Lam 序列和 Hall 六次剩余序列在 $\mathbb{F}_2$ 上的 1-错线性复杂度，并限制 2 在模 p 的阶的某些取值，给出了这些序列在 $\mathbb{F}_2$ 上的 k -错线性复杂度的一些结果。周期序列的离散傅里叶变换在本文的证明中起到了关键作用。

下面介绍线性复杂度、k -错线性复杂度和周期序列的离散傅里叶变换等概念。

对于 $\mathbb{F}_2$ 上周期为 T 的序列 (s_u)，其线性复杂度（记为 $\mathrm{LC}((s_u))$）定义为 (s_u) 满足 $\mathbb{F}_2$ 上的如下线性递归关系的最小阶 L。

$$s_{u+L}=c_{L-1}s_{u+L-1}+\cdots+c_1s_{u+1}+c_0s_u$$

其中，$u\geqslant 0, c_0\neq 0, c_1,\cdots,c_{L-1}\in\mathbb{F}_2$。记 $S(X)=s_0+s_1X+s_2X^2+\cdots+s_{T-1}X^{T-1}\in\mathbb{F}_2[X]$，$S(X)$ 为 (s_u) 的生成多项式。

那么，(s_u) 在 $\mathbb{F}_2$ 上的线性复杂度可通过式(4)计算。

$$\mathrm{LC}((s_u))=T-\deg\left(\gcd(X^T-1,S(X))\right) \tag{4}$$

对于整数 $k\geqslant 0$，(s_u) 在 $\mathbb{F}_2$ 上的 k -错线性复杂度（记为 $\mathrm{LC}_k((s_u))$）是指在序列的一个周期中改变至多 k 个元素后所得这些序列在 $\mathbb{F}_2$ 上的线性复杂度的最小值[26]。即

$$\mathrm{LC}_k((s_u))=\min_{W_H((e_u))\leqslant k}\mathrm{LC}((s_u+e_u)) \tag{5}$$

其中，(e_u) 为周期为 T 的错误序列，$W_H((e_u))$ 为 (e_u) 的一个周期中所含 1 的个数。k -错线性复杂度也被称为球体复杂度[27]，本文不做详细描述。易知，$\mathrm{LC}_0((s_u))=\mathrm{LC}((s_u))$，且

$$T\geqslant \mathrm{LC}_0((s_u))\geqslant \mathrm{LC}_1((s_u))\geqslant\cdots\geqslant \mathrm{LC}_l((s_u))=0$$

其中，$l=W_H((s_u))$。

线性复杂度和 k -错线性复杂度是序列的重要密码学性质，它们刻画的是序列的可预测性，从而衡量该序列是否适用于密码学领域。从密码学应用角度考虑，一个序列的线性复杂度应尽可能大，并且序列在改变若干项后其线性复杂度不应明显降低。

对于奇数 T，序列 (s_u) 的离散傅里叶变换 $(\rho_0,\rho_1,\cdots,\rho_{T-1})$ 和序列 (s_u) 的线性复杂度具有紧密的联系。记 $m=\mathrm{ord}_T(2)$ 表示 2 在模 T 的乘法阶。对于 T 阶本原单位根 $\beta\in\mathbb{F}_{2^m}$，离散傅里叶变换（DFT，discrete Fourier transform）[28-29]定义为

$$\rho_i=\sum_{0\leqslant u<T}s_u\beta^{-iu}\in\mathbb{F}_{2^m}, 0\leqslant i<T \tag{6}$$

Blahut 定理[30]给出了序列 (s_u) 的线性复杂度及其与 DFT 之间的关系，如式(7)所示。

$$\mathrm{LC}((s_u))=\#\{i:\rho_i\neq 0, 0\leqslant i<T\} \tag{7}$$

其中，$\#\{\cdot\}$ 表示集合 $\{\cdot\}$ 中的元素个数。

多项式 $G(X)=\sum_{0\leqslant i<T}\rho_iX^i\in\mathbb{F}_{2^m}[x]$ 在编码理论中被称为 Mattson-Solomon 多项式[31]。由 DFT 的逆变换，有

$$s_u=\sum_{0\leqslant i<T}\rho_i\beta^{iu}=G(\beta^u), 0\leqslant u<T \tag{8}$$

对于给定的 β，$G(X)$ 在模 x^T-1 下是唯一确定的，$G(X)$ 也称为序列 (s_u) 对应于 β 的 defining 多项式[34]。

2　离散傅里叶变换

Alecu 和 Sălăgean[33-34]利用离散傅里叶变换给出了一个计算序列的 k-错线性复杂度的近似算法。他们的方法有助于本文考虑 Legendre 序列、Ding-Helleseth-Lam 序列和Hall六次剩余序列的 k-错线性复杂度。本节计算了这些序列的离散傅里叶变换。更详细的讨论见文献[32]。

由 $D_l^{(r)}$ 的定义可知

$$uD_l^{(r)} \triangleq \{uv \pmod p : v \in D_l^{(r)}\} = D_{l+j}^{(r)}$$

其中，$u \in D_j$。下文中 $D^{(r)}$ 下标的计算都是在模 r 下进行的，即对所有的 $0 \leqslant l < r$，有 $D_{l+r}^{(r)} = D_l^{(r)}$。定义

$$D_l^{(r)}(X) = \sum_{u \in D_l^{(r)}} X^u \in \mathbb{F}_2[X]$$

$$\mathcal{C}_l^{(r)}(X) = (D_l^{(r)}(X), D_{l+1}^{(r)}(X), \cdots, D_{l+r-1}^{(r)}(X))$$

其中，$0 \leqslant l < r$。本文首先给出并证明如下关于内积计算 $\mathcal{C}_i^{(r)}(\beta)\mathcal{C}_j^{(r)}(\beta)$ 的引理，其中 $0 \leqslant i, j < r$。

引理 1　设 β 为 $\mathbb{F}_2$ 的某一个扩域上的 p 阶本原单位根。对任意一对整数 i, j 满足 $0 \leqslant i, j < r$，有

$$\mathcal{C}_i^{(r)}(\beta)\mathcal{C}_j^{(r)}(\beta) + \frac{p-1}{r} = \begin{cases} 1, & r \mid (\dfrac{p-1}{2} + i - j) \\ 0, & \text{其他} \end{cases}$$

证明　对任意的 $0 \leqslant l < r$，由于 $D_l^{(r)} = g^l D_0^{(r)}$，可得

$$\mathcal{C}_i^{(r)}(\beta)\mathcal{C}_j^{(r)}(\beta) = \sum_{k=0}^{r-1} \sum_{u \in D_0^{(r)}} \beta^{ug^{i+k}} \sum_{v \in D_0^{(r)}} \beta^{vg^{j+k}} =$$

$$\sum_{k=0}^{r-1} \sum_{u \in D_0^{(r)}} \beta^{ug^{i+k}} \sum_{w \in D_0^{(r)}} \beta^{uwg^{j+k}} \ (\text{令} v = uw) =$$

$$\sum_{k=0}^{r-1} \sum_{u \in D_0^{(r)}} \sum_{w \in D_0^{(r)}} \beta^{ug^{j+k}(g^{i-j}+w)} =$$

$$\sum_{w \in D_0^{(r)}} \sum_{k=0}^{r-1} \sum_{z \in D_{j+k}^{(r)}} \gamma_w^z \ (\text{令} z = ug^{j+k}, \gamma_w = \beta^{g^{i-j}+w}) =$$

$$\sum_{w \in D_0^{(r)}} \sum_{z=1}^{p-1} \gamma_w^z$$

设 $\mathrm{ord}(\gamma_w)$ 表示 γ_w 的阶。由于 β 是 p 阶本原单位根，则有 $\mathrm{ord}(\gamma_w) \mid p$。若 $\mathrm{ord}(\gamma_w) = p$，则

$$\sum_{z=1}^{p-1} \gamma_w^z = \sum_{z=0}^{p-1} \gamma_w^z - 1 = \frac{1-\gamma_w^p}{1-\gamma_w} - 1 = 1 \in \mathbb{F}_2$$

