arXiv:2305.06322v1 [math.NT] 10 May 2023

利用广义雷代函数构造置换多项式

丁志国和迈克尔·E·齐夫

Abstract. 我们确定了有限域上两个大型多项式类中的所有置换多项式。这两类多项式的构造都涉及一类有理函数的分母，该类函数推广了经典的雷代函数。我们的结果推广了文献中近期的八项结果；对于这些更一般结果，我们的证明比特殊情形的已有证明简短得多，也简单得多。

1. Introduction

本文确定了两个大型多项式族中的所有置换多项式。主要结果如下，其中 μ_{q+1} 表示 $\mathbb{F}_{q^2}^*$中所有$(q+1)$次单位根组成的集合。

定理 1.1。取正整数 r 和 n，满足 $r \equiv n$ (模 $q+1$)，取互不相同的 u、$v \in \mu_{q+1}$以及 a、$b \in \mathbb{F}_{q^2}^*$，并记

$$B(X) := a(X+u)^n + b(X+v)^n.$$

那么，$f(X) := X^r B(X^{q-1})$ 当且仅当$(b/a)^{q-1} \neq (v/u)^n$且$\gcd(rn, q-1) = 1$时，置换 $\mathbb{F}_{q^2}$。

定理 1.2. 取正整数 r, n，使得 $r \equiv n$ (模 $q+1$)，并取元素 $a, b, v \in \mathbb{F}_{q^2}^*$，满足 $v \notin \mu_{q+1}$，并记为

$$B(X) := a(X+v^{-q})^n + b(X+v)^n.$$

那么 $f(X) := X^r B(X^{q-1})$ 置换 $\mathbb{F}_{q^2}$，当且仅当 $bv^n/a \notin \mu_{q+1}$ 且 $\gcd(r, q-1) = 1 = \gcd(n, q+1)$。

<escape>我们还证明，定理 1.1 和 1.2 的特殊情形蕴含 [9, 定理 3.3 和 3.5], [11, 定理 1.1 和 1.2]，以及以下定理的修正版本 [4，定理 1 和 2] 和 [7，定理 8 和 9]。
</escape>

除了对这些多项式的简单描述之外，许多作者研究定理 1.1 和 1.2 中多项式的具体实例，其原因在于，从某种意义上说，这些多项式是由一类重要的有理函数构造而成的，这类函数称为 R´edei 函数。这些有理函数最初是在 [8] 奇数阶有限域上引入的，而在 [6]

Date: 2023年5月11日。*Key words and phrases.* 置换多项式，有限域，R´edei 函数。

在偶数阶有限域上。R´edei 函数具有如下形式： $\rho(X) \circ X^n \circ \eta(X)$，其中 ρ、$\eta \in \mathbb{F}_{q^2}(X)$ 是某些一次有理函数。定理 1.1 和 1.2 中的多项式$B(X)$ 是此类有理函数的分母，其中 $\rho(X)$ 和 $\eta(X)$ 允许属于比 R´edei 函数定义中所使用的更一般的一次有理函数类。由于 R´edei 函数能够在某些有限域上诱导置换，因此，直观而言，由 R´edei 函数的分母构造出的多项式也可能诱导置换，这或许是合理的。然而，这种联系并非显而易见；当我们使用广义 R´edei 函数而非 R´edei 函数时，这种联系就显得更加神秘。

R´edei 函数与置换多项式之间的联系最早见于 [11], ，随后又在 [4, 7, 9]中得到进一步发展。上述论文均使用经典 R´edei 函数的某些特例。本文从三个方面进行了推广：研究所有经典 R´edei 函数，而不仅限于特定特例；同时讨论奇数和偶数 q；并使用上文讨论的广义 R´edei 函数。我们得到了比以往论文中的结果一般得多的结论。证明结合了 [11] 中的部分策略和其他思路。这使论证尤为简洁，且比我们结果中特例的先前证明显著短得多。我们指出，´中对 R [1], edei 函数作了简明的概念性阐述，而全面的论述将见于我们即将发表的论文 [3]。

