Pure Mathematics 理论数学, 2024, 14(8), 153-161
Published Online August 2024 in Hans. https://www.hanspub.org/journal/pm
https://doi.org/10.12677/pm.2024.148313

Hans汉斯

线性化多项式核的刻画

郭嘉鑫，金　永

中国民航大学理学院，天津

收稿日期：2024年5月14日；录用日期：2024年7月29日；发布日期：2024年8月21日

摘　要

本文在总结相关文献的基础上，整理了$\mathbb{F}_{q^n}$上的线性化多项式核的多种刻画方式。首先，总结了$\mathbb{F}_q$上线性化多项式代数$\mathbb{L}\left(\mathbb{F}_q\right)$的循环矩阵刻画。接着在回顾了线性化多项式的“迹表示”后，通过“迹表示”及初等方法证明了Dickson关于线性化置换多项式的知名判定法则，并再次得到了$\mathbb{F}_{q^n}$上的线性化多项式代数与Dickson矩阵代数间的同构关系。

关键词

线性化多项式，Dickson矩阵，迹表示，循环矩阵

Characterizations of Kernel of Linearized Polynomials

Jiaxin Guo, Yong Jin

College of Science, Civil Aviation University of China, Tianjin

Received: May 14th, 2024; accepted: Jul. 29th, 2024; published: Aug. 21st, 2024

Abstract

In this paper, we summarize some characterizations of the kernel of linearized polynomials over $\mathbb{F}_{q^n}$ after reviewing related articles. Firstly, circulant matrices characterization of algebra $\mathbb{L}\left(\mathbb{F}_q\right)$ over $\mathbb{F}_q$ are summed up. Then, after reviewing the “trace representations” of linearized polynomials, we prove Dickson’s well-known decision rule for permutation linearized polynomials by elementary methods and “trace representations”, then obtain the isomorphism between linear-

文章引用: 郭嘉鑫, 金永. 线性化多项式核的刻画[J]. 理论数学, 2024, 14(8): 153-161. DOI: 10.12677/pm.2024.148313

ized polynomials algebra and Dickson matrices algebra over $\mathbb{F}_{q^n}$ again.

Keywords

Linearized Polynomial, Dickson Matrix, Trace Representation, Circulant Matrix

1. 引言

设 $\mathbb{F}_q$ 是有 q 个元素的有限域，其中 q 是一个素数的方幂。设 K 是 $\mathbb{F}_q$ 的一个扩张次数为 n 的扩域，将其记为 $\mathbb{F}_{q^n}$。将形如

$$L(x)=\sum_{i=0}^{t}a_i x^{q^i},\ t\in\mathbb{N},\ a_i\in\mathbb{F}_{q^n}, \tag{1}$$

的多项式称为 $\mathbb{F}_{q^n}$ 上的线性化多项式。显然，$\forall x,y\in\mathbb{F}_{q^n}$，$a,b\in\mathbb{F}_q$，$L(ax+by)=aL(x)+bL(y)$，即线性化多项式 $L(x)$ 可以诱导出 $\mathbb{F}_{q^n}$ 上的 $\mathbb{F}_q$-线性变换。由于扩域 $\mathbb{F}_{q^n}$ 上的元素满足 $x^{q^n}-x=0$，故线性化多项式也可以被视为

$$L(x)=\sum_{i=0}^{n-1}a_i x^{q^i}\in\mathbb{F}_{q^n}[x]/\left(x^{q^n}-x\right). \tag{2}$$

记 $\mathbb{F}_{q^n}$ 上的全体形如(2)式的线性化多项式集合为 $\mathbb{L}\left(\mathbb{F}_{q^n}\right)$，在 $\mathbb{L}\left(\mathbb{F}_{q^n}\right)$ 中存在一类核为{0}的线性化多项式，称其为置换线性化多项式。换句话说，置换线性化多项式作为 $\mathbb{F}_{q^n}$ 上的线性变换是可逆的。

由于 $\mathbb{F}_{q^n}$ 也可以看作有限域 $\mathbb{F}_q$ 的 n 维线性空间，所以 Carlitz 在[1]中得出了 $\mathbb{F}_q$ 上的 n 阶矩阵与线性化多项式代数 $\mathbb{L}\left(\mathbb{F}_{q^n}\right)$ 间的同构。Dickson 进一步给出了 $\mathbb{L}\left(\mathbb{F}_{q^n}\right)$ 与 Dickson 矩阵代数间的同构，这是一个极为重要的同构关系。近年来，许多学者通过“迹表示”对线性化多项式进行刻画，这种特殊的表示方法，最早是由林杉等在[2]中证明的，袁平之等借助林杉的结论在[3]中得到了置换多项式的充要条件。吴保峰等在[4]中借助 Dickson 矩阵的代数余子式给出了 x^q+ax 型线性化多项式的逆。赵岩和林东岱在[5]中给出了 $\mathbb{F}_q$ 上的 Dickson 矩阵(即循环矩阵)可逆的充要条件，这一结论对于 $\mathbb{F}_q$ 上的线性化多项式核的刻画有着重要的意义。线性化多项式在密码学中有着重要应用，例如，Eli Ben-Sasson 等学者通过满足条件的线性化多项式的解构造了一类新的循环子空间码。在构造子空间码的过程中，确定线性化多项式核的维数是十分重要的。