若 $\mathrm{ord}(\gamma_w) = 1$，则

$$\sum_{z=1}^{p-1} \gamma_w^z = p - 1 = 0 \in \mathbb{F}_2$$

下面分别计算使 $\mathrm{ord}(\gamma_w) = 1$ 和 $\mathrm{ord}(\gamma_w) = p$ 的元素 $w \in D_0^{(r)}$ 的个数。

可以注意到 $\mathrm{ord}(\gamma_w) = 1$ 当且仅当 $g^{i-j} + w \equiv 0 \pmod p$，即 $w \equiv g^{\frac{p-1}{2}+i-j} \pmod p$。由于 $w \in D_0^{(r)}$，则 $r \mid (\dfrac{(p-1)}{2} + i - j)$。也就是说，存在 $w \in D_0^{(r)}$ 使 $g^{i-j} + w \equiv 0 \pmod p$ 等式成立，当且仅当 $r \mid (\dfrac{p-1}{2} + i - j)$ 并且 w 是唯一的，因此，当 $r \mid (\dfrac{p-1}{2} + i - j)$ 时，有 $\dfrac{p-1}{r} - 1$ 个元素 $w \in D_0^{(r)}$ 满足 $\mathrm{ord}(\gamma_w) = p$，而只有一个 $w \in D_0^{(r)}$ 满足 $\mathrm{ord}(\gamma_w) = 1$。若 $r \nmid (\dfrac{p-1}{2} + i - j)$，则对所有的 $w \in D_0^{(r)}$，都有 $\mathrm{ord}(\gamma_w) = p$。

综上所述，可得

$$\mathcal{C}_i^{(r)}(\beta)\mathcal{C}_j^{(r)}(\beta) = \begin{cases} \dfrac{p-1}{r} - 1, & r \mid (\dfrac{p-1}{2} + i - j) \\ \dfrac{p-1}{r}, & \text{其他} \end{cases}$$

证毕。

下面给出 Legendre 序列、Ding-Helleseth-Lam 序列和 Hall 六次剩余序列的 Mattson-Solomon 多项式。

当 $r = 2$ 时，若 $2 \in D_0^{(2)}$，则 $D_i^{(2)}(\beta) \in \mathbb{F}_2$；若 $2 \in D_1^{(2)}$，则 $D_i^{(2)}(\beta) \in \mathbb{F}_4 \setminus \mathbb{F}_2$，其中 $i = 0,1$。

注意到 $2 \in D_0^{(2)}$（即 2 为模 p 的平方剩余）当且仅当 $p \equiv \pm 1 \pmod 8$，$2 \in D_1^{(2)}$ 当且仅当 $p \equiv \pm 3 \pmod 8$。

命题 2　设 β 为 $\mathbb{F}_2$ 的某一个扩域上的 p 阶本原单位根满足：当 $p \equiv \pm 1 \pmod 8$ 时，$D_0^{(2)}(\beta) = 0$；当 $p \equiv \pm 3 \pmod 8$ 时，$D_0^{(2)}(\beta) = \omega$，其中 $\omega \in \mathbb{F}_4 \setminus \mathbb{F}_2$。那么，式(1)定义的 Legendre 序列 (s_u) 的对应于 β 的 Mattson-Solomon 多项式为

$$G(X) = \begin{cases} D_0^{(2)}(X), & p \equiv 1 \pmod 8 \\ D_1^{(2)}(X) + 1, & p \equiv -1 \pmod 8 \\ \omega D_0^{(2)}(X) + \omega^2 D_1^{(2)}(X) + 1, & p \equiv 3 \pmod 8 \\ \omega^2 D_0^{(2)}(X) + \omega D_1^{(2)}(X), & p \equiv -3 \pmod 8 \end{cases}$$

需要说明的是，当 $p \equiv \pm 1 \pmod 8$ 时，选择 $D_0^{(2)}(\beta) = 1$；当 $p \equiv \pm 3 \pmod 8$ 时，选择 $D_0^{(2)}(\beta) = \omega^2 \in \mathbb{F}_4$。这样虽然得到不同形式的 $G(x)$，但是并

不影响本文的讨论结果。

证明 由引理 1 可得式(1)定义的 Legendre 序列 (s_u) 的 Mattson-Solomon 多项式为

$$G(X)=\begin{cases}\mathcal{C}_1^{(2)}(\beta)\mathcal{C}_0^{(2)}(X), & p\equiv 1\ (\mathrm{mod}\ 4)\\ \mathcal{C}_0^{(2)}(\beta)\mathcal{C}_0^{(2)}(X)+1, & p\equiv 3\ (\mathrm{mod}\ 4)\end{cases}=$$

$$\begin{cases}D_1^{(2)}(\beta)D_0^{(2)}(X)+D_0^{(2)}(\beta)D_1^{(2)}(X), & p\equiv 1(\mathrm{mod}\ 4)\\ D_0^{(2)}(\beta)D_0^{(2)}(X)+D_1^{(2)}(\beta)D_1^{(2)}(X)+1, & p\equiv 3(\mathrm{mod}\ 4)\end{cases}$$

显然，在已知条件 $D_0^{(2)}(\beta)$ 的取值假设下，当 $p\equiv 1\ (\mathrm{mod}\ 4)$ 时，易知

$$G(\beta^u)=\begin{cases}0, & u\in D_0^{(2)}\\ 1, & u\in D_1^{(2)}\\ \dfrac{p-1}{2}=0, & p\mid u\end{cases}$$

即 $s_u=G(\beta^u)$，当 $u\geqslant 0$。对于 $p\equiv 3\ (\mathrm{mod}\ 4)$ 的情况可类似验证。

证毕。

由式(7)可得如下结论。

推论 1[3] 由式(1)定义的 Legendre 序列 (s_u) 的线性复杂度为

$$\mathrm{LC}((s_u))=\begin{cases}\dfrac{p-1}{2}, & p\equiv 1\ (\mathrm{mod}\ 8)\\ \dfrac{p+1}{2}, & p\equiv -1\ (\mathrm{mod}\ 8)\\ p, & p\equiv 3\ (\mathrm{mod}\ 8)\\ p-1, & p\equiv -3\ (\mathrm{mod}\ 8)\end{cases}$$

对于 $r=4$ 的情况，由 $4\mid(p-1)$，则 p 满足 $p\equiv 1\ (\mathrm{mod}\ 8)$ 或 $p\equiv -3\ (\mathrm{mod}\ 8)$。由引理 1 可知，由式(2)定义的 Ding-Helleseth-Lam 序列 (s_u) 的 Mattson-Solomon 多项式如下所示。