本文的组织结构如下。下一节将介绍本文所使用的符号，并回顾一些简单的已知结果。随后，我们将在第1.1节和第1.2 节中证明定理3。最后，在第4节中，我们将描述定理1.1 和1.2 的具体特殊情形，这些情形蕴含了文献中已有的八个结果，从而结束本文。

2. Background results

本节将回顾一些简单的已知结果。

2.1. 记号。 本文通篇使用以下记号和术语：

- q 是一个固定的素数幂；
- μ_{q+1} 表示 $\mathbb{F}_{q^2}$中$(q+1)$次单位根的集合；
- $\mathbb{P}^1(\mathbb{F}_q) := \mathbb{F}_q \cup \{\infty\}$;
- 对于任意 $g(X) \in \mathbb{F}_{q^2}(X)$，我们将 $g^{(q)}(X)$ 记为由 $g(X)$ 中的每个系数替换为其 q 次幂后得到的有理函数；
- 非零有理函数 $g(X)$ 的次数是 $N(X)$ 和 $D(X)$ 的次数中的较大者，其中 $N(X)$ 和 $D(X)$ 是任意给定的互素多项式，满足 $g(X) = N(X)/D(X)$。

2.2. 置换与单位根。 以下结果是 [10,引理 21]的一个特例。

引理 2.1。设 $f(X) = X^r B(X^{q-1})$，其中 r 是正整数，q 是素数幂，且 $B(X) \in \mathbb{F}_{q^2}[X]$。那么，当且仅当$\gcd(r, q-1) = 1$ 且 $g_0(X) := X^r B(X)^{q-1}$ 置换 μ_{q+1}时，$f(X)$ 置换 $\mathbb{F}_{q^2}$。

以下结果概述了 [11]，中引入的一个过程，具体说明见 [12,引理 2。2]。

引理 2.2。设 q 是一个素数幂，并记 $g_0(X) = X^r B(X)^{q-1}$，其中 $r \in \mathbb{Z}$，且 $B(X) \in \mathbb{F}_{q^2}[X]$。那么，$g_0(X)$ 是 μ_{q+1} 上的置换，当且仅当 $B(X)$ 在 μ_{q+1} 中无根，且 $g(X) := X^r B^{(q)}(1/X)/B(X)$ 是 μ_{q+1} 上的置换。

引理 2.3。记 $g(X) := X^n B^{(q)}(1/X)/B(X)$ 为某个非零的 $B(X) \in \mathbb{F}_{q^2}[X]$ 与某个整数 n，且满足 $n \geq \deg(B)$。若 $\deg(g) = n$，则 $B(X)$ 在 μ_{q+1} 中无根，且 $g(\mu_{q+1}) \subseteq \mu_{q+1}$。

证明。注意到 $g(X) = N(X)/B(X)$，其中 $N(X) := X^n B^{(q)}(1/X)$，并且假设 $n \geq \deg(B)$ 意味着 $N(X) \in \mathbb{F}_{q^2}[X]$。由于

$$\max(\deg(B), \deg(N)) \leq n = \deg(g) \leq \max(\deg(B), \deg(N)),$$

第二个不等式必为等式，因此 $B(X)$ 和 $N(X)$ 互素。由此可知，$B(X)$ 在 μ_{q+1} 中没有根，因为若 $\alpha \in \mu_{q+1}$ 是 $B(X)$ 的根，则 $0 = B(\alpha)^q = B^{(q)}(1/\alpha)$，因此 α 也是 $N(X)$ 的根，这与 $B(X)$ 和 $N(X)$ 互素相矛盾。因此，对于任意 $\alpha \in \mu_{q+1}$，有

$$g(\alpha)^q = \Big(\frac{\alpha^n B^{(q)}(1/\alpha)}{B(\alpha)}\Big)^q = \frac{B(\alpha)}{\alpha^n B^{(q)}(1/\alpha)} = \frac{1}{g(\alpha)},$$

因此 $g(\alpha) \in \mu_{q+1}$，从而 $g(\mu_{q+1}) \subseteq \mu_{q+1}$。 □

2.3. **一次有理函数**。我们从一次有理函数众所周知且易于证明的描述开始。

引理 2.4. 对于满足 $\{\gamma, \delta\} \neq \{0\}$ 的 α、β、γ、$\delta \in \mathbb{F}_{q^2}$，有理函数$(\alpha X + \beta)/(\gamma X + \delta)$ 的次数为 1 当且仅当 $\alpha\delta \neq \beta\gamma$。