我们设 $\mathbb{L}\left(\mathbb{F}_q\right)$ 是全体系数在 $\mathbb{F}_q$ 上的线性化多项式集合，则 $\mathbb{L}\left(\mathbb{F}_q\right)$ 构成了 $\mathbb{L}\left(\mathbb{F}_{q^n}\right)$ 的一个子代数。在本文中我们假设 $\{\beta_i\}_{i=0}^{n-1}$ 是一组给定的正规基，即 $\beta_i=\beta^{q^i}, 0\le q\le n-1$，其中 β 是 $\mathbb{F}_{q^n}$ 的本原元。在这组基下，得到了 $\mathbb{L}\left(\mathbb{F}_q\right)$ 与 $\mathbb{F}_q$ 上的循环矩阵代数 $\mathbb{C}\left(\mathbb{F}_q\right)$ 间的同构，从而给出 $\mathbb{L}\left(\mathbb{F}_q\right)$ 上线性化多项式的核的循环矩阵刻画。通过整理赵岩等在[5]中的研究，我们进一步总结了 $\mathbb{L}\left(\mathbb{F}_q\right)$ 中的线性化多项式在 n 与 q 互素和 $n=eq^k$ 的情况下置换多项式存在的条件(其中 e 和 k 都是整数且 k 与 q 互素)。关于 $\mathbb{L}\left(\mathbb{F}_{q^n}\right)$，本文

回顾了林杉等在[2]中对于$\mathbb{L}\left(\mathbb{F}_{q^n}\right)$上的线性化多项式的“迹表示”刻画，进一步通过“迹表示”及初等方法证明了 Dickson 的一个关于线性化置换多项式的知名判定法则。

本文安排如下：第一部分为导言，在第二部分我们总结了$\mathbb{L}\left(\mathbb{F}_q\right)$的部分刻画方法，在第三部分我们总结了$\mathbb{L}\left(\mathbb{F}_{q^n}\right)$的相关研究，第四部分为结束语。

2. 关于$\mathbb{L}\left(\mathbb{F}_q\right)$的刻画

首先我们回顾有限域中的重要定理，在此之前我们需要定义$\mathbb{F}_q$上的循环矩阵。

若$\mathbb{F}_q$上的矩阵 C 具有以下形式：

$$C=\begin{pmatrix} a_0 & a_1 & \cdots & a_{n-1} \\ a_{n-1} & a_0 & \cdots & a_{n-2} \\ \vdots & \vdots & & \vdots \\ a_1 & a_2 & \cdots & a_0 \end{pmatrix}, a_i \in \mathbb{F}_q,$$

我们称其为$\mathbb{F}_q$上的循环矩阵。循环矩阵 C 总是可以被表示为

$$C_{\mathbb{F}}=\begin{pmatrix} a_0 & a_1 & \cdots & a_{n-1} \\ a_{n-1} & a_0 & \cdots & a_{n-2} \\ \vdots & \vdots & & \vdots \\ a_1 & a_2 & \cdots & a_0 \end{pmatrix}=P(J)=\sum_{i=0}^{n-1} a_i J^i, a_i \in \mathbb{F}_q,$$

其中 J 为

$$J=\begin{pmatrix} 0 & 1 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & 1 \\ 1 & 0 & \cdots & 0 \end{pmatrix}.$$

称 J 为单位循环矩阵。

定理 1 [6]：设$\mathbb{F}_{q^n}$为$\mathbb{F}_q$的 n 次扩张，则存在$\mathbb{F}_q$上的正规基$\{\beta_i\}_{i=0}^{n-1}$，其中$\beta_i=\beta^{q^i}, 0\le q\le n-1$，$\beta$ 为$\mathbb{F}_{q^n}$的本原元。

我们设$L(x)=\sum_{i=0}^{n-1} a_i x^{q^i} \in \mathbb{L}\left(\mathbb{F}_q\right)$，由定理 1 我们可以选取正规基$\{\beta_i\}_{i=0}^{n-1}$。根据线性代数知识，$L(x)$在这组基下的像可以表示为

$$\begin{bmatrix} L(\beta) \\ L\left(\beta^q\right) \\ \vdots \\ L\left(\beta^{q^{n-1}}\right) \end{bmatrix}=\begin{pmatrix} a_0 & a_1 & \cdots & a_{n-1} \\ a_{n-1} & a_0 & \cdots & a_{n-2} \\ \vdots & \vdots & & \vdots \\ a_1 & a_2 & \cdots & a_0 \end{pmatrix}\begin{bmatrix} \beta \\ \beta^q \\ \vdots \\ \beta^{q^{n-1}} \end{bmatrix} \triangleq C_{\mathbb{F}}\begin{bmatrix} \beta \\ \beta^q \\ \vdots \\ \beta^{q^{n-1}} \end{bmatrix},$$

