doi: 10.3969/j.issn.0490-6756.2020.06.004

Fibonacci 多项式的置换性质

王智坚
(四川大学数学学院, 成都 610064)

摘 要: 置换多项式在代数学、组合学、数论、编码理论、密码学等领域中均有广泛而又重要的应用. 本文主要研究 Fibonacci 多项式. 通过计算其函数值的等幂和,本文得到了判定这些定义在有限域上的 Fibonacci 多项式为置换多项式的必要条件,解决了 Fernando 和 Rashid 提出的一个公开问题,从而推广了有关 Fibonacci 多项式置换性的已有结论.

关键词: 置换性; Fibonacci 多项式; 有限域; 编码理论
中图分类号: O156.1 **文献标识码**: A **文章编号**: 0490-6756(2020)06-1047-05

Permutation properties of the Fibonacci polynomials

WANG Zhi-Jian
(School of Mathematics, Sichuan University, Chengdu 610064, China)

Abstract: Permutation polynomial has wide and important applications in algebra, combinatorics, number theory, coding theory, cryptography, etc. In this paper, by calculating the sum of the Fibonacci polynomial, we obtain some necessary conditions that a Fibonacci polynomial, defined on a finite field, is a permutation polynomial, solve the open problem introduced by Fernando and Rashid and generalize the existing results.

Keywords: Permutation property; Fibonacci polynomial; Finite field; Coding theory
(2010 MSC 11R09, 11R04)

1 引 言

对非负整数 n,Fibonacci 多项式 $f_n(x)$是由如下递推关系给出的整系数多项式:

$$f_0(x)=0, f_1(x)=1,$$
$$f_n(x)=xf_{n-1}(x)+f_{n-2}(x), n\geqslant 2.$$

由于 $f_n(1)=f_{n-1}(1)+f_{n-2}(x)$,这正好是 Fibonacci 数的递推关系,即 Fibonacci 多项式可以看作是 Fibonacci 数的推广. 当 $x=2$ 时, $f_n(2)=2f_{n-1}(2)+f_{n-2}(2)$. 此时 $f_n(2)$便是著名的 Pell 数.

Fibonacci 多项式是比利时数学家 Catalan 和德国数学家 Jacobsthal 在 1883 年首先提出来的[1]. 有关 Fibonacci 多项式的一般性质,尤其是算术性质,已得到广泛的研究[2-3].

设 p 为素数,e 为正整数. 若有限域 F_{p^e} 上的多项式 $f(x)$作为 F_{p^e} 上的多项式函数诱导出 F_{p^e} 的一个双射,则称 $f(x)$为 F_{p^e} 上的置换多项式. 置换多项式在代数学、组合学、数论、编码理论、密码学等领域中均有广泛而又重要的应用. 如何判定和构造置换多项式始终是置换多项式研究领域的主要课题.

Fibonacci 多项式原本定义在整数环上,它们自然可以被视为任何有限域上的多项式,从而可讨论它们在有限域上的置换性质. 最近, Koroglu, Ozbek 及 Siap[4]研究了有限域上以 Fibonacci 多项

收稿日期: 2019-05-14
作者简介: 王智坚(1993-), 男, 湖北人, 硕士研究生, 主要研究方向为数论. E-mail: 605258703@qq.com

式为生成多项式之一的循环码. Kitayama 和 Shiomi[5]研究了有限域上 Fibonacci 多项式的不可约性.

在本文中,我们采用与 Fernando 和 Rashid 类似的方法来研究 Fibonacci 多项式在有限域 F_{p^e} 上的置换性质. Fernando 和 Rashid 给出了当 q 为偶数时 $A_n=\sum_{x\in F_q} f_n^2(x)$ 的值[1],而对 q 为奇数时的情形未给出结果,并作为公开问题提出. 本文计算了 q 为奇数时 $A_n=\sum_{x\in F_q} f_n^2(x)$ 的值,解决了 Fernando 和 Rashid 提出的公开问题,得到了关于 Fibonacci 多项式的置换性质更加精细的刻画,进而判定出某些 Fibonacci 多项式不是置换多项式.