当 $p\equiv 1\ (\mathrm{mod}\ 8)$ 时，

$$G(X)=\mathcal{C}_0^{(4)}(\beta)\mathcal{C}_0^{(4)}(X)+\mathcal{C}_1^{(4)}(\beta)\mathcal{C}_1^{(4)}(X)=$$
$$(D_0^{(4)}(\beta)+D_1^{(4)}(\beta))D_0^{(4)}(X)+(D_1^{(4)}(\beta)+D_2^{(4)}(\beta))D_1^{(4)}(X)+$$
$$(D_2^{(4)}(\beta)+D_3^{(4)}(\beta))D_2^{(4)}(X)+(D_3^{(4)}(\beta)+D_0^{(4)}(\beta))D_3^{(4)}(X)$$

当 $p\equiv -3\ (\mathrm{mod}\ 8)$ 时，

$$G(X)=\mathcal{C}_0^{(4)}(\beta)\mathcal{C}_2^{(4)}(X)+\frac{p-1}{4}+$$
$$\mathcal{C}_0^{(4)}(\beta)\mathcal{C}_1^{(4)}(X)+\frac{p-1}{4}=$$
$$(D_2^{(4)}(\beta)+D_3^{(4)}(\beta))D_0^{(4)}(X)+(D_3^{(4)}(\beta)+D_0^{(4)}(\beta))D_1^{(4)}(X)+$$
$$(D_0^{(4)}(\beta)+D_1^{(4)}(\beta))D_2^{(4)}(X)+(D_1^{(4)}(\beta)+D_2^{(4)}(\beta))D_3^{(4)}(X)$$

另外，注意到 $\sum_{i=0}^{3}D_i^{(4)}(\beta)=1$，易证对于 $0\leqslant i<4$ 有

$$(D_i^{(4)}(\beta)+D_{i+1}^{(4)}(\beta))^2=$$
$$\begin{cases}D_i^{(4)}(\beta)+D_{i+1}^{(4)}(\beta), & 2\in D_0^{(4)}\\ 1+D_i^{(4)}(\beta)+D_{i+1}^{(4)}(\beta), & 2\in D_2^{(4)}\end{cases}$$

和

$$(D_i^{(4)})(\beta)+(D_{i+1}^{(4)})(\beta)^4=$$
$$1+D_i^{(4)}(\beta)+D_{i+1}^{(4)}(\beta),\ 2\in D_1^{(4)}\cup D_3^{(4)}$$

因此，可得

$$D_i^{(4)}(\beta)+D_{i+1}^{(4)}(\beta)\in\begin{cases}\mathbb{F}_2, 2\in D_0^{(4)}\\ \mathbb{F}_4/\mathbb{F}_2, 2\in D_2^{(4)}\\ \mathbb{F}_{16}/\mathbb{F}_8, 2\in D_1^{(4)}\cup D_3^{(4)}\end{cases}$$

其中，$0\leqslant i\leqslant 4$。

注意到，若 $p\equiv 1\ (\mathrm{mod}\ 8)$，则 $2\in D_0^{(4)}\cup D_2^{(4)}$（即 2 是模 p 的平方剩余），有 $D_0^{(4)}(\beta)+D_2^{(4)}(\beta)\in\mathbb{F}_2$。综上所述，可得命题 3。

命题 3 设 β 为 $\mathbb{F}_2$ 的某一个扩域上的 p 阶本原单位根。

1) 若 $p\equiv 1\ (\mathrm{mod}\ 8)$，令 $D_0^{(4)}(\beta)+D_2^{(4)}(\beta)=0$，则由式(2)定义的 Ding-Helleseth-Lam 序列 (s_u) 对应于 β 的 Mattson-Solomon 多项式 $G(x)$ 如下。

若 $2\in D_0^{(4)}$ 且 $D_0^{(4)}(\beta)+D_1^{(4)}(\beta)=0$，则

$$G(X)=D_2^{(4)}(X)+D_3^{(4)}(X)$$

若 $2\in D_2^{(4)}$ 且 $D_0^{(4)}(\beta)+D_1^{(4)}(\beta)=\omega\in\mathbb{F}_4\setminus\mathbb{F}_2$，则 $\tilde{G}(X)=G(X)+G_k(X),=\omega D_0^{(4)}(X)+\omega D_1^{(4)}(X)+(1+\omega)D_2^{(4)}(X)+(1+\omega)D_3^{(4)}(X)$。

2) 若 $p\equiv -3\ (\mathrm{mod}\ 8)$，令 $D_0^{(4)}(\beta)+D_1^{(4)}(\beta)=\theta\in\mathbb{F}_{16}$ 且 $\theta^4=1+\theta$，则由式(2)定义的 Ding-Helleseth-Lam 序列 (s_u) 对应于 β 的 Mattson-Solomon 多项式 $G(x)$ 如下。

若 $2\in D_1^{(4)}$，则

$$G(X)=(1+\theta)D_0^{(4)}(X)+(1+\theta^2)D_1^{(4)}(X)+\theta D_2^{(4)}(X)+\theta^2D_3^{(4)}(X),$$

若 $2\in D_3^{(4)}$，则

$$G(X)=(1+\theta)D_0^{(4)}(X)+\theta^2D_1^{(4)}(X)+\theta D_2^{(4)}(X)+(1+\theta^2)D_3^{(4)}(X)$$

在命题 3 中，当 $p\equiv 1\ (\mathrm{mod}\ 8)$ 时，若选择 $D_0^{(4)}(\beta)+D_2^{(4)}(\beta)$ 和 $D_0^{(4)}(\beta)+D_1^{(4)}(\beta)$ 的其他取值，虽然得到不同形式的 $G(x)$，但是并不影响讨论结果。

推论 2[5]　由式(2)定义的 Ding-Helleseth-Lam 序列 (s_u) 的线性复杂度为

$$\mathrm{LC}((s_u))=\begin{cases}\dfrac{p-1}{2}, & 2\in D_0^{(4)}\\ p-1, & \text{其他}\end{cases}$$

对于 Hall 六次剩余序列，由于 $p=4x^2+27$，则有 $p\equiv -1\ (\mathrm{mod}\ 8)$ 或 $p\equiv 3\ (\mathrm{mod}\ 8)$。

此外，若 $p\equiv -1\ (\mathrm{mod}\ 8)$，那么由[6, Lemma 2]，可知 $D_0^{(6)}(\beta)+D_3^{(6)}(\beta)$、$D_1^{(6)}(\beta)+D_4^{(6)}(\beta)$ 和 $D_2^{(6)}(\beta)+D_5^{(6)}(\beta)$ 中有一个值为 1，其他 2 个值为 0，其中 β 是 $\mathbb{F}_2$ 的某一个扩域的 p 阶本原单位根。由[6, Theorem 1]，存在 β 使得 $D_0^{(6)}(\beta)+D_1^{(6)}(\beta)+D_3^{(6)}(\beta)=1$，对同一个 β，由[6, Theorem 1]的证明可得式(9)。

$$D_1^{(6)}(\beta)=D_2^{(6)}(\beta)=D_5^{(6)}(\beta)=1,\ \text{且}$$
$$D_0^{(6)}(\beta)=D_3^{(6)}(\beta)=D_4^{(6)}(\beta)=0 \tag{9}$$

