Wuhan University
Journal of Natural Sciences

2022, Vol.27 No.5, 372-374

Article ID 1007-1202(2022)05-0372-03
DOI https://doi.org/10.1051/wujns/2022275372

A Class of *n*-to-1 Binomials over Finite Fields

□ QIN Xiaoer[1], YAN Li[2†]

1. School of Mathematics and Big Data, Chongqing University of Education, Chongqing 400065, China;

2. School of Mathematical Sciences, Chongqing Normal University, Chongqing 401331, China

Abstract: n-to-1 mappings have many applications in combinatorial design, coding theory and cryptography. In this paper, by using piecewise method and monomials on subsets of $q+1$-th roots of unity, we show a class of n-to-1 binomials having the form $x^r(a+x^{s(q-1)})$ over F_{q^2}.

Key words: finite field; n-to-1 mapping; binomial
CLC number: O 156.1

Received date: 2022-06-22
Foundation item: Supported by the National Natural Science Foundation of China (11926344)
Biography: QIN Xiaoer, male, Ph. D., Associate professor, research direction: finite fields. E-mail: qincn328@sina.com
† To whom correspondence should be addressed. E-mail: yanl930@163.com

0 Introduction

Let n be a positive integer and F_q be the finite field having q elements. n-to-1 mappings (see Definition 1) of finite fields have wide applications in cryptography, finite geometry, coding theory and combinatorial design, and it has become an interesting topic in finite fields. Especially, when $n=1$, n-to-1 mappings become permutation polynomials.

The study of permutation polynomials has a long history in finite fields, many classes of permutation polynomials are studied, and there are a few surveys on permutation polynomials[1-3]. When $n=2$, Mesnager and Qu[4] studied 2-to-1 mappings of finite fields, and gave many explicit constructions of 2-to-1 mappings. Recently, Li *et al*[5] continued to study 2-to-1 mappings, and constructed several classes of 2-to-1 trinomials and quadrinomials over finite fields. Yuan *et al*[6] constructed a few classes of 2-to-1 mappings having the form $g\left(x^q-x+\delta\right)+x$ over $F_{2^{2m}}$. More recently, Gao *et al*[7] generalized the definition of 2-to-1 mappings to n-to-1 mappings. Niu *et al*[8] showed some approaches to construct n-to-1 mappings of finite fields. Therefore, to find more classes of n-to-1 mappings of finite fields still is an open problem. In this paper, we focus on constructing n-to-1 binomials over F_{q^2}. By using monomials and piecewise method, the authors[9-12] characterized several classes of permutation polynomials. Activated by the method, we generalized this approach to construct some n-to-1 binomials with the form $x^r h(x^{q-1})$ of F_{q^2}.

1 Preliminaries

In Ref.[8], the authors gave the definition of n-to-1 mappings as follows:

Definition 1[8] Let f be a mapping from one finite set A to another finite set B. Then f is called an n-to-1 mapping if one of the following two cases holds:

(1) if n divides $\#A$, for any b in B, it has either n or 0 preimages in A ;

(2) if n does not divide $\#A$, for almost b in B, it has either n or 0 preimages in A, and for only one exception element, it has exactly $\#A \pmod n$ preimages in A.

Lemma 1[8] Let $f(x)=ax^d$ be a monomial over F_q, where $a\neq 0$, and A be a subset in F_q. Then f is an n-to-1 mapping over A if and only if $\gcd(d,\#A)=n$.

In Ref.[8], the authors established an AGW-like criterion for n-to-1 mappings in the following.

Lemma 2[8] Let A, S and $\bar{S}$ be finite sets with $\#S=\#\bar{S}$, and $\#A\equiv\#S \pmod n$. Let $f: A\to A$, $g: S\to\bar{S}$, $\lambda: A\to S$, and $\bar{\lambda}: A\to\bar{S}$ be maps such that $\bar{\lambda}\circ f=g\circ\lambda$, where both λ and $\bar{\lambda}$ are surjective.

Assume that f is a bijection form $\lambda^{-1}(s)$ to $\bar{\lambda}^{-1}(g(s))$ for every $s\in S$. There are three statements as follows:

1) f is an n-to-1 mapping of A;

2) g is an n-to-1 mapping from S to $\bar{S}$;

3) n divides $\#A$ and that n does not divide $\#A$ and the exception $\bar{s}_0\in\bar{S}$ which has t preimages in S satisfies $\bar{\lambda}^{-1}(\bar{s}_0)=1$ where $t\equiv\#A \pmod n$.

