ARTICLE IN PRESS

Discrete Applied Mathematics ▮ (▮▮▮▮) ▮▮▮–▮▮▮

Contents lists available at ScienceDirect

Discrete Applied Mathematics

journal homepage: www.elsevier.com/locate/dam

# Compositional inverses and complete mappings over finite fields☆

Aleksandr Tuxanidy, Qiang Wang*

*School of Mathematics and Statistics, Carleton University, Ottawa, ON K1S 5B6, Canada*

ARTICLE INFO

*Article history:*
Received 6 March 2015
Received in revised form 25 July 2016
Accepted 4 September 2016
Available online xxxx

*Keywords:*
Permutation polynomials
Complete mappings
Compositional inverse
Linearized polynomials
Finite fields

ABSTRACT

We study compositional inverses of permutation polynomials and complete mappings over finite fields. Recently the compositional inverses of linearized permutation binomials were obtained in Wu (2013). In this paper we obtain compositional inverses of a class of linearized binomials permuting the kernel of the trace map. It was also shown in Tuxanidy and Wang (2014) that computing inverses of bijections of subspaces has an application in determining the compositional inverses of certain permutation classes related to linearized polynomials. Consequently, we give the compositional inverse of a new class of complete mappings. This complete mapping class extends several recent constructions given in Laigle-Chapuy (2007), Samardjiska and Gligoroski (2014), Wu and Lin (2013), Wu and Lin (2015), Wu et al. (2013). We also construct recursively a class of complete mappings involving multi-trace functions.



## 1. Introduction

Let $q = p^m$ be the power of a prime number $p$, let $\mathbb{F}_q$ be a finite field with $q$ elements, and let $\mathbb{F}_q[x]$ be the ring of polynomials over $\mathbb{F}_q$. We call a polynomial $f \in \mathbb{F}_q[x]$ a *permutation polynomial* (PP) over $\mathbb{F}_q$ if it induces a permutation of $\mathbb{F}_q$ under evaluation. We denote the *composition* of two polynomials $f, g$ by $(f \circ g)(x) := f(g(x))$. It is clear that permutation polynomials over $\mathbb{F}_q$ form a group under composition and subsequent reduction modulo $x^q - x$ that is isomorphic to the symmetric group on $q$ letters. Thus for any permutation polynomial $f \in \mathbb{F}_q[x]$ there exists a unique $f^{-1} \in \mathbb{F}_q[x]$ of degree less than $q$ satisfying $f(f^{-1}(x)) \equiv f^{-1}(f(x)) \equiv x \pmod{x^q - x}$. We call $f^{-1}$ the *compositional inverse* of $f$ over $\mathbb{F}_q$.

The construction of permutation polynomials over finite fields is an old and difficult subject that continues to attract interest due to their applications in cryptography [23,26], coding theory [8,16], and combinatorics [9]. See also [3,2,1,4,5,7,11–16,18,19,32,40–44], and the references therein for some recent work in the area. However, the problem of determining the compositional inverse of a permutation polynomial seems to be an even more complicated problem. In fact, there are very few known permutation polynomials whose explicit compositional inverses have been obtained [6,20,29–31,34,39], and the resulting expressions are usually of a complicated nature except for the classes of the permutation linear polynomials, monomials, Dickson polynomials. In addition, see [20,30] for the characterization of the inverse of permutations of $\mathbb{F}_q$ with form $x^r f(x^s)$ where $s \mid (q-1)$.

Of particular interest in the study of permutations of finite fields are the linearized polynomials. Polynomials with form $L(x) := \sum_{i=0}^{n-1} a_i x^{q^i}$ are called *linearized polynomials* or *q-polynomials*, which are $\mathbb{F}_q$-linear maps when seen as operators of

☆ Research of the authors is partially supported by OGS and NSERC, respectively, of Canada.

* Corresponding author.
*E-mail addresses:* AleksandrTuxanidyTor@cmail.carleton.ca (A. Tuxanidy), wang@math.carleton.ca (Q. Wang).

http://dx.doi.org/10.1016/j.dam.2016.09.009
0166-218X/

$\mathbb{F}_{q^n}$. Note that $L$ is a permutation polynomial over $\mathbb{F}_{q^n}$ if and only if its associate *Dickson matrix* given by

$$D_L = \begin{pmatrix} a_0 & a_1 & \cdots & a_{n-1} \\ a_{n-1}^q & a_0^q & \cdots & a_{n-2}^q \\ \vdots & \vdots & & \vdots \\ a_1^{q^{n-1}} & a_2^{q^{n-1}} & \cdots & a_0^{q^{n-1}} \end{pmatrix} \tag{1}$$

is non-singular [17]. We denote by $\mathscr{L}_n(\mathbb{F}_{q^n})$ the set of all $q$-polynomials over $\mathbb{F}_{q^n}$. Recently Wu and Liu obtained in [38] an expression for the compositional inverse of $L$ in terms of cofactors of $D_L$. Then using this result Wu computed in [34] the compositional inverses, in explicit form, of arbitrary linearized permutation binomials over finite fields.

More recently, Tuxanidy and Wang showed in [29] that the problem of computing the compositional inverses of certain classes of permutations is equivalent to obtaining the inverses of two other polynomials bijecting subspaces of the finite field, where one of these two is a linearized polynomial inducing a bijection between kernels of other linearized polynomials. For this they showed in Theorem 2.5 of [29] how to obtain linearized polynomials inducing the inverse map over subspaces on which a linearized polynomial induces a bijection. This in fact amounts to solving a system of linear equations. Thus, in particular, it is of interest to obtain explicit compositional inverses of linearized permutations of subspaces.