即$L(x)$在正规基下的矩阵为$C_{\mathbb{F}}$，显然$C_{\mathbb{F}}$是一个循环矩阵，同时满足

$$\dim\left(\ker\left(L(x)\right)\right)=n-\dim\left(C_{\mathbb{F}}\right).$$

接下来的定理就是显而易见的。

定理 2 [6]：$L(x)=\sum_{i=0}^{n-1} a_i x^{q^i} \in \mathbb{L}\left(\mathbb{F}_q\right)$是一个置换线性化多项式当且仅当$C_{\mathbb{F}}$是非奇异的。

我们令$\mathbb{C}\left(\mathbb{F}_q\right)$为$\mathbb{F}_q$上的全体循环矩阵$C_{\mathbb{F}}$所组成的集合，在矩阵的加法及以$\mathbb{F}_q$为数域的数乘运算下，

$\mathbb{C}\left(\mathbb{F}_q\right)$构成了一个$\mathbb{F}_q$-线性空间，进一步结合通常的矩阵乘法，$\mathbb{C}\left(\mathbb{F}_q\right)$构成了$\mathbb{F}_q$-代数。Ore 在[7]中定义了线性化多项式的复合乘法

$$\begin{aligned} L_1(x)\circ L_2(x) &= \sum_{i=0}^{n-1} a_i \left(\sum_{j=0}^{n-1} b_j x^{q^j} \right)^{q^i} \\ &= \sum_{i=0}^{n-1} \sum_{j=0}^{n-1} a_i b_j x^{q^{i+j}} \\ &= \sum_{i=0}^{n-1} \left(\sum_{k=0}^{n-1} a_k b_{i-k} \right) x^{q^i}. \end{aligned} \tag{3}$$

其中$L_1(x)=\sum_{i=0}^{n-1}a_i x^{q^i}, L_2(x)=\sum_{j=0}^{n-1}b_j x^{q^j}\in\mathbb{L}\left(\mathbb{F}_q\right)$，在多项式加法以及上面的复合乘法运算下，$\mathbb{L}\left(\mathbb{F}_q\right)$构成了$\mathbb{F}_q$-代数，注意到下列运算，事实上证明了$\mathbb{C}\left(\mathbb{F}_q\right)$与$\mathbb{L}\left(\mathbb{F}_q\right)$的$\mathbb{F}_q$-代数同构关系：

$$\left(a_{j-i}\right)\left(b_{j-i}\right)=\left(\sum_{k=0}^{n-1}a_{k-i}b_{j-k}\right)=\left(\sum_{k=0}^{n-1}a_k b_{j-i-k}\right)=\left(c_{j-i}\right),$$

其中，$a_i,b_i\in\mathbb{F}_q, 0\le i\le n-1$，$c_i=\sum_{k=0}^{n-1}a_i b_{i-k}, 0\le i\le n-1$。

从线性化多项式系数的角度出发，可以对定理 2 有更加深刻的认识，我们回顾赵岩等在[5]中给出的有限域中循环矩阵可逆的充分必要条件，从而得出$\mathbb{L}\left(\mathbb{F}_q\right)$上线性化多项式是置换线性化多项式的充要条件。为此先给出下面的定义：

定义：设$L(x)=\sum_{i=0}^{n-1}a_i x^{q^i}\in\mathbb{L}\left(\mathbb{F}_q\right)$，称形如

$$P(x)=\sum_{i=0}^{n-1}a_i x^i, a_i\in\mathbb{F}_q$$

的多项式为$L(x)$的伴随多项式。

2.1. $(q,n)=1$时

本小节我们总假定$(q,n)=1$成立，由[5]中定理 2.1 可知，分圆多项式在$\mathbb{F}_{q^n}$上必然存在n次本原单位根。

定理 3：当$(q,n)=1$时，$L(x)=\sum_{i=0}^{n-1}a_i x^{q^i}\in\mathbb{L}\left(\mathbb{F}_q\right)$是置换线性化多项式当且仅当$P\left(\varepsilon^l\right)\neq 0$，其中$l$为$0\le l\le n-1$的任意整数，$\varepsilon$是$\mathbb{F}_{q^n}$上的$n$次分圆多项式的本原单位根。

为了证明该定理，需要引入以下的引理：

引理 4 [5]：对于满足$0\le l\le n-1$的所有l，$P\left(\varepsilon^l\right)\neq 0$等价于$P(x)$与$x^n-1$是互素的，其中$\varepsilon$是$n$次分圆多项式的本原单位根。