若 $p\equiv 3\ (\mathrm{mod}\ 8)$，类似地，由[6, Lemma 1]，可知 $D_0^{(6)}(\beta)+D_3^{(6)}(\beta)$、$D_1^{(6)}(\beta)+D_4^{(6)}(\beta)$ 和 $D_2^{(6)}(\beta)+D_5^{(6)}(\beta)$ 中有一个值为 1，而其他 2 个值为 0。事实上，此时 $2\in D_3^{(6)}$，则有 $(D_i^{(6)}(\beta)+D_{i+3}^{(6)}(\beta))^2=D_i^{(6)}(\beta)+D_{i+3}^{(6)}(\beta)$，其中 $i=0,1,2$。注意到

$$\sum_{i=0}^{5}D_i^{(6)}(\beta)=1$$

若 $D_0^{(6)}(\beta)+D_3^{(6)}(\beta)=D_1^{(6)}(\beta)+D_4^{(6)}(\beta)=D_2^{(6)}(\beta)+D_5^{(6)}(\beta)=1$，则导出矛盾。因此，设 $D_1^{(6)}(\beta)+D_4^{(6)}(\beta)=1$，且 $D_0^{(6)}(\beta)+D_3^{(6)}(\beta)=D_2^{(6)}(\beta)+D_5^{(6)}(\beta)=0$。注意到，$D_0^{(6)}(\beta),D_2^{(6)}(\beta),D_3^{(6)}(\beta),D_5^{(6)}(\beta)\in\mathbb{F}_2$ 且 $D_1^{(6)}(\beta),D_4^{(6)}(\beta)\in\mathbb{F}_4\setminus\mathbb{F}_2$。与[6, Theorem 1]的证明类似，有

$$\begin{cases}D_1^{(6)}(\beta)=\omega\in\mathbb{F}_4\setminus\mathbb{F}_2\\ D_4^{(6)}(\beta)=1+\omega\\ D_0^{(6)}(\beta)=D_3^{(6)}(\beta)=1\\ D_2^{(6)}(\beta)=D_5^{(6)}(\beta)=0\end{cases} \tag{10}$$

则由引理 1，可得命题 4。

命题 4　设 β 是 $\mathbb{F}_2$ 的某个扩域上的 p 阶本原单位根，且当 $p\equiv -1\ (\mathrm{mod}\ 8)$ 时，β 满足式(9)；而当 $p\equiv 3\ (\mathrm{mod}\ 8)$ 时，β 满足式(10)，则由式(3)定义的 Hall 六次剩余序列 (s_u) 对应于 β 的 Mattson-Solomon 多项式如下所示。

若 $p\equiv -1\ (\mathrm{mod}\ 8)$，则 $G(X)=1+D_3^{(6)}(X)$，

若 $p\equiv 3\ (\mathrm{mod}\ 8)$，则

$$G(X)=1+(1+\omega)D_0^{(6)}(X)+D_1^{(6)}(X)+D_2^{(6)}(X)+\omega D_3^{(6)}(X)+D_4^{(6)}(X)+D_5^{(6)}(X)$$

推论 3[6]　由式(3)定义的 Hall 六次剩余序列 (s_u) 的线性复杂度为

$$LC((s_u))=\begin{cases}1+\dfrac{p-1}{6}, & p\equiv -1\ \ (\mathrm{mod}\ \ 8)\\ p, & p\equiv 3\ \ (\mathrm{mod}\ \ 8)\end{cases}$$

3　k-错线性复杂度

由式(5)可知，周期为 p 的二元序列 (s_u) 的 k-错线性复杂度是指在改变序列 (s_u) 的第一个周期中至多 k 项后（随后的其他周期中做相同改变），可得序列 $(\tilde{s}_u)$ 的最小线性复杂度，即

$$\tilde{s}_u=s_u+e_u\ (\mathrm{mod}\ \ 2), u\geqslant 0,$$

其中，(e_u) 为一个错误序列满足 $W_H((e_u))\leqslant k$。受到文献[33-34]的启发，下面给出使用 (e_u) 的离散傅里叶变换求序列的 k-错线性复杂度的方法。

设 $G(x)$、$G_k(X)$ 和 $\tilde{G}(X)$ 分别是 (s_u)、(e_u) 和 $(\tilde{s}_u)$ 的 Mattson-Solomon 多项式。记

$$G(X)=\sum_{0\leqslant i<p}\rho_i X^i$$
$$G_k(X)=\sum_{0\leqslant i<p}\eta_i X^i$$
$$\tilde{G}(X)=\sum_{0\leqslant i<p}\xi_i X^i$$

由式(8)知 $\tilde{G}(X)=G(X)+G_k(X)$, 则有

$$\xi_i=\rho_i+\eta_i, 0\leqslant i<p \tag{11}$$

由式(7)可知，序列 $(\tilde{s}_u)$ 的线性复杂度 $\mathrm{LC}((\tilde{s}_u))=\#\{i:\xi_i\neq 0, 0\leqslant i<p\}$。只要知道 ρ_i，则可计算得到 η_i，并由式(11)确定式(12)是否成立

$$\#\{i:\xi_i\neq 0,0\leqslant i<p\}<\#\{i:\rho_i\neq 0,0\leqslant i<p\} \tag{12}$$

由此证明，序列 (s_u) 在改变若干项之后其线性复杂度降低了。

3.1　1-错线性复杂度

命题 5　由式(1)定义的 Legendre 序列 (s_u) 在 $\mathbb{F}_2$ 上的 1-错线性复杂度如下

$$\mathrm{LC}_1((s_u))=\begin{cases}\dfrac{p-1}{2}, & p\equiv\pm 1\ (\mathrm{mod}\ \ 8)\\ p-1, & p\equiv\pm 3\ (\mathrm{mod}\ \ 8)\end{cases}$$

证明　不妨设错误序列 (e_u) 的第一个周期中对某个 $0\leqslant u_0<p$ 满足 $e_{u_0}=1$，而对其他 $0\leqslant u\neq$

$u_0 < p$ 满足 $e_u = 0$。(e_u) 的离散傅里叶变换为 $\eta_i = \beta^{iu_0}, 0 \leqslant i < p$。特别地，若 $u_0 = 0$，则对所有的 $0 \leqslant i < p$ 有 $\eta_i = 1$；否则，$\eta_0 = 1$ 且对所有的 $1 \leqslant i < p$ 有 η_i 的阶为 p。

下面考虑 $p \equiv -1 \pmod 8$ 的情况。由命题 2 和式(11)，可得

$$\xi_i = \rho_i + \eta_i = \begin{cases} \beta^{iu_0}, & i \in D_0^{(2)} \\ 1 + \beta^{iu_0}, & i \in D_1^{(2)} \\ 0, & i = 0 \end{cases}$$

若 $u_0 \neq 0$，则对所有的 $1 \leqslant i < p$ 有 $\xi_i \neq 0$，且修改后的序列 $(\tilde{s}_u)$ 的线性复杂度满足 $LC((\tilde{s}_u)) = p - 1 > LC((s_u))$。而当 $u_0 = 0$ 时，有

$$\mathrm{LC}((\tilde{s}_u)) = \frac{p-1}{2} < LC((s_u)) = \frac{p+1}{2}$$

这说明若改变序列 (s_u) 的第一项 s_0 的值后，其线性复杂度从 $\frac{p+1}{2}$ 降低为 $\frac{p-1}{2}$。这就证明了第一种情况，而对于其他 3 种情况的证明方法类似。