2 整环上的 Fibonacci 多项式

设 D 为特征不为 2 的整环,K 为它的分式域. 在没有混淆的情况下,我们以 f 简记 K 上的多项式 $f(x)$.

由 Fibonacci 多项式的定义,易见每个 Fibonacci 多项式均定义在整数环 $\mathbf{Z}$ 上,从而可定义在任何交换环上[6]. 我们首先将 Fibonacci 多项式看成定义在整环 D 上的多项式.

类似于 Fibonacci 数列,我们可以得到[7]

$$f_n=\frac{\alpha^n-\beta^n}{\alpha-\beta},$$

其中 $\alpha+\beta=x,\alpha\beta=-1$. 不失一般性,可取

$$\alpha=\frac{x+\sqrt{x^2+4}}{2},$$

$$\beta=\frac{x-\sqrt{x^2+4}}{2}\in K[x,\sqrt{x^2+4}].$$

引理 2.1 对于整环 D 上的 Fibonacci 多项式列$\{f_n\}$,有

(i) $f_nf_{n-2}=f_{n-1}^2+(-1)^{n+1}$;

(ii) $f_n^2=(x^2+2)f_{n-1}^2-f_{n-2}^2+2(-1)^{n-1}$;

(iii) $f_n^3=(x^3+3x)f_{n-1}^3+f_{n-2}^3+3(-1)^{n-1}xf_{n-1}$.

证明 (i) 利用 $f_n=\frac{\alpha^n-\beta^n}{\alpha-\beta}$ 可得 $f_nf_{n-2}-f_{n-1}^2=(-1)^{n+1}$. 故 $f_nf_{n-2}=f_{n-1}^2+(-1)^{n+1}$.

(ii) 由 $f_n=xf_{n-1}+f_{n-2}$ 可知,当 $n\geqslant 2$ 时,$x^2f_{n-1}^2=(f_n-f_{n-2})^2=f_n^2+f_{n-2}^2-2f_{n-1}^2-2(-1)^{n-1}$,故

$$f_n^2=(x^2+2)f_{n-1}^2-f_{n-2}^2+2(-1)^{n-1}.$$

这是多项式列$\{f_n^2\}$的递推关系.

(iii) 与(ii)类似,$x^3f_{n-1}^3=f_n^3-f_{n-2}^3-3f_nf_{n-2}(f_n-f_{n-2})$,故

$$f_n^3=(x^3+3x)f_{n-1}^3+f_{n-2}^3+3(-1)^{n-1}xf_{n-1}.$$

对于 D 上的多项式列$\{\varphi_n\}$,定义它们的生成函数为

$$G(\varphi_n)(z)=\sum_{j=0}^{\infty}\varphi_jz^j\in D[x][z].$$

这是系数在多项式环 $D[x]$ 上的一个形式幂级数.

引理 2.2 对于整环 D 上的 Fibonacci 多项式列$\{f_n\}$,有

$$G(f_n)(z)=\frac{z}{1-xz-z^2}\in D(x,z),$$

$$G(f_n^2)(z)=\frac{z(1-z)}{(1-z)^2(1+z)-z(1+z)x^2}\in D(x,z),$$

$$G(f_n^3)(z)=\frac{z(1-2xz-z^2)}{(1+xz-z^2)(1-(x^3+3x)z-z^2)}\in D(x,z).$$

证明 利用递推关系 $f_n=xf_{n-1}+f_{n-2},n\geqslant 2$ 以及 $f_0=0,f_1=1$ 可得

$$G(f_n)(z)=f_1z+\sum_{n=0}^{\infty}f_{n+2}z^{n+2}=z+xz\sum_{n=0}^{\infty}f_{n+1}z^{n+1}+z^2\sum_{n=0}^{\infty}f_nz^n.$$

故

$$G(f_n)(z)=\frac{z}{1-xz-z^2}\in Z(x,z).$$

类似地,多项式列$\{f_n^2\}$,$\{f_n^3\}$的生成函数可以利用引理 2.1 中的递推关系,用同样的方法得到.