证明：不妨设存在l使得$P\left(\varepsilon^l\right)=0$，即$\varepsilon^l$是$x^n-1$的根也是$P(x)$的根，从而$P(x)$与$x^n-1$不互素，故矛盾。另一方面，如果$P(x)$与$x^n-1$在$\mathbb{F}_q$上不互素，则必然存在$\mathbb{F}_q$上的元素$\eta$，使得$\eta$即是$P(x)$的根也是$x^n-1$的根，由于$x^n-1$的根都可以表示为$\varepsilon^l$的形式，那么必然存在$0\le l\le n-1$使得$P\left(\varepsilon^l\right)=0$。

设$L(x)=\sum_{i=0}^{n-1}a_i x^{q^i}\in\mathbb{L}\left(\mathbb{F}_q\right)$，其伴随多项式为$P(x)$，由$L(x)$诱导产生的循环矩阵$C_{\mathbb{F}}$总是可以由单位循环矩阵$J$表示为

$$C_{\mathbb{F}}=\begin{pmatrix} a_0 & a_1 & \cdots & a_{n-1} \\ a_{n-1} & a_0 & \cdots & a_{n-2} \\ \vdots & \vdots & & \vdots \\ a_1 & a_2 & \cdots & a_0 \end{pmatrix}=P(J)=\sum_{i=0}^{n-1}a_i J^i, a_i\in\mathbb{F}_q,$$

同时我们也称 $P(x)$ 是循环矩阵 $C_{\mathbb{F}}$ 的代表多项式。线性化多项式 $L(x)$ 的伴随多项式与对应的循环矩阵 $C_{\mathbb{F}}$ 的代表多项式形式相同，为了行文方便，下文不对这两种多项式加以区分。

结合引理 4，可以通过以下定理得到定理 3：

定理 5 [5]：循环矩阵 $C_{\mathbb{F}}$ 是非奇异的，当且仅当 $C_{\mathbb{F}}$ 的代表多项式 $P(x)$ 与 x^n-1 是互素的。

证明：我们可知：

$$C_{\mathbb{F}}=P(J),$$

由[5]中推论 2 可知，J 是可对角化的，说明 $C_{\mathbb{F}}$ 的特征值 $\lambda_i,0\le i\le n-1$ 总是满足

$$\lambda_i=P(\mu_i).$$

其中 $\mu_i,0\le i\le n-1$ 为 J 的特征值，同时 μ_i 也是分圆多项式 x^n-1 的根。

此时，若 $C_{\mathbb{F}}$ 是可逆的，说明 $C_{\mathbb{F}}$ 的特征值 $\lambda_i,0\le i\le n-1$ 都不为 0，若 $P(x)$ 与 x^n-1 不互素即 μ_i 是 $P(x)$ 的根，则 $C_{\mathbb{F}}$ 存在为 0 的特征值，故而矛盾。另一方面，若 $C_{\mathbb{F}}$ 是可逆的，说明 $C_{\mathbb{F}}$ 的特征值 $\lambda_i,0\le i\le n-1$ 都不为 0。由于 $P(x)$ 与 x^n-1 互素，故 x^n-1 的根 $\mu_i,0\le i\le n-1$ 令 $\lambda_i=P(\mu_i)\ne 0$，从而 $C_{\mathbb{F}}$ 可逆。

由于 $C_{\mathbb{F}}$ 可逆，则 $L(x)$ 是 $\mathbb{F}_q$ 上的置换多项式，再次结合引理 4 便可以得到定理 3 的结论。

2.2. $n=mq^k$ 时

赵岩等在[5]中得出了 $n=mq^k$ 时，循环矩阵可逆的条件：

引理 6 [5]：V 是循环矩阵，若 $n=mq^k$，$q\nmid m$，ε 是分圆多项式的 m 次本原单位根，则 V^{q^k} 也是循环矩阵，其代表多项式为 $P_a(x)$，则如下条件等价：

1) 矩阵 V 可逆；

2) 对于任意 l，$0\le l\le n-1$，有 $P_a(\varepsilon^l)\ne 0$；

3) 多项式 $P_a(x)$ 与 x^m-1 是互素的。

根据 $\mathbb{L}(\mathbb{F}_q)$ 中线性化多项式与对应的循环矩阵间的关系，可以得到：

定理 7：若 $n=mq^k$，$q\nmid m$，ε 是分圆多项式的 m 次本原单位根，令 $L(x)\in\mathbb{L}(\mathbb{F}_q)$ 的 n 次复合乘法运算 $L(x)\circ L(x)\circ\cdots\circ L(x)=L^n(x)$，记 $L^{q^k}(x)$ 的伴随多项式为 $P_a(x)$，则如下条件等价：