证毕。

用命题 5 的证明方法，可以得到下面 2 个结论。

命题 6 由式(2)定义的 Ding-Helleseth-Lam 序列 (s_u) 在 $\mathbb{F}_2$ 上的 1-错线性复杂度为

$$\mathrm{LC}_1((s_u)) = \begin{cases} \dfrac{p-1}{2}, & 2 \in D_0^{(4)} \\ p-1, & \text{其他} \end{cases}$$

命题 7 由式(3)定义的 Hall 六次剩余序列 (s_u) 在 $\mathbb{F}_2$ 上的 1-错线性复杂度为

$$\mathrm{LC}_1((s_u)) = \begin{cases} 1 + \dfrac{p-1}{6}, & p \equiv -1 \pmod 8 \\ \dfrac{p-1}{3}, & p \equiv 3 \pmod 8 \end{cases}$$

3.2 *k*-错线性复杂度：几个特殊情况

对于 $k \geqslant 2$ 的情况，要确定 Legendre 序列、Ding-Helleseth-Lam 序列和 Hall 六次剩余序列的 k-错线性复杂度是不容易的。但是，在一些特定的条件下可以得到部分结果。通过错误序列 (e_u) 的离散傅里叶变换 $(\eta_0, \eta_1, \cdots, \eta_{p-1})$ 的适当取值，并通过式(11)使得式(13)成立。

$$\#\{i : \xi_i \neq 0, 0 \leqslant i < p\} < \#\{i : \rho_i \neq 0, 0 \leqslant i < p\} \quad (13)$$

也就是说，改变序列 (s_u) 的 $W_H((e_u))$ 项可使其线性复杂度降低。然后，从 $(\eta_0, \eta_1, \cdots, \eta_{p-1})$ 中计算得到 (e_u)，从而得到 $W_H((e_u))$，即 k 的值。

假设 $\mathrm{ord}_p(2) = \dfrac{p-1}{d}$，并定义

$$T_0 = \langle 2 \rangle = \{2^j \pmod p : 0 \leqslant j < \frac{p-1}{d}\}$$

$T_i = g^i T_0 = \{g^i 2^j \pmod p : 0 \leqslant j < \mathrm{ord}_p(2)\}$，$1 \leqslant i < d$ 其中 g 为第 1 节中定义的模 p 的本原元。令

$$T_i(X) = \sum_{u \in T_i} X^u \in \mathbb{F}_2[X]$$

设 ℓ_i 表示集合 T_i 中的最小元素值（也称为陪集首元），其中 $0 \leqslant i < d$。对于一个二元序列的离散傅里叶变换为 $(\phi_0, \phi_1, \cdots, \phi_{p-1})$，有 $\phi_0 \in \mathbb{F}_2$，并定义 $(\phi_0, \phi_1, \cdots, \phi_{p-1})$ 的 DFT-leader-vector 为 $[\phi_0; \phi_{\ell_0}, \phi_{\ell_1}, \cdots, \phi_{\ell_{d-1}}]$。

由上述 T_0 的定义易知，DFT-leader-vector 是由 $(\phi_0, \phi_1, \cdots, \phi_{p-1})$ 唯一确定的，反之亦然。具体地，若 $\phi_{\ell_i} = a \in \mathbb{F}_{2^{\frac{p-1}{d}}}$，则 $\phi_{2^j \ell_i \pmod p} = a^{2^j}$，其中 $0 \leqslant i < d$。

若 $\mathrm{ord}_p(2) = \dfrac{p-1}{2}$ 或 $\dfrac{4}{p-1}$，下面先证明 Legendre 序列的 k-错线性复杂度的部分结果。若 $\mathrm{ord}_p(2) = p-1$，由推论 1、命题 1 和命题 5 可得如下结论。

当 $p \equiv -3 \pmod 8$ 时，

$$\mathrm{LC}_k((s_u)) = \begin{cases} p-1, & 0 \leqslant k < \dfrac{p-1}{2} \\ 0, & k \geqslant \dfrac{p-1}{2} \end{cases}$$

当 $p \equiv 3 \pmod 8$ 时，

$$\mathrm{LC}_k((s_u)) = \begin{cases} p, & k = 0 \\ p-1, & 1 \leqslant k < \dfrac{p-1}{2} \\ 0, & k \geqslant \dfrac{p-1}{2} \end{cases}$$

命题 8 设 $\mathrm{ord}_p(2) = \dfrac{p-1}{2}$，则由式(1)定义的 Legendre 序列在 $\mathbb{F}_2$ 上的 k-错线性复杂度如下。

当 $p \equiv 1 \pmod 8$ 时，

$$\mathrm{LC}_k((s_u))=\begin{cases}\dfrac{p-1}{2}, & 0\leqslant k<\dfrac{p-1}{2}\\ 0, & k\geqslant\dfrac{p-1}{2}\end{cases}$$

当 $p\equiv -1\,(\mathrm{mod}\ 8)$ 时，

$$\mathrm{LC}_k((s_u))=\begin{cases}\dfrac{p+1}{2}, & k=0\\ \dfrac{p-1}{2}, & 1\leqslant k<\dfrac{p-1}{2}\\ 0, & k\geqslant\dfrac{p-1}{2}\end{cases}$$

证明　由于 $\mathrm{ord}_p(2)=\dfrac{p-1}{2}$，2 是模 p 的平方剩余，因此，$p\equiv 1\,(\mathrm{mod}\ 8)$ 或 $p\equiv -1\,(\mathrm{mod}\ 8)$。那么，由推论 1、命题 1 和命题 5 即得所要结果。

命题 9　设 $\mathrm{ord}_p(2)=\dfrac{p-1}{4}$，则由式(1)定义的 Legendre 序列在 $\mathbb{F}_2$ 上的 k-错线性复杂度如下

$$\mathrm{LC}_k((s_u))=\begin{cases}\dfrac{p-1}{2}, & 0\leqslant k\leqslant 1\\ \dfrac{p-1}{4}, & \dfrac{p-1}{4}\leqslant k<\dfrac{p-1}{2}\\ 0, & k\geqslant\dfrac{p-1}{2}\end{cases}$$

或

$$\mathrm{LC}_k((s_u))=\begin{cases}\dfrac{p-1}{2}, & 0\leqslant k\leqslant 1\\ 1+\dfrac{p-1}{4}\text{或}\dfrac{p-1}{4}, & 1+\dfrac{p-1}{4}\leqslant k<\dfrac{p-1}{2}\\ 0, & k\geqslant\dfrac{p-1}{2}\end{cases}$$

证明　由 $\mathrm{ord}_p(2)=\dfrac{p-1}{4}, 2\in D_0^{(2)}$，则 $p\equiv 1\,(\mathrm{mod}\ 8)$。另外，根据上述定义的 T_i，有 $D_0^{(2)}=T_0\cup T_2$，$D_1^{(2)}=T_1\cup T_3$ 和 $T_i(\beta)\in\mathbb{F}_2$，其中 $0\leqslant i<4$。由命题 2 中假设的 $D_0^{(2)}(\beta)=0$，有 $T_0(\beta)=T_2(\beta)=1$ 或 $T_0(\beta)=T_2(\beta)=0$。