接下来我们注意到，在有理函数的两侧复合一次有理函数，其次数保持不变：

引理 2.5. 对于任意非常值 $g(X) \in \mathbb{F}_{q^2}(X)$，以及任意一次$\rho, \eta \in \mathbb{F}_{q^2}(X)$，$\eta(g(\rho(X)))$ 的次数为$\deg(g)$。

证明。这很容易直接验证。或者，由以下事实可知：如果 x 在 $\mathbb{F}_{q^2}$ 上超越，且 $h(X) \in \mathbb{F}_{q^2}(X)$ 非常数，则 $\deg(h) = [\mathbb{F}_{q^2}(x) : \mathbb{F}_{q^2}(h(x))]$（例如参见 [2, 引理 2.2]）。 □

接下来的两个结果是对 [11, 引理 2.1 和 3.1]的重新表述。

引理 2.6. 若 $\alpha, \beta \in \mathbb{F}_{q^2}$ 满足 $\alpha^{q+1} \neq \beta^{q+1}$，则 $(\beta^q X + \alpha^q)/(\alpha X + \beta)$置换 μ_{q+1}。

引理 2.7。若 $\alpha \in \mathbb{F}_{q^2} \setminus \mathbb{F}_q$ 且 $\beta \in \mu_{q+1}$，则 $(\alpha X + \beta\alpha^q)/(X + \beta)$ 将μ_{q+1} 双射到 $\mathbb{P}^1(\mathbb{F}_q)$。

3. Proofs of main results

在本节中，我们证明定理 1.1和1.2。

定理 1.1 的证明。由引理 2.1 和 2.2， $f(X)$ 置换 $\mathbb{F}_{q^2}$ 当且仅当 $\gcd(r, q-1) = 1$, $B(X)$ 在 μ_{q+1} 中没有根，并且有理函数 $g(X) := X^n B^{(q)}(1/X)/B(X)$ 置换 μ_{q+1}。显然， $B(X) \neq 0$ ，并且

$$X^n B^{(q)}(1/X) = a^q u^{-n}(X+u)^n + b^q v^{-n}(X+v)^n,$$

以便使得

$$g(X) = \frac{a^q u^{-n} X + b^q v^{-n}}{aX+b} \circ X^n \circ \frac{X+u}{X+v}.$$

根据引理 2.4，当 $a^q u^{-n} b = b^q v^{-n} a$ 时， $g(X)$ 为常数（因此不是双射），或者等价地，$(b/a)^{q-1} = (v/u)^n$。现在假设 $(b/a)^{q-1} \neq (b/u)^n$，则根据引理 2.4，$(a^q u^{-n} X + b^q v^{-n})/(aX+b)$ 和 $(X+u)/(X+v)$ 的次数均为一，因此由引理 2.5 可得 $\deg(g) = n$。于是，引理 2.3 表明， $B(X)$ 在 μ_{q+1} 中没有根，且 $g(\mu_{q+1}) \subseteq \mu_{q+1}$。因此，$g(X)$ 置换 μ_{q+1} 当且仅当 $g(X)$ 在 μ_{q+1} 上是单射的。取 w ，使得 $w^{q-1} = u/v$。则 $w \in \mathbb{F}_{q^2} \setminus \mathbb{F}_q$ 和

$$\frac{X+u}{X+v} = w^{-1}\frac{wX+vw^q}{X+v} = w^{-1}\rho(X),$$

其中 $\rho(x) := (wX + vw^q)/(X+v)$ 由引理 2.7 诱导出一个双射 $\mu_{q+1} \to \mathbb{P}^1(\mathbb{F}_q)$。因此，对某个一次 $\eta(X) \in \mathbb{F}_{q^2}(X)$，有 $g(X) = \eta(X) \circ X^n \circ \rho(X)$，从而 $g(X)$ 在 μ_{q+1} 上是单射，当且仅当 X^n 在$\mathbb{P}^1(\mathbb{F}_q)$上是单射，等价地，$\gcd(n, q-1) = 1$。□

