Journal der mathematischen Ablehnungen

Paper No.32 (2014)

A note on interpolation of permutations of a subset of a finite field

Chris Castillo, Robert S. Coulter and Stephen Smith

Department of Mathematical Sciences, University of Delaware, Newark, DE, 19716, United States of America.

AMS Subject class: 11T06, 12E10

Keywords: interpolation, permutation polynomials

Abstract

We determine several variants of the classical interpolation formula for finite fields which produce polynomials that induce a desirable mapping on the non-specified elements, and without increasing the number of terms in the formula. As a corollary, we classify those permutation polynomials over a finite field which are their own compositional inverse, extending work of C. Wells.

§ 1. Introduction

The idea of polynomial interpolation has been known now for several centuries. The classical Lagrangian form is as follows: Given some field $\mathcal{F}$, and some partial function ϕ on $\mathcal{F}$ – i.e. a function defined on a subset $A = \{a_0, a_2, \ldots, a_n\}$ of $\mathcal{F}$ satisfying $\phi(a_i) = b_i \in \mathcal{F}$ for $0 \leq i \leq n$ – the unique polynomial $f \in \mathcal{F}[X]$ of degree at most n which satisfies $f(a_i) = b_i$ is given by

$$f(X) = \sum_{i=0}^{n} b_i \prod_{\substack{a \in A \\ a \neq a_i}} \left(\frac{X - a}{a_i - a} \right). \tag{1}$$

While the Lagrange Interpolation Formula has many practical uses, a modern instance being in secret-sharing schemes for example, when used in a discrete setting, the resulting polynomial may not necessarily be the most useful. For example, in discrete settings it is often desirable to have more control over the behaviour of the polynomial f on $\mathcal{F} \setminus A$, and the behaviour of the polynomial $f(X)$ in (1) is unpredictable on $\mathcal{F} \setminus A$.

In this note we are interested in looking at several alternative versions of polynomial interpolation in the discrete setting which produce polynomials that induce a desirable mapping on the non-specified elements, and this without increasing the number of terms in the formula. For various reasons, we restrict ourselves to the case where $\mathcal{F}$ is a finite field. Specifically, we are interested in versions of interpolation for representing

partial functions ϕ which permute a specified subset A of $\mathcal{F}$. A previous study of representing partial functions in the discrete setting and without the permutation requirement can be found in Wesselkamper [5], though Wesselkamper's results stem from a different motivation. Depending on the situation, there are a variety of ways of extending the partial function to the whole of $\mathcal{F}$. Here we consider two such circumstances, namely where the polynomial acts on the non-specified elements as either the identity map or a constant. The former situation yields another generic method for constructing permutation polynomials over finite fields using interpolation – methods for constructing permutation polynomials over finite fields via Lagrange interpolation were noted previously by Carlitz [1], Dickson [2], and Zsigmondy [6]. An immediate corollary of this permutation result is a complete description of all polynomials defined over a finite field which form their own compositional inverse. We use this corollary to identify one particularly special permutation polynomial class; those that represent a permutation of the finite field which switches some nonzero element with its additive inverse and otherwise fixes the field. Our results are given in Section 3.

§ 2. Notation and preliminaries

Throughout q is some prime power. We use $\mathbb{F}_q$ to denote a finite field with q elements, $\mathbb{F}_q^\star$ its non-zero elements, and $\mathbb{F}_q[X]$ to be the polynomial ring in indeterminate X over $\mathbb{F}_q$. It is well known that any function on $\mathbb{F}_q$ can be uniquely represented by a reduced polynomial in $\mathbb{F}_q[X]$; that is one of degree at most $q-1$ – in fact, this follows from Lagrange interpolation!

An important polynomial in what follows is the "all ones" polynomial $h_k(X) = 1 + X + X^2 + \ldots + X^k$, where k is a non-negative integer. Some results concerning $h_k(X)$ have appeared previously in the literature. Of interest is the work of Matthews [3], who classified the permutation behaviour of these polynomials over fields of odd characteristic; this problem remains open in even characteristic. We list some useful identities for $h_k(X)$.