3 有限域上 Fibonacci 多项式的置换性质

现将 Fibonacci 多项式看成 q 元域 F_q 上的多项式,我们来讨论它们作为有限域 F_q 上多项式函数的性质,这里 p 为奇素数,$q=p^e$.

若从 F_q 到 F_q 的多项式函数 $f:c\mapsto f(c)$ 是 F_q 的一个置换,则称多项式 $f\in F_q[x]$ 是 F_q 上的一个置换多项式. 例如,Fibonacci 多项式中的 $f_2(x)=x$ 是任何一个有限域 F_q 上的置换多项式.

引理 3.1[8] 多项式 $f(x)$ 是 F_q 上的置换多项式的充要条件是

$$\sum_{a\in F_q}f^k(a)=\begin{cases}0,\text{若 } 0\leqslant k\leqslant q-2,\\-1,\text{若 } k=q-1.\end{cases}$$

由此可知,要判断 Fibonacci 多项式 $f_n(x)$ 是否为 F_q 上的置换多项式,我们只需计算 $\sum_{a\in F_q}f_n^k(a)$

的所有值($k=0,1,\cdots,q-1$). 下面我们将计算

$$A_n=\sum_{x\in F_q} f_n^2(x) \tag{1}$$

的值，由此来得到 Fibonacci 多项式是置换多项式的必要条件.

Fernando 和 Rashid 得出了关于 Fibinacci 多项式的如下结论.

引理 3.2[1]　(i) 当 $p\equiv 3(\bmod 4)$且 e 为奇数时，若 $n_1\equiv n_2(\bmod p^{2e}-1)$，则 $f_{n_1}(x)$和 $f_{n_2}(x)$作为 F_{p^e} 上的函数相同；

(ii) 当 e 是偶数，或者 e 是奇数且 $p\equiv 1(\bmod 4)$时，若 $n_1\equiv n_2(\bmod \frac{p(p^{2e}-1)}{2})$，则 $f_{n_1}(x)$和 $f_{n_2}(x)$作为 F_{p^e} 上的函数相同.

引理 3.2 表明，当我们讨论 F_{p^e} 上的 Fibonacci 多项式函数 $f_n(x)$时只需关注 $n<p^{2e}-1$ 或 $n<\frac{p(p^{2e}-1)}{2}$的情形.

定理 3.3　设 f_n 为第 n 个 Fibonacci 多项式，素数 $p\equiv 3(\bmod 4)$，e 为奇数，$q=p^e$.

(i) 当 $q=3$，即 $p=3$，$e=1$ 时，有

$$A_n=\begin{cases}0, n=1,\\ -b_1, n=2,\\ -b_{j-1}-A_{n-2}, 3\leqslant n\leqslant 6,\\ 0, 7\leqslant n\leqslant 8.\end{cases}$$

(ii) 当 $q>3$ 时，我们有

$$A_n=\begin{cases}0, 1\leqslant n\leqslant \dfrac{q-1}{2},\\ -b_1, n=\dfrac{q+1}{2},\\ \displaystyle\sum_{k=1}^{n-\frac{q-1}{2}}(-1)^{k+n}b_k-A_{n-\frac{q+1}{2}}, \dfrac{q+3}{2}\leqslant n\leqslant q-1,\\ \displaystyle\sum_{k=n-(q-2)}^{n-\frac{q-1}{2}}(-1)^{k+n}b_k-A_{n-\frac{q+1}{2}}, q\leqslant n\leqslant q^2-\dfrac{q+3}{2},\\ 0, q^2-\dfrac{q+1}{2}\leqslant n\leqslant q^2-1,\end{cases}$$