1) $L(x)$ 是一个置换线性化多项式；

2) 对于任意 l，$0\le l\le n-1$，有 $P_a(\varepsilon^l)\ne 0$；

3) 多项式 $P_a(x)$ 与 x^m-1 是互素的。

证明：由于线性化多项式 $L(x)$ 对应的线性变换的矩阵为 $C_{\mathbb{F}}$，则线性化多项式 $L^{q^k}(x)$ 对应的线性变换的矩阵为 $C_{\mathbb{F}}^{q^k}$，其代表多项式也为 $P_a(x)$，再根据引理 6 可以得到定理 7 的结论。

3. 关于 $\mathbb{L}(\mathbb{F}_{q^n})$ 的刻画

定义：设 $a_i\in\mathbb{F}_{q^n},0\le i\le n-1$ 称具有如下形式的矩阵为 Dickson 矩阵，记为 D_L。

$$\begin{bmatrix} a_0 & a_1 & \cdots & a_{n-1} \\ a_{n-1}^q & a_0^q & \cdots & a_{n-2}^q \\ \vdots & \vdots & \ddots & \vdots \\ a_1^{q^{n-1}} & a_2^{q^{n-1}} & \cdots & a_0^{q^{n-1}} \end{bmatrix},$$

令 $\mathcal{D}_n(\mathbb{F}_{q^n})$ 为 $\mathbb{F}_{q^n}$ 上的全体 Dickson 矩阵 D_L 所组成的集合，在矩阵的加法及以 $\mathbb{F}_q$ 为数域的数乘运算下，$\mathcal{D}_n(\mathbb{F}_{q^n})$ 构成了一个 $\mathbb{F}_q$-线性空间。

引理 8 [6]：我们称 $\mathbb{F}_{q^n}$ 上的多项式函数 $y(x)=x+x^q+x^{q^2}+\cdots+x^{q^{n-1}}$ 为迹函数，记为 $\mathrm{tr}(x)$，则迹函数 $\mathrm{tr}(x)$ 是一个从 $\mathbb{F}_{q^n}$ 到 $\mathbb{F}_q$ 上的线性映射。

引理 8 是显然的，因为对于 $\mathbb{F}_{q^n}$ 中的任意元素 x，迹函数总是满足 $\mathrm{tr}(x)=\mathrm{tr}(x^q)$。

定理 9 [5]：设 $L(x)\in\mathbb{L}(\mathbb{F}_{q^n})$，$\{\omega_i\}_{i=0}^{n-1}$ 为 $\mathbb{F}_{q^n}$ 关于 $\mathbb{F}_q$ 的任一组给定基，则存在唯一确定的系数 $\{\theta_i\}_{i=0}^{n-1}\subseteq\mathbb{F}_{q^n}$，使得

$$L(x)=\sum_{i=0}^{n-1}\mathrm{tr}(\omega_i x)\theta_i.$$

证明：我们设 $L(x)=\sum_{i=0}^{n-1}a_i x^{p^i}\in\mathbb{L}(\mathbb{F}_{q^n})$，由[6]中的定理 2.38 可知，$\begin{bmatrix}\omega_0 & \omega_1 & \cdots & \omega_{n-1}\\ \omega_0^q & \omega_1^q & \cdots & \omega_{n-1}^q\\ \vdots & \vdots & \ddots & \vdots\\ \omega_0^{q^{n-1}} & \omega_1^{q^{n-1}} & \cdots & \omega_{n-1}^{q^{n-1}}\end{bmatrix}$可逆，因此这组系数 $\{a_i\}_{i=0}^{n-1}$ 在基 $\{\omega_i\}_{i=0}^{n-1}$ 下有以下分解

$$[a_0,a_1,\cdots,a_{n-1}]=[\theta_0,\theta_1,\cdots,\theta_{n-1}]\begin{bmatrix}\omega_0 & \omega_0^q & \cdots & \omega_0^{q^{n-1}}\\ \omega_1 & \omega_1^q & \cdots & \omega_1^{q^{n-1}}\\ \vdots & \vdots & \ddots & \vdots\\ \omega_{n-1} & \omega_{n-1}^q & \cdots & \omega_{n-1}^{q^{n-1}}\end{bmatrix}.$$

其中 $\{\theta_i\}_{i=0}^{n-1}\subseteq\mathbb{F}_{q^n}$ 存在，从而

$$\begin{aligned}L(x)=&\theta_0\left(\omega_0x+(\omega_0x)^q+\cdots+(\omega_0x)^{q^{n-1}}\right)\\&+\theta_1\left(\omega_1x+(\omega_1x)^q+\cdots+(\omega_1x)^{q^{n-1}}\right)\\&+\cdots\\&+\theta_{n-1}\left(\omega_{n-1}x+(\omega_{n-1}x)^q+\cdots+(\omega_{n-1}x)^{q^{n-1}}\right).\end{aligned}$$