再由命题 2，序列 (s_u) 的离散傅里叶变换 $(\rho_0,\rho_1,\cdots,\rho_{p-1})$ 的 DFT-leader-vector 是 $[0;1,0,1,0]$。为了使 (s_u) 的 k-错线性复杂度降低，即使序列 $(\tilde{s}_u)$ 的离散傅里叶变换 $(\xi_0,\xi_1,\cdots,\xi_{p-1})$ 满足

$$\#\{i:\xi_i\neq 0, 0\leqslant i<p\}<\#\{i:\rho_i\neq 0, 0\leqslant i<p\}$$

由式(11)可知，错误序列 (e_u) 的离散傅里叶变换 $(\eta_0,\eta_1,\cdots,\eta_{p-1})$ 的 DFT-leader-vector 有以下几种情况。

$$[\eta_0;1,0,a,0],[\eta_0;b,0,1,0],[\eta_0;1,c,1,0],[\eta_0;1,0,1,d]$$

其中 $\eta_0\in\mathbb{F}_2$，$a,b\in\mathbb{F}_{2^{(p-1)/4}}\setminus\{1\}$ 和 $c,d\in\mathbb{F}_{2^{(p-1)/4}}\setminus\{0\}$。

取序列 (e_u) 的离散傅里叶变换 $(\eta_0,\eta_1,\cdots,\eta_{p-1})$ 的 DFT-leader-vector 为 $[\eta_0;1,1,1,0]$，序列 (s_u) 的线性复杂度从 $\dfrac{p-1}{2}$ 降低为 $\eta_0+\dfrac{p-1}{4}$，则可通过如下计算得到 (e_u)。

$$e_u=\sum_{0\leqslant i<p}\eta_i\beta^{ui}=\eta_0+T_0(\beta^u)+T_1(\beta^u)+T_2(\beta^u)=$$

$$\eta_0+D_0^{(2)}(\beta^u)+T_1(\beta^u)=$$

$$\begin{cases}\eta_0+D_0^{(2)}(\beta)+T_1(\beta), & u\in T_0\\ \eta_0+D_1^{(2)}(\beta)+T_2(\beta), & u\in T_1\\ \eta_0+D_0^{(2)}(\beta)+T_3(\beta), & u\in T_2\\ \eta_0+D_1^{(2)}(\beta)+T_0(\beta), & u\in T_3\\ \eta_0+\dfrac{p-1}{2}+\dfrac{p-1}{4}, & u=0\end{cases}=$$

$$\begin{cases}\eta_0+T_1(\beta), & u\in T_0\\ \eta_0+1+T_2(\beta), & u\in T_1\\ \eta_0+T_3(\beta), & u\in T_2\\ \eta_0+1+T_0(\beta), & u\in T_3\\ \eta_0, & u=0\end{cases}$$

若命题 2 中选择的 β 满足 $T_0(\beta)=T_2(\beta)=1$，则设 $\eta_0=0$。由于 $D_1^{(2)}(\beta)=1=T_1(\beta)+T_3(\beta)$，则有 $W_H((e_u))=\dfrac{p-1}{4}$，因此 $T_1(\beta)=0$ 且 $T_3(\beta)=1$，或 $T_1(\beta)=1$ 且 $T_3(\beta)=0$。可得

$$\mathrm{LC}_{\frac{p-1}{4}}((s_u))\leqslant\frac{p-1}{4},$$

由此完成了第一种情况的证明。

若命题 2 中选择的 β 满足 $T_0(\beta)=T_2(\beta)=0$，选择 $\eta_0=1$，则可计算得到满足 $W_H((e_u))=1+\dfrac{p-1}{4}$ 的错误序列 (e_u)，进而有 $\mathrm{LC}_{1+\frac{p-1}{4}}((s_u))\leqslant 1+\dfrac{p-1}{4}$。由命题 1 可完成第二种情况的证明。

证毕。

下面考虑由式(2)定义的 Ding-Helleseth-Lam 序列 (s_u)。若 $\mathrm{ord}_p(2)=p-1$，则有 $2\in D_1^{(4)}\cup D_3^{(4)}$。由推论 2、命题 1 和命题 3 可得

$$\mathrm{LC}_k((s_u))=\begin{cases}p-1, & 0\leqslant k<\dfrac{p-1}{2}\\ 0, & k\geqslant\dfrac{p-1}{2}\end{cases}$$

命题 10　设 $\mathrm{ord}_p(2)=\dfrac{p-1}{2}$，由式(2)定义的 Ding-Helleseth-Lam 序列 (s_u) 在 $\mathbb{F}_2$ 上的 k-错线性复杂度为

$$\mathrm{LC}_k((s_u))=\begin{cases}p-1, & 0\leqslant k\leqslant 1\\ \dfrac{p-1}{2}, & \dfrac{p-1}{4}\leqslant k<\dfrac{p-1}{2}\\ 0, & k\geqslant\dfrac{p-1}{2}\end{cases}$$

或

$$\mathrm{LC}_k((s_u))=\begin{cases}p-1, & 0\leqslant k\leqslant 1\\ 1+\dfrac{p-1}{2}\text{或}\dfrac{p-1}{2}, & 1+\dfrac{p-1}{4}\leqslant k<\dfrac{p-1}{2}\\ 0, & k\geqslant\dfrac{p-1}{2}\end{cases}$$

证明　由命题 3 可知，(s_u) 的离散傅里叶变换为

$$\rho_i=\begin{cases}\omega, & i\in D_0^{(4)}\\ \omega, & i\in D_1^{(4)}\\ 1+\omega, & i\in D_2^{(4)}\\ 1+\omega, & i\in D_3^{(4)}\\ 0, & i=0\end{cases}$$

取 (e_u) 的离散傅里叶变换 $(\eta_0,\eta_1,\cdots,\eta_{p-1})$ 为

$$\eta_i=\begin{cases}\omega, & i\in D_0^{(4)}\\ 0, & i\in D_1^{(4)}\\ 1+\omega, & i\in D_2^{(4)}\\ 0, & i\in D_3^{(4)}\\ \delta, & i=0\end{cases}$$

其中，$\delta\in\mathbb{F}_2$。通过如下方式计算得到 (e_u)。

$$e_u=\sum_{0\leqslant i<p}\eta_i\beta^{ui}=\delta+\omega D_0^{(4)}(\beta^u)+(1+\omega)D_2^{(4)}(\beta^u)=$$

$$\delta+\begin{cases}\omega D_0^{(4)}(\beta)+(1+\omega)D_2^{(4)}(\beta), & u\in D_0^{(4)}\\ \omega D_1^{(4)}(\beta)+(1+\omega)D_3^{(4)}(\beta), & u\in D_1^{(4)}\\ \omega D_2^{(4)}(\beta)+(1+\omega)D_0^{(4)}(\beta), & u\in D_2^{(4)}\\ \omega D_3^{(4)}(\beta)+(1+\omega)D_1^{(4)}(\beta), & u\in D_3^{(4)}\\ \omega\dfrac{p-1}{4}+(1+\omega)\dfrac{p-1}{4}, & u=0\end{cases}$$