其中 $1\leqslant k\leqslant q^2-q+1$，

$$b_k=\begin{cases}1, \text{若 } k=1,\\ (-1)^{t-1}\binom{q-1}{t-1}, \text{若 } k=1+t(q-1),\\ \quad 1\leqslant t\leqslant q,\\ 0, \text{其他.}\end{cases}$$

证明　由引理 2.2 可知，f_n^2 的生成函数为

$$\sum_{n=0}^{\infty} f_n^2 z^n=\frac{z(1-z)}{(1-z)^2(1+z)-z(1+z)x^2}.$$

将该式右端按 x 展开可得

$$\frac{z(1-z)}{(1-z)^2(1+z)-z(1+z)x^2}=\frac{z}{1-z^2}\frac{1}{1-\frac{z}{(1-z)^2}x^2}=\frac{z}{1-z^2}\sum_{k\geqslant 0}\frac{z^k}{(1-z)^{2k}}x^{2k}=\frac{z}{1-z^2}\left(1+\sum_{k=1}^{\frac{q-1}{2}}\sum_{l\geqslant 0}\frac{z^{k+\frac{(q-1)l}{2}}}{(1-z)^{2k+l(q-1)}}x^{2k+(q-1)l}\right).$$

故

$$\sum_{n=0}^{\infty} f_n^2 z^n\equiv\frac{z}{1-z^2}+\frac{z}{1-z^2}\sum_{k=1}^{\frac{q-1}{2}}\cdot\sum_{l\geqslant 0}\left(\frac{z}{(1-z)^2}\right)^{k+\frac{(q-1)l}{2}}x^{2k}(\bmod x^q-x)\equiv\frac{z}{1-z^2}+\frac{z}{1-z^2}\sum_{k=1}^{\frac{q-1}{2}}\frac{z^k(1-z)^{q-1-2k}}{(1-z)^{q-1}-z^{\frac{q-1}{2}}}x^{2k}\ (\bmod x^q-x) \tag{2}$$

当 $p\equiv 3(\bmod 4)$且 e 为奇数时，由引理 3.2，我们有

$$\sum_{n=0}^{\infty} f_n^2 z^n=\sum_{n=1}^{q^2-1}\sum_{l\geqslant 0} f_{n+l(q^2-1)}^2 z^{n+l(q^2-1)}\equiv\sum_{n=1}^{q^2-1} f_n^2 z^n\sum_{l\geqslant 0} z^{l(q^2-1)}(\bmod x^q-x).$$

故

$$\sum_{n=1}^{\infty} f_n^2 z^n\equiv\frac{1}{1-z^{q^2-1}}\sum_{n=1}^{q^2-1} f_n^2 z^n(\bmod x^q-x) \tag{3}$$

由(2)和(3)式可知

$$\sum_{n=1}^{q^2-1} f_n^2 z^n\equiv\frac{z(1-z^{q^2-1})}{1-z^2}\left(1+\sum_{k=1}^{\frac{q-1}{2}}\frac{z^k(1-z)^{q-1-2k}}{(1-z)^{q-1}-z^{\frac{q-1}{2}}}x^{2k}\right)(\bmod x^q-x)\equiv\frac{z(1-z^{q^2-1})}{1-z^2}+\frac{z(1-z^{q^2-1})}{(1-z^2)((1-z)^{q-1}-z^{\frac{q-1}{2}})}\sum_{k=1}^{\frac{q-1}{2}}z^k(1-z)^{q-1-2k}x^{2k})(\bmod x^q-x) \tag{4}$$

上式关于 $x\in F_q$ 求和，利用

$$\sum_{x\in F_q}x^k=\begin{cases}0, \text{若 } 0\leqslant k\leqslant q-2,\\ -1, \text{若 } k=q-1\end{cases}$$