Lemma 1. *The following statements hold.*

(i) For any k, $h_k(1) = k+1$, and

$$h_k(x) = \frac{x^{k+1}-1}{x-1}, \text{ if } x \neq 1. \tag{2}$$

(ii) For $a \in \mathbb{F}_q^\star$, $(X-a)^{q-1} = X^{q-1} + h_{q-2}(a^{-1}X)$.

(iii) For $a, x \in \mathbb{F}_q$, we have

$$h_{q-2}(a^{q-2}x) = \begin{cases} 1 & \text{if } ax = 0, \\ 0 & \text{if } ax \neq 0 \text{ and } x \neq a, \\ -1 & \text{if } x = a \neq 0. \end{cases}$$

Proof. Part (i) is immediate, while (ii) follows from the Binomial Theorem and the easily proved observation that $\binom{q-1}{i} \equiv (-1)^i \bmod p$.

For (iii), if either a or x is zero, then $h_k(0) = 1$ is clear for any non-negative k. For the remainder of the proof we assume $ax \neq 0$. If $x = a$, then $a^{q-2}x = a^{q-1} = 1$, and we can appeal to (i) to obtain $h_{q-2}(a^{q-2}x) = q-1 = -1$, as claimed. Now suppose $x \neq a$, so that $a^{q-2}x \neq 1$. Then appealing to (2) we find

$$\begin{aligned} h_{q-2}(a^{q-2}x) &= \frac{(a^{-1}x)^{q-1}-1}{a^{-1}x-1} \\ &= \frac{1-1}{a^{-1}x-1} \\ &= 0, \end{aligned}$$

completing the proof. □

Note that the last statement of the lemma shows how $h_{q-2}(X)$ can be used as a form of indicator function. It is in this capacity that we utilise $h_{q-2}(X)$ below.

§ 3. Polynomials representing partial functions

We first consider polynomial interpolation for a permutation of $\mathbb{F}_q$ (we use cycle notation to represent the permutation).

Theorem 2. *Let α be the permutation of $\mathbb{F}_q$ represented as the product of disjoint cycles as*

$$\alpha = (a_{00}, a_{01}, \ldots, a_{0n_0})(a_{10}, a_{11}, \ldots, a_{1n_1}) \ldots (a_{k0}, a_{k1}, \ldots, a_{kn_k}).$$

Then α is represented by the reduced polynomial

$$T(X) = X + \sum_{i=0}^{k} \sum_{j=0}^{n_i} a_{ij}^{q-1} h_{q-2}(a_{ij}^{q-2} X)(a_{ij} - a_{i(j+1)}),$$

where the subscript j in a_{ij} is read modulo $n_i + 1$.

Proof. We split the proof into two cases, depending on whether α fixes 0. Since the degree of T is clearly at most $q-1$, in either case, we need only prove T induces the mapping α under evaluation.
Case 1: α fixes 0.
Then $a_{ij} \neq 0$ for all i, j. Consequently, $a_{ij}^{q-1} = 1$ and the value of $h_{q-2}(a_{ij}^{q-2}x)$ is described by Lemma 1. Evaluating $T(x)$ at $x = 0$ gives

$$T(0) = 0 + \sum_{i=0}^{k} \sum_{j=0}^{n_i} h_{q-2}(0)(a_{ij} - a_{i(j+1)}).$$

By Lemma 1, $h_{q-2}(0) = 1$, so

$$\begin{aligned} T(0) &= \sum_{i=0}^{k} \sum_{j=0}^{n_i} (a_{ij} - a_{i(j+1)}) \\ &= (a_{00} - a_{01} + a_{01} - a_{02} + \cdots + a_{0(n_0-1)} - a_{0n_0} + a_{0n_0} - a_{00}) \\ &\quad + \ldots + (a_{k0} - a_{k1} + a_{k1} - a_{k2} + \cdots + a_{kn_k} - a_{k0}) \\ &= 0, \end{aligned}$$

as desired.