定理 1.2 的证明。由引理 2.1 和 2.2， $f(X)$ 置换 $\mathbb{F}_{q^2}$ 当且仅当 $\gcd(r, q-1) = 1$, $B(X)$ 在 μ_{q+1} 中无根，且有理函数 $g(X) := X^n B^{(q)}(1/X)/B(X)$ 置换 μ_{q+1}。显然 $B(X) \neq 0$ ，并且

$$X^n B^{(q)}(1/X) = a^q v^{-n}(X+v)^n + b^q v^{qn}(X+v^{-q})^n,$$

因此

$$g(X) = \frac{a^q v^{-n} X + b^q v^{qn}}{bX+a} \circ X^n \circ \frac{X+v}{X+v^{-q}}.$$

根据引理 2.4， $g(X)$ 是常数（因此不是双射），当且仅当 $a^{q+1} v^{-n} = b^{q+1} v^{qn}$，等价地， $bv^n/a \in \mu_{q+1}$。现在假设 $bv^n/a \notin \mu_{q+1}$，于是由引理 2.4 可知，$(a^q v^{-n} X + b^q v^{qn})/(bX+a)$ 和 $(X+v)/(X+v^{-q})$ 的次数均为 1，进而由引理 2.5 得到 $\deg(g) = n$。接着，引理 2.3 表明 $B(X)$ 在 μ_{q+1} 中没有根，且 $g(\mu_{q+1}) \subseteq \mu_{q+1}$。因此， $g(X)$ 是 μ_{q+1} 的置换，当且仅当 $g(X)$ 在 μ_{q+1} 上是单射。这里，根据引理 2.6， $\rho(X) := (X+v)/(v^q X+1)$ 是 μ_{q+1} 的置换，因此 $g(X)$ 在 μ_{q+1} 上是单射，当且仅当 X^n 在 μ_{q+1} 上是单射，等价地，$\gcd(n, q+1) = 1$。□

4. Connection with previous results

定理 1 与 [4, 定理 2] （限定在情形 $n+m(q+1) > 0$ 成立时）所得的结论，包含在以下特殊情形的结果组合之中：

- 定理 1.1 同时满足 $b = \pm a$ 和 $v = -u$;
- 定理 1.2 同时具有 $b = \pm a$ 和 $v^{q+1} = -1$。

一个反例是 [4, 定理 1 和 2]，在这种情况下，这些结果中关于 $n = 1 = -m$和 n 的条件均得到满足，但这些结果中的函数 $m(P)$ 却不能将 x映射为一个置换 $\mathbb{F}_{q^2}$。

[7, 定理 8] 的一个修正版包含在定理 1.1 的特殊情形中，其中 q 为偶数，$a = b = 1$，且 $\{u, v\} = \mathbb{F}_4 \setminus \mathbb{F}_2$。在这一特殊情形下，我们的结果给出的置换条件为 $\gcd(rn, q-1) = 1$ 且 $3 \nmid n$。相比之下，[7, 定理 8] 中的条件为 $\gcd(r, q-1) = 1 = \gcd(n, q^2-1)$。[7, 定理 8] 的一个反例是 $q = 32$、$n = 11$和$r = n+q+1$（或用 [7]的记号表示为 $m = 1$），它给出了 $\mathbb{F}_{q^2}$ 的一个置换，却违反了 [7, 定理 8] 中的条件 $\gcd(n, q^2-1) = 1$。