可得

$$\sum_{n=1}^{q^2-1}A_n z^n=\frac{z-z^{q^2}}{(1-z^2)((1-z)^{q-1}-z^{\frac{q-1}{2}})}\cdot$$

$$\sum_{k=1}^{\frac{q-1}{2}} z^k (1-z)^{q-1-2k}\Big(\sum_{x\in F_q} x^{2k}\Big) = \frac{(z^{q^2}-z)z^{\frac{q-1}{2}}}{(1-z^2)((1-z)^{q-1}-z^{\frac{q-1}{2}})}.$$

注意到 $z-z^{q^2}=(z-z^q)(1+(z-z^q)^{q-1})$, $z-z^q=(z-z^{\frac{q+1}{2}})(1+z^{\frac{q-1}{2}})$,且

$$(1-z^2)((1-z)^{q-1}-z^{\frac{q-1}{2}}) = (1+z)(((1-z)^q)-z^{\frac{q-1}{2}}(1-z)) = (1+z)(1-z^{\frac{q-1}{2}})(1+z^{\frac{q+1}{2}}),$$

则有

$$\sum_{n=1}^{\infty} A_n z^n = -\frac{z^{\frac{q-1}{2}}(z^{\frac{q-1}{2}}+1)(z+z(z-z^q)^{q-1})}{(1+z)(1+z^{\frac{q+1}{2}})} = -\frac{z^{\frac{q-1}{2}}(1-z+z^2+\cdots+z^{\frac{q-3}{2}})(z+z(z-z^q)^{q-1})}{1+z^{\frac{q+1}{2}}}.$$

又 $z+z(z-z^q)^{q-1}=\sum_{k=1}^{q^2-q+1} b_k z^k$,其中

$$b_k=\begin{cases}1, \text{若 } k=1,\\ (-1)t-1\binom{q-1}{t-1}, \text{若 } k=1+t(q-1),\\ \quad \text{其中 } 1\leqslant t\leqslant q,\\ 0, \text{其他},\end{cases}$$

则有

$$(1+z^{\frac{q+1}{2}})\sum_{n=1}^{q^2-1} A_n z^n = -(z^{\frac{q-1}{2}}-z^{\frac{q+1}{2}}+\cdots+z^{q-2})\sum_{k=1}^{q^2-q+1} b_k z^k \tag{5}$$

比较(5)式关于项 z^i 的系数即可得到定理.

定理 3.4 设 f_n 为第 n 个 Fibonacci 多项式,素数 $p\equiv 1(\bmod 4)$或 $p\equiv 3(\bmod 4)$, e 为偶数, $q=p^e$. 令 $s=\frac{p(q^2-1)}{2}$. 则

(i) 当 $q=5$,即 $p=5$, $e=1$ 时,有

$$A_n=\begin{cases}0, & 1\leqslant n\leqslant 2,\\ -b_1, & n=3,\\ -b_2+b_1, & n=4,\\ -b_{n-\frac{q-1}{2}}-b_{n-(q-1)}-(A_{n-1}+A_{n-\frac{q+1}{2}}+A_{n-\frac{q+3}{2}}), & \\ \qquad 5\leqslant n\leqslant s-3,\\ 0, & s-2\leqslant n\leqslant s;\end{cases}$$

(ii) 当 $q>5$ 时,有

$$A_n=\begin{cases}0, & 1\leqslant n\leqslant \frac{q-1}{2},\\ -b_1, & n=\frac{q+1}{2},\\ -b_2+b_1, & n=\frac{q+3}{2},\\ -b_{n-\frac{q-1}{2}}-(A_{n-1}+A_{n-\frac{q+1}{2}}+A_{n-\frac{q+3}{2}}), & \\ \qquad \frac{q+5}{2}\leqslant n\leqslant q-1,\\ -b_{n-\frac{q-1}{2}}-b_{n-(q-1)}-(A_{n-1}+A_{n-\frac{q+1}{2}}+A_{n-\frac{q+3}{2}}), & \\ \qquad q\leqslant n\leqslant s-\frac{q+1}{2},\\ 0, & s-\frac{q-1}{2}\leqslant n\leqslant s,\end{cases}$$