即 $L(x)=\sum_{i=0}^{n-1}\mathrm{tr}(\omega_i x)\theta_i$，我们称这种表示形式为线性化多项式的迹表示。

设 $\{\omega_i\}_{i=0}^{n-1}$ 是 $\mathbb{F}_{q^n}$ 在 $\mathbb{F}_q$ 上的一组基，根据定理 9，$L(x)\in\mathbb{L}(\mathbb{F}_{q^n})$ 可以在这组基下被表示为

$$\begin{aligned}\left[L(\omega_0),L(\omega_1),\cdots,L(\omega_{n-1})\right]&=[\theta_0,\theta_1,\cdots,\theta_{n-1}]\begin{bmatrix}\mathrm{tr}(\omega_0\omega_0) & \mathrm{tr}(\omega_1\omega_0) & \cdots & \mathrm{tr}(\omega_{n-1}\omega_0)\\ \mathrm{tr}(\omega_0\omega_1) & \mathrm{tr}(\omega_1\omega_1) & \cdots & \mathrm{tr}(\omega_{n-1}\omega_1)\\ \vdots & \vdots & \ddots & \vdots\\ \mathrm{tr}(\omega_0\omega_{n-1}) & \mathrm{tr}(\omega_1\omega_{n-1}) & \cdots & \mathrm{tr}(\omega_{n-1}\omega_{n-1})\end{bmatrix}\\&\triangleq[\theta_0,\theta_1,\cdots,\theta_{n-1}]W.\end{aligned}\tag{4}$$

由引理 8 可知，(4)式中的矩阵 W 是 $\mathbb{F}_q$ 上的矩阵。由[6]中的定理 2.37 可以得到，W 在 $\mathbb{F}_q$ 上是非奇异的，因此借助(4)式可以证明袁平之等在[3]中提出的以下定理：

引理 10 [3]：设 $L(x)\in\mathbb{L}(\mathbb{F}_{q^n})$，$\{\omega_i\}_{i=0}^{n-1}$ 为 $\mathbb{F}_{q^n}$ 关于 $\mathbb{F}_q$ 的任一组给定基，且 $L(x)=\sum_{i=0}^{n-1}\mathrm{tr}(\omega_i x)\theta_i$，则 $L(x)$

为置换线性化多项式当且仅当$\{\theta_i\}_{i=0}^{n-1}$为$\mathbb{F}_{q^n}$关于$\mathbb{F}_q$的一组基。

证明：$\{\theta_i\}_{i=0}^{n-1}$作为$\mathbb{F}_q$上的向量组，可以在基$\{\omega_i\}_{i=0}^{n-1}$下被表示为

$$[\theta_0,\theta_1,\cdots,\theta_{n-1}]=[\omega_0,\omega_1,\cdots,\omega_{n-1}]\begin{bmatrix}\theta_{00} & \theta_{01} & \cdots & \theta_{0n-1}\\ \theta_{10} & \theta_{11} & \cdots & \theta_{1n-1}\\ \vdots & \vdots & \ddots & \vdots\\ \theta_{n-10} & \theta_{n-11} & \cdots & \theta_{n-1n-1}\end{bmatrix}\triangleq[\omega_0,\omega_1,\cdots,\omega_{n-1}]\Theta. \tag{5}$$

即(5)中的矩阵Θ是向量组$\{\theta_i\}_{i=0}^{n-1}$在$\mathbb{F}_q$上的分量矩阵。由(4)可知，(5)还可以被表示为

$$\left[L(\omega_0),L(\omega_1),\cdots,L(\omega_{n-1})\right]=[\omega_0,\omega_1,\cdots,\omega_{n-1}]\Theta W,$$

从而

$$\dim\left(\ker\left(L(x)\right)\right)=n-\dim(\Theta),$$

则引理结论可得。

根据[2]中的定理 2.38，可以得到以下关系

$$n-\dim\left(\ker\left(L(x)\right)\right)=\dim\left(\mathrm{Im}\left(L(x)\right)\right)=\dim(\Theta)=\dim\left([\theta_0,\theta_1,\cdots,\theta_{n-1}]\right)=\dim\left(\begin{bmatrix}\theta_0 & \theta_1 & \cdots & \theta_{n-1}\\ \theta_0^{\,q} & \theta_1^{\,q} & \cdots & \theta_{n-1}^{q}\\ \vdots & \vdots & \ddots & \vdots\\ \theta_0^{\,q^{n-1}} & \theta_1^{\,q^{n-1}} & \cdots & \theta_{n-1}^{q^{n-1}}\end{bmatrix}\right). \tag{6}$$