Then, if 1) holds, so does 2). If both 2) and 3) hold, so does 1).

As a special case of Lemma 2, the authors of Ref. [8] gave the following result.

Lemma 3[8] Let q be a prime power, r be a positive integer such that $\gcd(r,q-1)=1$ and $n|(q+1)$. Let $f(x)=x^r h(x^{q-1})$, where $h(x)\in F_{q^2}[x]$ such that $h(x)\neq 0$ if $x\neq 0$. Then $f(x)$ is an n-to-1 mapping over F_{q^2} if and only if $x^r h(x)^{q-1}$ is an n-to-1 mapping over μ_{q+1}.

2 Main Results

In this section, we will focus on constructing some n-to-1 mappings over F_{q^2}.

Theorem 1 Let q be a prime power, and r,s,n be positive integers having $\gcd(r,q-1)=1$. Let a in F_{q^2} satisfy $a^{q+1}=1$ and $a+x^s$ have no roots in μ_{q+1}. Then $f(x)=x^r(a+x^{s(q-1)})$ is an n-to-1 mapping over F_{q^2} if and only if $\gcd(r-s,q+1)=n$.

Proof By using Lemma 3, we know that $f(x)$ is an n-to-1 mapping over F_{q^2} if and only if $g(x)=x^r(a+x^s)^{q-1}$ is an n-to-1 mapping over μ_{q+1}. Thus we only need to show that $g(x)$ is an n-to-1 mapping over μ_{q+1} if and only if $\gcd(r-s,q+1)=n$.

By $a+x^s$ having no roots in μ_{q+1}, we can rewrite $g(x)$ as

$$g(x)=x^r(a+x^s)^{q-1}=x^r\frac{(a+x^s)^q}{a+x^s}=x^r\frac{a^q+x^{-s}}{a+x^s}$$
$$=a^q x^{r-s}\frac{x^s+\dfrac{1}{a^q}}{a+x^s}.$$

Since $a^{q+1}=1$, we get that $\dfrac{1}{a^q}=a$. Thus $g(x)=a^q x^{r-s}$. Then by Lemma 1, it follows that $g(x)$ is an n-to-1 mapping over μ_{q+1} if and only if $\gcd(r-s,q+1)=n$.

The proof of Theorem 1 is completed.

Furthermore, if we divide μ_{q+1} as $\mu_{q+1/2}$ and $-\mu_{q+1/2}$, then the n-to-1 property on μ_{q+1} is translated to that on $\mu_{q+1/2}$ and $-\mu_{q+1/2}$.

Lemma 4 Let $(q+1)/d$ and n be positive integers with $n|(q+1)/d$, and $A_i\in\mu_{q+1}$ for $0\leqslant i\leqslant d-1$. For $g(x)\in F_{q^2}[x]$, if $g(x)=A_i x^{r_i}$, for $x\in S_i$. Then $g(x)$ is an n-to-1 mapping of μ_{q+1} if and only if each of following is true:

(1) $\gcd(r_i,(q+1)/d)=n$, for $0\leqslant i\leqslant d-1$;

(2) $A_i x_i^{r_i}\neq A_j x_j^{r_j}$, for $x_i\in S_i$ and $x_j\in S_j$.

Proof By using Lemma 1 and Theorem 1.2 in Ref.[11], we can easily get the desired result.

By using Lemma 4, we can get the following result.

Theorem 2 Let q be a prime power with $q\equiv 1 \pmod 4$, and r,n be positive integers having $\gcd(r,q-1)=1$ and $n|(q+1)/2$. Let s be an even number and a in F_{q^2} satisfy $a^{(q+1)/2}=1$. Then $f(x)=x^r(a+x^{s(q-1)})$ is an n-to-1 mapping over F_{q^2} if and only if $\gcd(r-s,(q+1)/2)=n$.

Proof By Lemma 3, we know that $f(x)$ is an n-to-1 mapping of F_{q^2} if and only if $\gcd(r,q-1)=1$ and $g(x)=x^r(a+x^s)^{q-1}$ is an n-to-1 mapping over μ_{q+1}.