其中

$$b_k=\begin{cases}1, \text{若 } k=1+t(q-1), 0\leqslant t\leqslant \frac{p(p+1)}{2}-1,\\ 0, \text{其他}.\end{cases}$$

证明 当 $p\equiv 1(\bmod 4)$, e 为任意数,或 $p\equiv 3(\bmod 4)$且 e 为偶数时,令 $s=\frac{p(q^2-1)}{2}$. 由引理 3.2,如果 $n_1\equiv n_2(\bmod s)$,则有 $f_{n_1}\equiv f_{n_2}(\bmod x^q-x)$. 根据模$(x^q-x)$意义下的周期性,类似定理 3.3 的计算可得

$$\sum_{n\geqslant 0} f_n^2 z^n \equiv \frac{1}{1-z^s}\sum_{n=1}^{s} f_n^2 z^n (\bmod x^q-x) \tag{6}$$

联立式(2)和(6)有

$$\frac{1}{1-z^s}\sum_{n=1}^{s} f_n^2 z^n \equiv \frac{z}{1-z^2}+\Big(\frac{z}{1-z^2}\cdot \sum_{k=1}^{\frac{q-1}{2}} \frac{z^k(1-z)^{q-1-2k}}{(1-z)^{q-1}-z^{\frac{q-1}{2}}} x^{2k}\Big)(\bmod x^q-x).$$

同样,上式关于 $x\in F_q$ 求和可得

$$\sum_{n=1}^{s} A_n z^n \equiv \frac{z(1-z^s)z^{\frac{q-1}{2}}}{(1-z^2)((1-z)^{q-1}-z^{\frac{q-1}{2}})} (\bmod x^q-x).$$

化简上式有

$$\sum_{n=1}^{s} A_n z^n \equiv \frac{(z-z^{s+1})z^{\frac{q-1}{2}}(z^{\frac{q-1}{2}}+1)}{(z^{q-1}-1)(1+z)(1+z^{\frac{q+1}{2}})} (\bmod x^q-x).$$

从而

$$(1+z+z^{\frac{q+1}{2}}+z^{\frac{q+3}{2}})\sum_{n=1}^{s} A_n z^n = -(z^{\frac{q-1}{2}}+z^{q-1})\sum_{k=1}^{s-q+2} b_k z^k \tag{7}$$

比较式(7)关于项 z^i 的系数即可得到定理.

根据以上两个定理，任意给定 q，我们都可以算出每一个 $f_n^2(x)$ 在有限域 F_q 上的取值之和（即 A_n），从而可以得到一些 Fibonacci 多项式使其在 F_q 上不是置换多项式.

推论 3.5　设 f_n 为第 n 个 Fibonacci 多项式，$q=p^e$.

(i) 若 q 为奇数，则 $f_{\frac{q+1}{2}}$ 是 F_q 上的置换多项式的充要条件是 $q=3$；

(ii) 若 q 为奇数，则 $f_{\frac{q+3}{2}}$ 与 $f_{\frac{q+5}{2}}$ 不是 F_q 上的置换多项式.

证明　(i) 当 $p\equiv 3 \pmod 4$，e 为奇数时，若 $q=3$ 则 $f_{\frac{q+1}{2}}=f_2=x$ 在任意的有限域 F_q 上都是置换多项式. 若 $q>3$，根据定理 3.3 可以算出 $b_1=1$，$b_2=0$，$b_3=0$，则有 $A_{\frac{q+1}{2}}=-b_1=-1$. 从而根据引理 3.1 可知 $f_{\frac{q+1}{2}}$ 不是 F_q 上的置换多项式.

当 $p\equiv 1 \pmod 4$ 且 e 为任意数，或者 $p\equiv 3 \pmod 4$ 且 e 为偶数时，由定理 3.4 可知 $b_1=1$，$b_2=0$，$b_3=0$，$b_4=0$. 所以 $A_{\frac{q+1}{2}}=-b_1=-1$. 根据引理 3.1 可知 $f_{\frac{q+1}{2}}$ 不是 F_q 上的置换多项式. 综上，当 q 为奇数时，$f_{\frac{q+1}{2}}$ 是 F_q 上的置换多项式的充要条件是 $q=3$.