Now let a be any element of $\mathbb{F}_q^\star$ fixed by α. Evaluating $T(x)$ at $x = a$ gives

$$T(a) = a + \sum_{i=0}^{k} \sum_{j=0}^{n_i} h_{q-2}(a_{ij}^{q-2} a)(a_{ij} - a_{i(j+1)}).$$

Since a is fixed by α, $a \neq a_{ij}$ for all i, j. Combining this with $a \neq 0$, by Lemma 1 we have that $h_{q-2}(a_{ij}^{q-2} a) = 0$ for all i, j, so that $T(a) = a$.

Now let $a \in \alpha$. Then $a = a_{st}$ for some s, t. Evaluating $T(x)$ at $x = a$ gives

$$T(a) = a + \sum_{i=0}^{k} \sum_{j=0}^{n_i} h_{q-2}(a_{ij}^{q-2} a)(a_{ij} - a_{i(j+1)}).$$

Now $a \neq 0$ by the assumption of this case. By Lemma 1, $h_{q-2}(a_{ij}^{q-2} a) = 0$ for all $(i, j) \neq (s, t)$ and $h_{q-2}(a_{st}^{q-2} a) = -1$. Thus

$$\begin{aligned} T(a) &= a + (-1)(a_{st} - a_{s(t+1)}) \\ &= a_{st} + (-1)(a_{st} - a_{s(t+1)}) \\ &= a_{s(t+1)}, \end{aligned}$$

so the polynomial T maps every element of $\mathbb{F}_q$ as prescribed by α.
Case 2: α does not fix 0.
Without loss of generality, let $a_{00} = 0$. Then $a_{00}^{q-1} = 0^{q-1} = 0$ while $a_{ij}^{q-1} = 1$ for $a_{ij} \neq a_{00}$. We have

$$\begin{aligned} T(X) = X &+ \sum_{j=1}^{n_0} a_{0j}^{q-1} h_{q-2}(a_{0j}X)(a_{0j} - a_{0(j+1)}) \\ &+ \sum_{i=1}^{k}\sum_{j=0}^{n_i} a_{ij}^{q-1} h_{q-2}(a_{ij}^{q-2}X)(a_{ij} - a_{i(j+1)}). \end{aligned}$$

By Lemma 1, if $x = 0$, then $h_{q-2}(a_{ij}^{q-2}x) = 1$ for all i, j. Evaluating $T(x)$ at $x = 0$ gives

$$\begin{aligned} T(0) &= 0 + \sum_{j=1}^{n_0}(a_{0j} - a_{0(j+1)}) + \sum_{i=1}^{k}\sum_{j=0}^{n_i}(a_{ij} - a_{i(j+1)}) \\ &= (a_{01} - a_{02} + a_{02} - a_{03} + \cdots + a_{0(n_0-1)} - a_{0n_0} + a_{0n_0} - a_{00}) \\ &\quad + \ldots + (a_{k0} - a_{k1} + a_{k1} - a_{k2} + \cdots + a_{kn_k} - a_{k0}) \\ &= a_{01}. \end{aligned}$$

So $0 = a_{00}$ maps to a_{01}, as required.

Now let $a \in \mathbb{F}_q^\star$ be fixed by α. Evaluating $T(x)$ at $x = a$ gives

$$\begin{aligned} T(a) = a &+ \sum_{j=1}^{n_0} a_{0j}^{q-1} h_{q-2}(a_{0j}a)(a_{0j} - a_{0(j+1)}) \\ &+ \sum_{i=1}^{k}\sum_{j=0}^{n_i} a_{ij}^{q-1} h_{q-2}(a_{ij}^{q-2}a)(a_{ij} - a_{i(j+1)}). \end{aligned}$$

Since a is fixed by α, $a \neq a_{ij}$ for all i, j. Again, we combine this with $a \neq 0$ and find, by Lemma 1, that $h_{q-2}(a_{ij}^{q-2}a) = 0$ provided $(i, j) \neq (0, 0)$. Thus $T(a) = a$.