由于 $\mathrm{ord}_p(2)=\dfrac{p-1}{2}$，则 $p\equiv 1 \bmod 8$ 且 $2\in D_2^{(4)}$。由命题 3 的假设，则有式(14)或式(15)成立。

$$D_0^{(4)}(\beta)=D_2^{(4)}(\beta)=0, D_1^{(4)}(\beta)=\omega\in\mathbb{F}_4\setminus\mathbb{F}_2,$$
$$D_3^{(4)}(\beta)=1+\omega \tag{14}$$

$$D_0^{(4)}(\beta)=D_2^{(4)}(\beta)=1, D_1^{(4)}(\beta)=1+\omega,$$
$$D_3^{(4)}(\beta)=\omega \tag{15}$$

若命题 3 中选择的 β 满足式(14)，则选择 $\delta=0$，使 $W_H((e_u))=\dfrac{p-1}{4}$，则有 $\mathrm{LC}_{\frac{p-1}{2}}((s_u))\leqslant\dfrac{p-1}{2}$。再由命题 1 即可完成第一种情况的证明。

若命题 3 中选择的 β 满足式(13)，则选择 $\eta_0=1$ 和 $\delta=0$，使 $W_H((e_u))=1+\dfrac{p-1}{4}$，则有 $\mathrm{LC}_{1+\frac{p-1}{2}}((s_u))\leqslant 1+\dfrac{p-1}{2}$。再由命题 1 即可完成第二种情况的证明。证毕。

命题 11　设 $\mathrm{ord}_p(2)=\dfrac{p-1}{4}$，则由式(2)定义的 Ding-Helleseth-Lam 序列 (s_u) 在 $\mathbb{F}_2$ 上的 k-错线性复杂度为

$$\mathrm{LC}_k((s_u))=\begin{cases}\dfrac{p-1}{2}, & 0\leqslant k\leqslant 1\\ \dfrac{p-1}{4}, & \dfrac{p-1}{4}\leqslant k<\dfrac{p-1}{2}\\ 0, & k\geqslant\dfrac{p-1}{2}\end{cases}$$

或

$$\mathrm{LC}_k((s_u))=\begin{cases}\dfrac{p-1}{2}, & 0\leqslant k\leqslant 1\\ 1+\dfrac{p-1}{4}\text{或}\dfrac{p-1}{4}, & 1+\dfrac{p-1}{4}\leqslant k<\dfrac{p-1}{2}\\ 0, & k\geqslant\dfrac{p-1}{2}\end{cases}$$

证明　由于 $\mathrm{ord}_p(2)=\dfrac{p-1}{4}$，则有 $2\in D_0^{(4)}$ 且 $T_i=D_i^{(4)}$，其中 $0\leqslant i<4$。容易验证每个 $T_i(\beta)\in\mathbb{F}_2$ 且在命题 3 的假设下，若 $D_0^{(4)}(\beta)+D_1^{(4)}(\beta)=0$，则式(16)或式(17)成立。

$$T_i(\beta)=\begin{cases}0, & i=0\\ 0, & i=1\\ 0, & i=2\\ 1, & i=3\end{cases} \tag{16}$$

$$T_i(\beta)=\begin{cases}1, & i=0\\ 1, & i=1\\ 1, & i=2\\ 0, & i=3\end{cases} \tag{17}$$

再由命题 3 可知，(s_u) 的 DFT-leader-vector 为 $[0;0,0,1,1]$。仿照命题 9 的证明，通过式(16)选择错误序列 (e_u) 的离散傅里叶变换 $(\eta_0,\eta_1,\cdots,\eta_{p-1})$ 的 DFT-leader-vector 为 $[0;0,0,1,0]$，或通过式(17)则选为 $[1;0,0,1,0]$。 通过类似的计算，即得所要证明的结果。

证毕。

最后，考虑由式(3)定义的 Hall 六次剩余序列 (s_u) 的 k-错线性复杂度。由[6, Lemma 1]知，当 $p\equiv -1 \pmod 8$ 时，$2\in D_0^{(6)}$；当 $p\equiv 3 \pmod 8$ 时，$2\in D_3^{(6)}$。因此，当 $p\equiv -1 \pmod 8$ 时，$\mathrm{ord}_p(2)\leqslant \dfrac{p-1}{6}$；当 $p\equiv 3 \pmod 8$ 时，$\mathrm{ord}_p(2)\leqslant \dfrac{p-1}{3}$。下面分析 $\mathrm{ord}_p(2)$ 取最大的情况。

命题 12　由式(3)定义的 Hall 六次剩余序列 (s_u) 在 $\mathbb{F}_2$ 上的 k-错线性复杂度如下。

若 $p\equiv -1 \pmod 8$ 且 $\mathrm{ord}_p(2)=\dfrac{p-1}{6}$，则有

$$\mathrm{LC}_k((s_u))=\begin{cases}1+\dfrac{p-1}{6}, & 0\leqslant k\leqslant 1\\ \dfrac{p-1}{6}, & 1+\dfrac{p-1}{3}\leqslant k<\dfrac{p-1}{2}\\ 0, & k\geqslant \dfrac{p-1}{2}\end{cases}$$

若 $p\equiv 3 \pmod 8$ 且 $\mathrm{ord}_p(2)=\dfrac{p-1}{3}$，则有

$$\mathrm{LC}_k((s_u))=\begin{cases}p-1, & k=0\\ \dfrac{p-1}{3}, & 1\leqslant k<\dfrac{p-1}{2}\\ 0, & k\geqslant \dfrac{p-1}{2}\end{cases}$$

证明　当 $p\equiv -1 \pmod 8$ 时，由命题 4 可知，(s_u) 的离散傅里叶变换 $(\rho_0,\rho_1,\cdots,\rho_{p-1})$ 的 DFT-leader-vector 为 $[1;0,0,0,1,0,0]$。选择错误序列 (e_u) 的离散傅里叶变换 $(\eta_0,\eta_1,\cdots,\eta_{p-1})$ 的 DFT-leader-vector 为 $[1;0,0,1,1,0,0]$，则可计算得出 e_u。

$$e_u=\begin{cases}0, & u\in D_0^{(6)}\cup D_1^{(6)}\cup D_3^{(6)}\cup D_5^{(6)}\\ 1, & u\in D_2^{(6)}\cup D_4^{(6)}\\ 1, & u=0\end{cases}$$

因此，可以找到一个错误序列 (e_u) 满足 $W_H((e_u))=1+\dfrac{p-1}{3}$ 使得序列 (s_u) 的线性复杂度从 $1+\dfrac{p-1}{6}$ 降低为 $\dfrac{p-1}{6}$。从而完成了第一种情况的证明。而对于第二种情况，则由命题 4 和命题 1 即得。

证毕。

4　结束语

本文分别利用 Legendre 序列、Ding-Helleseth-Lam 序列和 Hall 六次剩余序列的离散傅里叶变换确定这些序列的 1-错线性复杂度，并在特定条件 $\mathrm{ord}_p(2)=\dfrac{p-1}{d}$ 下得到这些序列的 k-错线性复杂度的部分结果，其中 $k>1$ 且 d 为小的正整数。

认为考虑一般的 $\mathrm{ord}_p(2)$ 和适当大的 k 的情况是一个具有挑战性的工作。若错误序列 (e_u) 的 DFT-leader-vector 为 $[a_0;a_{\ell_0},a_{\ell_1},\cdots,a_{\ell_{d-1}}]$ 满足 $a_0\in\mathbb{F}_2$ 且对其他 $0\leqslant i<d$ 有 $a_{\ell_i}\in\mathbb{F}_{2^{(p-1)/d}}$，那么 (e_u) 可通过如式(18)所示的迹函数的和计算得到。

$$e_u=a_0+\mathrm{Tr}(a_{\ell_1}\beta^{\ell_0 u})+\mathrm{Tr}(a_{\ell_2}\beta^{\ell_1 u})+\cdots+\mathrm{Tr}(a_{\ell_{d-1}}\beta^{\ell_{d-1}u}),0\leqslant u<p \tag{18}$$

其中，迹函数 $\mathrm{Tr}(\cdot)$ 是从 $\mathbb{F}_{2^{\frac{p-1}{d}}}$ 到 $\mathbb{F}_2$ 的映射。而计算该和式的最小重量 $W_H((e_u))$（即最小的 k）似乎是困难的，需要用到更多的知识。需要指出的是，迹函数在编码理论中具有广泛的应用，而文献[35]的思想可能有助于解决这个问题。

参考文献：

[1] CUSICK T, DING C, RENVALL A. Stream ciphers and number theory[M]. Elsevier, 2004.