(ii) 当 $p\equiv 3 \pmod 4$，e 为奇数时，若 $q=3$，则 $f_{\frac{q+3}{2}}=f_3=x^2+1$，$f_{\frac{q+5}{2}}=f_4=x^3+2x$，此时 $b_1=1$，$b_2=0$，$b_3=1$. 则 $A_3=-b_2-A_1=0$，$A_4=-b_3-A_2=-1-(-1)=0$. 所以由引理 3.1 可知 f_3 和 f_4 都不是 F_3 上的置换多项式. 若 $q>3$，则 $b_1=1$，$b_2=0$，$b_3=0$，根据定理 3.3，

$$A_{\frac{q+3}{2}}=-b_2+b_1-A_1=1,$$

$$A_{\frac{q+5}{2}}=-b_3+b_2-b_1-A_2=-1.$$

于是由引理 3.1 可知 $f_{\frac{q+3}{2}}$ 与 $f_{\frac{q+5}{2}}$ 在有限域 F_q 上都不是置换多项式.

当 $p\equiv 1 \pmod 4$，e 为任意数，或者 $p\equiv 3 \pmod 4$，e 为偶数时，若 $q=5$ 则有 $b_1=1$，$b_2=0$，$b_3=0$，$b_4=0$，$A_4=-b_2+b_1=1$，$A_5=-(b_3+b_1)-(A_4+A_2+A_1)=-1-1=-2$. 由引理 3.1 知 f_4 和 f_5 在 F_5 上不是置换多项式. 当 $q>5$ 时，同样的有 $b_1=1$，$b_2=0$，$b_3=0$，$b_4=0$. 根据定理 3.4，

$$A_{\frac{q+3}{2}}=-b_2+b_1=1,$$

$$A_{\frac{q+5}{2}}=-b_3-(A_{\frac{q+3}{2}}+A_2+A_1)=-1.$$

由引理 3.1 可知 $f_{\frac{q+3}{2}}$ 与 $f_{\frac{q+5}{2}}$ 在有限域 F_q 上都不是置换多项式. 综上，当 q 为奇数时 $f_{\frac{q+3}{2}}$ 与 $f_{\frac{q+5}{2}}$ 不是 F_q 上的置换多项式.

参考文献：

[1] Fernando N, Rashid M H. Fibonacci permutation polynomials [EB/OL]. arxiv: 1712.07723v4.

[2] Cigler J. q-Fibonacci polynomials [J]. Fibonacci Quart, 2003, 41: 3140.

[3] Hoggatt V E, Bicknell Jr M. Roots of Fibonacci polynomials [J]. Fibonacci Quart, 1973, 11: 271.

[4] Koroglu M E, Ozbek I, Siap I. Optimal codes from Fibonacci polynomials and secret sharing schemes [J]. Arab J Math, 2017, 6: 297308.

[5] Kitayama H, Shiomi D. On the irreducibility of Fibonacci and Lucas polinamials over finite fields [J]. Finite Fields Appl, 2017, 48: 420.

[6] Tasyurdu Y, Deveci O. The Fibonacci polynomials in rings [J]. Ars Combin, 2017, 133: 355.

[7] Koshy T. Fibonacci and Lucas numbers with applications [M]. New York: Wiley, 2001.

[8] Lidl R, Niederreiter H. Finite fields [M]. Cambridge: Cambridge University Press, 1974.

引用本文格式：

中　文：王智坚. Fibonacci 多项式的置换性质[J]. 四川大学学报：自然科学版，2020，57：1047.

英　文：Wang Z J. Permutation properties of the Fibonacci polynomials [J]. J Sichuan Univ: Nat Sci Ed, 2020, 57: 1047.