Denote by $T_{q^n|q} : \mathbb{F}_{q^n} \to \mathbb{F}_q$ the (linearized) *trace* map given by

$$T_{q^n|q}(x) = \sum_{i=0}^{n-1} x^{q^i}.$$

When it will not cause confusion, we abbreviate this with $T$. In Section 2 of this paper we determine a class of linearized binomials permuting the kernel of the trace map and proceed to obtain its inverses on the kernel. See Theorem 2.4 for more details.

*Complete permutation polynomials* (CPP) over $\mathbb{F}_q$, also called *complete mappings*, are permutation polynomials $f \in \mathbb{F}_q[x]$ such that $f(x) + x$ is also a permutation polynomial over $\mathbb{F}_q$. CPPs have recently become a strong source of interest due to their connection to combinatorial objects such as orthogonal Latin squares [10,24,25], and due to their applications in cryptography; in particular, in the construction of bent functions [21,22,25,27]. See also [28,36,37,35] and the references therein for some recent work in the area. In Section 3 we study complete mappings and give an improvement (Theorem 3.3) to Theorem 3.7 of [36] by Wu–Lin. This result generalized some earlier corresponding ones found in [15,25,37,35]. We also give a recursive construction of complete mappings involving multi-trace functions (see Theorem 3.6). In addition we employ the CPP class of Theorem 3.3 to construct a set of mutually orthogonal complete mappings (see Corollary 3.8). Two mappings $f, g$, of $\mathbb{F}_q$, are said to be *orthogonal* if $f - g$ permutes $\mathbb{F}_q$. Note in particular that from such a set one may also readily obtain a set of mutually orthogonal Latin squares, an object of special interest in the literature (see for example [10]).

As an application of Theorem 2.4 where we obtained the compositional inverses of linearized binomials permuting the kernel of the trace, we derive in Section 4 the compositional inverse of the complete permutation class in Theorem 3.3 generalizing some of the classes recently studied in [15,25,36,37,35]. Note that since inverses of complete mappings are also complete mappings, Theorem 4.2 and Corollary 4.3 imply the construction of a new, if rather complicated, class of complete permutation polynomials.

Before we move on to the following sections let us fix the following notations and definitions. If we view $f \in \mathbb{F}_q[x]$ as a map of $\mathbb{F}_q$ and we are given a subset $V$ of $\mathbb{F}_q$, we mean by $f|_V$ the map obtained by restricting $f$ to $V$, and $f|_V^{-1}$ denotes the inverse map of $f|_V$. When the context is clear we may however denote by $f|_V^{-1}$ a polynomial in $\mathbb{F}_q[x]$ inducing the inverse map of $f|_V$. When a polynomial $f$ is viewed as a mapping $\mathbb{F}_q \to \mathbb{F}_q$, we denote by $1/f$ the polynomial $f^{q-2}$. Similarly if $x$ is viewed as a point of $\mathbb{F}_q$, we denote $1/f(x) := f(x)^{q-2}$. In this case we call $f^{-1}(x)$ the *preimage* of $x$ under $f$.

## 2. Inverses of linearized binomials permuting kernels of traces

In this section we study the compositional inverses of binomials permuting the kernel of the trace map. More precisely, given a positive integer $r < n$, consider the binomial $L_{c,r}(x) := x^{p^r} - cx \in \mathbb{F}_{q^n}[x]$, where $c \in \mathbb{F}_q$. Note that $L_{c,r}(\ker(T_{q^n|q})) \subseteq \ker(T_{q^n|q})$, where $\ker(T_{q^n|q}) = \{\beta^q - \beta \mid \beta \in \mathbb{F}_{q^n}\}$ is the kernel of the additive map of $T_{q^n|q}$ on $\mathbb{F}_{q^n}$. We would like to discover what are the necessary and sufficient conditions for $L_{c,r}$ to be a permutation of $\ker(T_{q^n|q})$, and in such cases obtain a polynomial in $\mathbb{F}_{q^n}[x]$ inducing the inverse map of $L_{c,r}|_{\ker(T_{q^n|q})}$. We only need to consider the case when $L_{c,r}$ permutes $\mathbb{F}_{q^n}$ and the case when $L_{c,r}$ permutes $\ker(T_{q^n|q})$ but not $\mathbb{F}_{q^n}$. The former case has already been tackled in [34] (see Theorem 2.1 here) and so we focus on the latter case. We give the result in Theorem 2.6 of Section 2.1. Then in Section 2.2 we explain the method used to obtain the result. We remark that in Corollary 2.10 we show that under some restrictions of the characteristic, $p$, and the extension degree, $n$, $L_{c,r}$ permutes $\ker(T_{q^n|q})$ for each $c \in \mathbb{F}_q$. Therefore it is quite useful to use this result to construct some permutation polynomials which are also complete mappings. Indeed, we demonstrate the application of Corollary 2.10 in the proof of Theorem 3.3 in Section 3.

Please cite this article in press as: A. Tuxanidy, Q. Wang, Compositional inverses and complete mappings over finite fields, Discrete Applied Mathematics (2016), http://dx.doi.org/10.1016/j.dam.2016.09.009