In the following, we will focus on proving that $g(x)$ is an n-to-1 mapping over μ_{q+1}.

First, we consider the case of $x \in \mu_{q+1/2}$. Since $q \equiv 1 \pmod 4$, then $q+1/2$ is odd. By using $a^{q+1/2}=1$, it implies from n being even that $a+x^s \neq 0$ for any $x \in \mu_{q+1/2}$. Thus

$$g(x)=x^r\frac{(a+x^s)^q}{a+x^s}=x^r\frac{a^q+x^{-s}}{a+x^s}=a^q x^{r-s}\frac{x^s+\dfrac{1}{a^q}}{a+x^s}.$$

It follows from $a^{q+1/2}=1$ that $g(x)=a^q x^{r-s}$. We get that $g(x)$ is an n-to-1 mapping of $\mu_{q+1/2}$ if and only if $\gcd(r-s, q+1/2)=n$.

Next, for $x \in -\mu_{q+1/2}$, it is also trivial to find that $a+x^s$ has no roots in $-\mu_{q+1/2}$. We reduce that $g(x)=a^q x^{r-s}$. It is easy to conclude that $g(x)$ is an n-to-1 mapping of $-\mu_{q+1/2}$ if and only if $\gcd(r-s, q+1/2)=n$.

Then by Lemma 4, we get that $g(x)$ is an n-to-1 mapping over μ_{q+1} if and only if $\gcd(r-s, q+1/2)=n$. Therefore, we can conclude that $f(x)$ is an n-to-1 mapping over F_{q^2} if and only if $\gcd(r-s, q+1/2)=n$. We complete the proof of Theorem 2.

References

[1] Hou X D. Permutation polynomials over finite fields—A survey of recent advances [J]. *Finite Fields Appl*, 2015, **32**: 82-119.

[2] Li N Q, Zeng X Y. A survey on the applications of Niho exponents [J]. *Cryptogr Commun*, 2019, **11**(3): 509-548.

[3] Wang Q. Polynomials over finite fields: An index approach [J]. *Combinatorics and Finite Fields*: *Difference Sets*, *Polynomials*, *Pseudorandomness and Applications*, 2019, **23**: 319-348.

[4] Mesnager S, Qu L J. On two-to-one mappings over finite fields [J]. *IEEE Transactions on Information Theory*, 2020, **65**(12): 7884-7895.

[5] Li K Q, Mesnager S, Qu L J. Further study of 2-to-1 mappings over $F_{2^{2n}}$[J]. *IEEE Transactions on Information Theory*, 2021, **67**(6): 3486-3496.

[6] Yuan M, Zheng D B, Wang Y P. Two-to-one mappings and involutions without fixed points over $F_{2^{2n}}$[J]. *Finite Fields Appl*, 2021, **76**: 101913.

[7] Gao Y, Yao Y F, Shen L Z. *m*-to-1 mappings over finite fields F_q[J]. *IEICE Transactions on Fundamentals of Electronics*, *Communications and Computer Sciences*, 2021, **E104.A**(11): 1612-1618.

[8] Niu T L, Li K Q, Qu L J, *et al*. Characterizations and constructions of *n*-to-1 mappings over finite fields [EB/OL]. [2020-10-29]. *https://arXiv.org/abs/*2201.10290v1 [cs.IT].

[9] Kyureghyan K, Zieve M. Permutation polynomials of the form $x+\gamma Tr(x^k)$[C]// *Contemporary Developments in Finite Fields and Applications*. Singapore: World Scientific, 2016: 178-194.

[10] Lavorante V. New families of permutation trinomials constructed by permutations of μ_{q+1}[EB/OL]. [2021-10-12]. *https//arXiv.org/abs/*2105.12012.v4 [math.CO].

[11] Qin X E, Yan L. Constructing permutation trinomials via monomials on the subsets of μ_{q+1}[J]. *Applicable Algebra in Engineering*, *Communication and Computing*, 2021, **33**: 505-512. DOI: 10.1007/s00200-021-00505-8.

[12] Zheng D B, Yuan M, Yu L. Two types of permutation polynomials with special forms [J]. *Finite Fields Appl*, 2019, **56** : 1-16.

□