[7, 定理 9]的修正版包含在定理 1.1 的特殊情形中，其中 q 为偶数，$a = v$、$b = u$和 $\{u, v\} = \mathbb{F}_4 \setminus \mathbb{F}_2$。在这一特殊情形下，我们的结果给出的置换条件为 $\gcd(rn, q-1) = 1$且 $n \not\equiv 2 \pmod 3$。相比之下，[7, 定理 9] 中的条件写作（记 $r = n+m(q+1)$）“$\gcd(n+m(q+1)\ q-1) = 1$，且 $\gcd(n, q^2-1) = 1$，当 $n \equiv 1 \pmod 3$时”。尽管这句话有歧义，但所有合理的解释都与例子 $q = 128$、$n = 43$和 $r = n+q+1$（因此 $m = 1$）相矛盾；该例给出了 $\mathbb{F}_{q^2}$ 的一个置换，满足 $n \equiv 1 \pmod 3$，但 $\gcd(n, q^2-1) \neq 1$。这里我们还指出，[7, 定理 9] 陈述中展示的恒等式是错误的。若以与 [7, 定理 8]相同的方式定义数a_i，则该恒等式成立。为避免这一错误恒等式造成混淆，我们指出，[7, 定理 8]的修正版采用了 [7, 第 5], 页底部的 $N_n(x)$定义，以及 [7, 第 4]页底部的 $N_n(x, \alpha)$定义。

定理 1.1 在 $a = (-b)^n$ 和 $u = vb^{q-1}$ 的特殊情形给出[9, 定理 3.5] 和 [11, 定理 1.2]。定理 1.2 在 $a = -1/v$ 和 $b = 1/v^n$ 的特殊情形给出 [9, 定理 3.3] 和 [11, 定理 1.1] 在两侧分别复合以标量倍数之后。

最后，我们指出，[4]和 [7]强调，R´edei 函数可以递归计算，其方法等价于通过$n-1$次乘法计算 n 次幂。在 [5]中给出了一种快得多的计算 R´edei 函数的方法，类似于通过重复平方计算 n 次幂的方法（所需乘法次数少于 $2\log_2(n)$）。

References

[1] Z. Ding 和 M. E. Zieve, *Tangent-Chebyshev rational maps and Rédei functions*, arXiv:2103.08128v1, 2021 年 3 月 15 日。2

[2] Z. Ding 和 M. E. Zieve, *Low-degree permutation rational functions over finite fields*, 《数论学报》 **202** 2022 253 280 3 ( ), –。Z. Ding 和 M. E. Zieve, [3] *Rédei functions* 2 , 预印本。S. Fu、X. Feng、D. Lin 和 Q. Wang, [4] *A recursive construction of permutation polynomials over* $\mathbb{F}_{q^2}$ *with odd characteristic related to Rédei functions* , 《设计、编码与密码学》 **87** 2019 1481 1498 1, 2, 5 ( ), –。W. More, *Fast evaluation of Rédei functions*, 《应用代数、工程、通信与计算》 **6** 1995 171 173 5 ( ), –。W. Nobauer, *Rédei-Funktionen für Zweierpotenzen*, 《匈牙利数学期刊》17 (1986), 37–44。1[7] D. Panario, N. Uyar 和 Q. Wang, [6] *A construction of permutation polynomials using Rédei function in even characteristic* 2305 03521 1, 5 2023 , arXiv: 。v May 。[8] ´ *Über eindeutig umkehrbare Polynome in endlichen Körpern* L. Redei, , 《塞格德大学学报：数学与科学辑》 **11** 1946 85 92 1 ( ), –。D. Wu、P. Yuan、C. Ding 和 Y. Ma, *Permutation trinomials over* $\mathbb{F}_{2^m}$, 《有限域及其应用》 **46** 2017 38 56 1, 2, 5 ( ), –。M. E. Zieve, *Some families of permutation polynomials over finite fields*, 《数论国际期刊》 **4** 2008 851 857 2 ( ), –。M. E. Zieve, [10] *Permutation polynomials on* $\mathbb{F}_q$ *induced from Rédei function bijections on subgroups of* $\mathbb{F}_q^*$ 1310 0776 2, 7 2013 1, 2, , 《月刊数学》, 即将发表。arXiv: 。v Oct 。[12] M. E. Zieve, *A note on the paper arXiv:2112.14547*, arXiv:2201.01106v2, 2022年8月2日。3

Hunan Institute of Traffic Engineering, Hengyang, Hunan 421001 China
Email address: ding8191@qq.comDepartment of Mathematics,
University of Michigan, 530 Church Street,Ann Arbor, MI 48109-1043 USA
Email address: zieve@umich.edu*URL*: http://www.math.lsa.umich.edu/∼zieve/