通过以上结论，我们可以用初等方法证明吴保峰等学者提出的命题。

定理 11 [4]：设$L(x)=\sum_{i=0}^{n-1}a_ix^{p^i}\in\mathbb{L}\left(\mathbb{F}_{q^n}\right)$，$\{\omega_i\}_{i=0}^{n-1}$为$\mathbb{F}_{q^n}$关于$\mathbb{F}_q$的任一组给定基，且存在唯一的一组系数$\{\theta_i\}_{i=0}^{n-1}\subseteq\mathbb{F}_{q^n}$，使得$L(x)=\sum_{i=0}^{n-1}\mathrm{tr}(\omega_ix)\theta_i$，且满足

$$\dim\left(\mathrm{Im}\left(L(x)\right)\right)=\dim\left(\begin{bmatrix}\theta_0 & \theta_1 & \cdots & \theta_{n-1}\\ \theta_0^{q} & \theta_1^{q} & \cdots & \theta_{n-1}^{q}\\ \vdots & \vdots & \ddots & \vdots\\ \theta_0^{q^{n-1}} & \theta_1^{q^{n-1}} & \cdots & \theta_{n-1}^{q^{n-1}}\end{bmatrix}\right)=\dim\left(\begin{bmatrix}a_0 & a_1 & \cdots & a_{n-1}\\ a_{n-1}^{q} & a_0^{q} & \cdots & a_{n-2}^{q}\\ \vdots & \vdots & \ddots & \vdots\\ a_1^{q^{n-1}} & a_2^{q^{n-1}} & \cdots & a_0^{q^{n-1}}\end{bmatrix}\right). \tag{7}$$

证明：不妨先考虑(7)中等式右侧 Dickson 矩阵D_L的第一行，由$L(x)=\sum_{i=0}^{n-1}\mathrm{tr}(\omega_ix)\theta_i=\sum_{i=0}^{n-1}a_ix^{q^i}$可以得到

$$[a_0,a_1,\cdots,a_{n-1}]=[\theta_0,\theta_1,\cdots,\theta_{n-1}]\begin{bmatrix}\omega_0 & \omega_0^{q} & \cdots & \omega_0^{q^{n-1}}\\ \omega_1 & \omega_1^{q} & \cdots & \omega_1^{q^{n-1}}\\ \vdots & \vdots & \ddots & \vdots\\ \omega_{n-1} & \omega_{n-1}^{q} & \cdots & \omega_{n-1}^{q^{n-1}}\end{bmatrix}, \tag{8}$$

再考虑D_L的第二行

$$\left[a_0^q,a_1^q,\cdots,a_{n-1}^q\right]=\left[\theta_0^q,\theta_1^q,\cdots,\theta_{n-1}^q\right]\begin{bmatrix}\omega_0^{q} & \omega_0^{q^2} & \cdots & \omega_0\\ \omega_1^{q} & \omega_1^{q^2} & \cdots & \omega_1\\ \vdots & \vdots & \ddots & \vdots\\ \omega_{n-1}^{q} & \omega_{n-1}^{q^2} & \cdots & \omega_{n-1}\end{bmatrix},$$

从而得到

$$\left[a_{n-1}^{q},a_{0}^{q},\cdots,a_{n-2}^{q}\right]=\left[\theta_{n-1}^{q},\theta_{0}^{q},\cdots,\theta_{n-2}^{q}\right]\begin{bmatrix}\omega_0 & \omega_0^{q} & \cdots & \omega_0^{q^{n-1}}\\ \omega_1 & \omega_1^{q} & \cdots & \omega_1^{q^{n-1}}\\ \vdots & \vdots & \ddots & \vdots\\ \omega_{n-1} & \omega_{n-1}^{q} & \cdots & \omega_{n-1}^{q^{n-1}}\end{bmatrix},$$

以此类推

$$\begin{bmatrix}a_0 & a_1 & \cdots & a_{n-1}\\ a_{n-1}^{q} & a_0^{q} & \cdots & a_{n-2}^{q}\\ \vdots & \vdots & \ddots & \vdots\\ a_1^{q^{n-1}} & a_2^{q^{n-1}} & \cdots & a_0^{q^{n-1}}\end{bmatrix}=\begin{bmatrix}\theta_0 & \theta_1 & \cdots & \theta_{n-1}\\ \theta_0^{\ q} & \theta_1^{q} & \cdots & \theta_{n-1}^{q}\\ \vdots & \vdots & \ddots & \vdots\\ \theta_0^{\ q^{n-1}} & \theta_1^{\ q^{n-1}} & \cdots & \theta_{n-1}^{q^{n-1}}\end{bmatrix}\begin{bmatrix}\omega_0 & \omega_0^{q} & \cdots & \omega_0^{q^{n-1}}\\ \omega_1 & \omega_1^{q} & \cdots & \omega_1^{q^{n-1}}\\ \vdots & \vdots & \ddots & \vdots\\ \omega_{n-1} & \omega_{n-1}^{q} & \cdots & \omega_{n-1}^{q^{n-1}}\end{bmatrix}.$$