[2] DING C. Pattern distributions of Legendre sequences[J]. IEEE Transactions on Information Theory, 1998, 44(4): 1693-1698.

[3] DING C, HELLESETH T, SHAN W. On the linear complexity of Legendre sequences[J]. IEEE Transactions on Information Theory, 1998, 44(3): 1276-1278.

[4] KIM J, SONG H. Trace representation of Legendre sequences[J]. Designs, Codes and Cryptography, 2001, 24(3): 343-348.

[5] DING C, HELLESETH T, LAM K. Several classes of binary sequences with three-level autocorrelation[J]. IEEE Transactions on Information Theory, 1999, 45(7): 2606-2612.

[6] KIM J, SONG H. On the linear complexity of Hall's sextic residue sequences[J]. IEEE Transactions on Information Theory, 2001, 47(5): 2094-2096.

[7] KIM J, SONG H, GONG G. Trace function representation of Hall's sextic residue sequences of period $p \equiv 7 (\mathrm{mod}\ 8)$[M]. NewYork: Kluwer Academic Publishers, 2003, 23-32.

[8] CAI Y, DING C. Binary sequences with optimal autocorrelation[J]. Theoretical Computer Science, 2009, 410(24-25): 2316-2322.

[9] DING C, HELLESETH T. On cyclotomic generator of orderr[J]. Information Processing Letters, 1998, 66(1): 21-25.

[10] WANG Q, LIN D, GUANG X. On the linear complexity of Legendre sequences over F_g [J]. IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences, 2014, 97(7): 1627-1630.

[11] HOFER R, WINTERHOF A. On the arithmetic autocorrelation of the Legendre sequence[J]. Advances in Mathematics of Communications, 2017, 11(1): 237-244.

[12] DU X, CHEN Z. A generalization of the Hall's sextic residue sequences[J]. Information Sciences, 2013, 222: 784-794.

[13] XIONG H, QU L, LI C. A new method to compute the 2-adic complexity of binary sequences[J]. IEEE Transactions on Information Theory, 2014, 60(4): 2399-2406.

[14] SU W, YANG Y, FAN C. New optimal binary sequences with period 4p via interleaving Ding-Helleseth-Lam sequences[J]. Designs, Codes and Cryptography, 2018, 86(6): 1329-1338.

[15] WHITEMAN A. A family of difference sets[J]. Journal of Mathematics., 1962, 6(1): 107-121.

[16] DING C, HELLESETH T. New generalized cyclotomy and its applications[J]. Finite Fields and their Applications, 1998, 4(2): 140-166.

[17] ZENG X, CAI H, TANG X, et al. Optimal frequency hopping sequences of odd length[J]. IEEE Transactions on Information Theory, 2013, 59(5): 3237-3248.

[18] 刘龙飞, 杨凯, 杨晓元. 新的周期为 p^m 的 GF(h)上广义割圆序列的线性复杂度[J]. 通信学报, 2017, 38(9): 39-45.
LIU L F,YANG K,YANG X Y. On the linear complexity of a new generalized cyclotomic sequence with length p^m over GF(h)[J]. Journal on Communications, 2017,38(9): 39-45.

[19] XIAO Z, ZENG X, LI C, et al. New generalized cyclotomic binary sequences of period p^2 [J]. Designs, Codes and Cryptography, 2018, 86(7): 1483-1497.

[20] CHEN Z, EDEMSKIY V, KE P, et al. On *k* -error linear complexity of pseudorandom binary sequences derived from Euler quotients[J]. Advances in Mathematics of Communications, 2018, 12(4): 805-816.

[21] WU C, XU C, Chen Z, et al. On error linear complexity of new generalized cyclotomic binary sequences of period p^2[J]. Information Processing Letters, 2019, 144: 9-15.

[22] CHEN Z, NIU Z, WU C. On the *k* -error linear complexity of binary sequences derived from polynomial quotients[J]. Science China Information Sciences, 2015, 58(9): 1-15.

[23] ALY H, MEIDL W, WINTERHOF A. On the *k*-error linear complexity of cyclotomic sequences[J]. Journal of Mathematical Cryptology, 2007, 1(3): 283-296.

[24] ALY H, WINTERHOF A. On the *k* -error linear complexity over F_p of Legendre and Sidel'nikov sequences[J]. Designs, Codes and Cryptography, 2006, 40(3): 369-374.

[25] DING C. Binary cyclotomic generators[C]//Fast Software Encryption-FSE'95. 1995: 29-60.

[26] STAMP M, MARTIN C. An algorithm for the *k*-error linear complexity of binary sequences with period 2^n [J]. IEEE Transactions on Information Theory, 1993, 39(4): 1398-1401.

[27] DING C, XIAO G, SHAN W. The stability theory of stream ciphers[M]. Berlin: Springer-Verlag,1991.

[28] MASSEY J. Codes and ciphers: Fourier and Blahut[M]. Boston: Springer, 1998: 105-119.

[29] MASSEY J, SERCONEK S. A Fourier transform approach to the linear complexity of nonlinearly filtered sequences[C]//Annual International Cryptology Conference. Springer. 1994: 332-340.

[30] BLAHUT R. Transform techniques for error control codes[J]. IBM Journal of Research and development, 1979, 23(3): 299-315.

[31] MACWILLIAMS F, SLOANE N. The theory of error-correcting codes[M]. Amsterdam: Elsevier, 1977.

[32] DAI Z, GONG G, SONG H, et al. Trace representation and linear complexity of binary *e* th power residue sequences of period *p* [J]. IEEE Transactions on Information Theory, 2011, 57(3): 1530-1547.

[33] ALECU A, SALAGEAN A. An approximation algorithm for computing the *k*-error linear complexity of sequences using the discrete fourier transform[C]// IEEE International Symposium on Information Theory, 2008, 2414-2418.

[34] SALAGEAN A, ALECU A. An improved approximation algorithm for computing the *k*-error linear complexity of sequences using the discrete fourier transform[C]// International Conference on Sequences and their Applications. 2010: 151-165.

[35] DING C, YANG J. Hamming weights in irreducible cyclic codes[J]. Discrete Mathematics, 2013, 313(4): 434-446.

[作者简介]

陈智雄（1972– ），男，福建莆田人，博士，莆田学院教授，主要研究方向为序列密码。

吴晨煌（1981– ），男，福建莆田人，莆田学院副教授，电子科技大学博士生，主要研究方向为序列密码。