Now let $a = a_{st}$ for some $s, t, (s, t) \neq (0, 0)$. Evaluating $T(x)$ at $x = a$ gives

$$\begin{aligned} T(a) = a &+ \sum_{j=1}^{n_0} a_{0j}^{q-1} h_{q-2}(a_{0j}a)(a_{0j} - a_{i(j+1)}) \\ &+ \sum_{i=1}^{k}\sum_{j=0}^{n_i} a_{ij}^{q-1} h_{q-2}(a_{ij}^{q-2}a)(a_{ij} - a_{i(j+1)}). \end{aligned}$$

As $a \neq 0$, Lemma 1 yields $h_{q-2}(a_{ij}^{q-2}a) = 0$ for all $i, j, (i, j) \notin \{(0, 0), (s, t)\}$ and $h_{q-2}(a_{st}^{q-2}a) = -1$. Thus

$$\begin{aligned} T(a) &= a + (-1)(a_{st} - a_{s(t+1)}) \\ &= a_{st} + (-1)(a_{st} - a_{s(t+1)}) \\ &= a_{s(t+1)}, \end{aligned}$$

and we have shown the polynomial T maps every element of $\mathbb{F}_q$ as prescribed by α. □

Note that the number of terms in the double sum is equal to the number of non-fixed points of the permutation, which is the same as in (1).

As an immediate application of Theorem 2, we classify those permutation polynomials over $\mathbb{F}_q$ which are their own compositional inverse.

Corollary 3. *Let $f \in \mathbb{F}_q[X]$ satisfy $f(f(X)) \equiv X \bmod (X^q - X)$. Then*

$$f(X) = X + \sum_{i=0}^{k}(a_{i0} - a_{i1})(a_{i0}^{q-1}h_{q-2}(a_{i0}^{-1}X) - a_{i1}^{q-1}h_{q-2}(a_{i1}^{-1}X)),$$

where the a_{ij} are distinct elements of $\mathbb{F}_q$. In particular, if $f(0) = 0$ also holds, then

$$\begin{aligned} f(X) &= X + \sum_{i=0}^{k}(a_{i0} - a_{i1})(h_{q-2}(a_{i0}^{-1}X) - h_{q-2}(a_{i1}^{-1}X)) \\ &= X + \sum_{i=0}^{k}(a_{i0} - a_{i1})((X - a_{i0})^{q-1} - (X - a_{i1})^{q-1}). \end{aligned}$$

The result follows immediately from Theorem 2 and the observation that any $f \in \mathbb{F}_q[X]$ satisfying the hypothesis must induce an involution $\alpha \in S_q$ of the form

$$\alpha = (a_{00}, a_{01})(a_{10}, a_{11}) \cdots (a_{k0}, a_{k1}),$$

with $a_{ij} \in \mathbb{F}_q$ distinct. The last observation concerning polynomials with no constant term follows from Lemma 1(ii).

We note in particular the form for those reduced polynomials representing involutions which fix all but two elements; these polynomials were previously described by Wells [4], and could in turn be used to establish Corollary 3. A particularly nice form of permutation polynomial comes from the involution $\alpha = (a, -a)$.

Corollary 4. *Let $a \in \mathbb{F}_q^\star$ for q odd and let $h_k(X) = 1 + X + X^2 + \cdots + X^k$ for any natural number k. The polynomial $f_a \in \mathbb{F}_q[X]$ given by*

$$f_a(X) = X + 4Xh_{\frac{q-3}{2}}\left((a^{-1}X)^2\right)$$

is a permutation polynomial over $\mathbb{F}_q$.