根据[2]中的定理 2.38，由基$\left\{\omega_i\right\}_{i=0}^{n-1}$组成的矩阵$\begin{bmatrix}\omega_0 & \omega_0^{q} & \cdots & \omega_0^{q^{n-1}}\\ \omega_1 & \omega_1^{q} & \cdots & \omega_1^{q^{n-1}}\\ \vdots & \vdots & \ddots & \vdots\\ \omega_{n-1} & \omega_{n-1}^{q} & \cdots & \omega_{n-1}^{q^{n-1}}\end{bmatrix}$是可逆的，因此可以得到

$$\dim\left(\begin{bmatrix}\theta_0 & \theta_1 & \cdots & \theta_{n-1}\\ \theta_0^{\ q} & \theta_1^{q} & \cdots & \theta_{n-1}^{q}\\ \vdots & \vdots & \ddots & \vdots\\ \theta_0^{\ q^{n-1}} & \theta_1^{\ q^{n-1}} & \cdots & \theta_{n-1}^{q^{n-1}}\end{bmatrix}\right)=\dim\left(\begin{bmatrix}a_0 & a_1 & \cdots & a_{n-1}\\ a_{n-1}^{q} & a_0^{q} & \cdots & a_{n-2}^{q}\\ \vdots & \vdots & \ddots & \vdots\\ a_1^{q^{n-1}} & a_2^{q^{n-1}} & \cdots & a_0^{q^{n-1}}\end{bmatrix}\right).$$

通过定理 11，我们可以得到[5]中的结论。

推论 12 [5]：$L(x)\in\mathbb{L}\left(\mathbb{F}_{q^n}\right)$是置换线性化多项式，当且仅当其诱导产生的 Dickson 矩阵是非奇异的。

定理 13 [5]：

$$\mathcal{D}_n\left(\mathbb{F}_{q^n}\right)\cong\mathbb{L}\left(\mathbb{F}_{q^n}\right).$$

证明：定理 12 说明，$\mathcal{D}_n\left(\mathbb{F}_{q^n}\right)$与$\mathbb{L}\left(\mathbb{F}_{q^n}\right)$向量空间同构。进一步结合通常的矩阵乘法，$\mathcal{D}_n\left(\mathbb{F}_{q^n}\right)$构成了$\mathbb{F}_q$-代数。在代数$\mathbb{L}\left(\mathbb{F}_{q^n}\right)$中定义的复合乘法下，显然也构成了$\mathcal{D}_n\left(\mathbb{F}_{q^n}\right)$与$\mathbb{L}\left(\mathbb{F}_{q^n}\right)$的$\mathbb{F}_q$-代数同构关系，证明类似于$\mathbb{C}\left(\mathbb{F}_q\right)$与$\mathbb{L}\left(\mathbb{F}_q\right)$的$\mathbb{F}_q$-代数同构。

4. 结束语

本文首先回顾了$\mathbb{F}_q$上的线性化多项式代数$\mathbb{L}\left(\mathbb{F}_q\right)$的一些刻画，借助这些刻画，总结了这类多项式中是置换多项式的条件。我们还研究了$\mathbb{F}_{q^n}$上的线性化多项式的“迹表示”，并通过“迹表示”再次证明了 Dickson 提出的重要结论。线性化多项式对应的 Dickson 矩阵在研究某些问题时非常重要，例如在[4]中，吴保峰等借助由线性化多项式诱导生成的 Dickson 矩阵，得到了x^q+ax型线性化多项式的逆。我们还在考虑能否借助 Dickson 矩阵得到更高阶线性化多项式的逆，从而解决极大秩距离码研究中遇到的一些问题。

基金项目

“中国民航大学大学生创新创业训练计划项目”，项目编号为“IECAUC2022063”；“天津市普通高等学校本科教学质量与教学改革研究重点项目”，项目编号为“A231005903”。

参考文献

[1] Carlitz, L. (1963) A Note on the Betti-Mathieu Group. *Portugaliae Mathematica*, **22**, 121-125.

[2] Ling, S. and Qu, L. (2012) A Note on Linearized Polynomials and the Dimension of Their Kernels. *Finite Fields and Their Applications*, **18**, 56-62. https://doi.org/10.1016/j.ffa.2011.06.002

[3] Yuan, P. and Zeng, X. (2011) A Note on Linear Permutation Polynomials. *Finite Fields and Their Applications*, **17**, 488-491. https://doi.org/10.1016/j.ffa.2011.02.013

[4] Wu, B. and Liu, Z. (2013) Linearized Polynomials over Finite Fields Revisited. *Finite Fields and Their Applications*, **22**, 79-100. https://doi.org/10.1016/j.ffa.2013.03.003

[5] Zhao, Y. and Lin, D.D. (2012) Nonsingular Circulant Matrices over Finite Fields. *Journal of Graduate University of Chinese Academy of Sciences*, **29**, 805-814.

[6] Lidl, R. and Niederreiter, H. (1997) Finite Fields, 2nd Edition. Encyclopedia of Mathematics and Its Applications, Vol. 20, Cambridge University Press, Cambridge, 60-61.

[7] Ore, O. (1933) On a Special Class of Polynomials. *Transactions of the American Mathematical Society*, **35**, 559-584. https://doi.org/10.1090/s0002-9947-1933-1501703-0