Proof. Set $\alpha = (a, -a)$. Appealing to Corollary 3 we find

$$\begin{aligned} f_a(X) &= X + (a - (-a))\left(h_{q-2}(a^{-1}X) - h_{q-2}((-a)^{-1}X)\right) \\ &= X + 2a\sum_{k=0}^{q-2}\left((a^{-1})^k - (-a)^{-k}\right)X^k \\ &= X + 2a\sum_{k=0}^{q-2}\left(1 - (-1)^k\right)(a^{-1}X)^k \\ &= X + 2a\sum_{k=0}^{\frac{q-3}{2}}2(a^{-1}X)^{2k+1} \\ &= X + 4a(a^{-1}X)\sum_{k=0}^{\frac{q-3}{2}}(a^{-1}X)^{2k} \\ &= X + 4Xh_{\frac{q-3}{2}}\left((a^{-1}X)^2\right). \end{aligned}$$

□

We now move to our second natural situation, where we extend the partial permutation function so that it acts as a constant on the non-specified elements.

Theorem 5. *Let $c \in \mathbb{F}_q$ be fixed, A be some subset of $\mathbb{F}_q$, and α be a permutation on A, represented as the product of disjoint (possibly trivial) cycles as*

$$(a_{00}, a_{01}, \ldots, a_{0n_0})(a_{10}, a_{11}, \ldots, a_{1n_1}) \ldots (a_{k0}, a_{k1}, \ldots, a_{kn_k}).$$

Then the polynomial

$$T(X) = c + \sum_{i=0}^{k} \sum_{j=0}^{n_i} (a_{i(j+1)} - c)(1 - (X - a_{ij})^{q-1}),$$

with the subscript j in a_{ij} read modulo $n_i + 1$, represents the permutation α on A while mapping all $a \in \mathbb{F}_q \setminus A$ to c.

Proof. As with the proof of Theorem 3, it suffices to prove the function induced by T on $\mathbb{F}_q$ is as claimed.

Let $a \in \mathbb{F}_q \setminus A$. Then $a \neq a_{ij}$ for all i, j. Consequently,

$$\begin{aligned} T(a) &= c + \sum_{i=0}^{k} \sum_{j=0}^{n_i} (a_{i(j+1)} - c)(1 - (a - a_{ij})^{q-1}) \\ &= c + \sum_{i=0}^{k} \sum_{j=0}^{n_i} (a_{i(j+1)} - c)(1 - 1) \\ &= c, \end{aligned}$$

so every $a \in \mathbb{F}_q \setminus A$ is mapped to c.

Now let $a \in A$. Then $a = a_{st}$ for some s, t. Here we have

$$\begin{aligned} T(a) &= c + \sum_{i=0}^{k} \sum_{j=0}^{n_i} (a_{i(j+1)} - c)(1 - (a - a_{ij})^{q-1}) \\ &= c + (a_{s(t+1)} - c)(1 - 0) \\ &= a_{s(t+1)}, \end{aligned}$$

and we are done. □

Versions of the types of functions considered in Theorem 5 can be useful in cryptography when attempting to construct a meet-in-the-middle attack, where one looks to split the encryption function E into a composition of two functions on at least some subset of the message space, and then use this to restrict the search space for potential messages. Whether the associated polynomials produced here could also be useful in such an attack is unclear.

References

[1] L. Carlitz, *A note on permutation functions over a finite field*, Duke Math J. **29** (1962), 325–332.

[2] L.E. Dickson, *The analytic representation of substitutions on a power of a prime number of letters with a discussion of the linear group*, Ann. of Math. **11** (1897), 65–120, 161–183.

[3] R. Matthews, *Permutation properties of the polynomials $1 + x + \cdots + x^k$ over a finite field*, Proc. Amer. Math. Soc. **120** (1994), 47–51.

[4] C. Wells, *The degrees of permutation polynomials over finite fields*, J. Combinatorial Theory **7** (1969), 49–55.

[5] T.C. Wesselkamper, *The algebraic representation of partial functions*, Discrete Appl. Math. **1** (1979), 137–142.

[6] K. Zsigmondy, *Über wurzellose Congruenzen in Bezug auf einen Primzalmodul*, Monatsh. Math. Phys. **8** (1897), 1–42.