A P-adic Lifting Lemma and Its Application to Permutation Polynomials

Daqing Wan
Department of Mathematical Sciences
University of Nevada, Las Vegas
Las Vegas, Nevada 89154

0. Introduction

Let F_q be the finite field of q elements, where $q = p^r$. A polynomial $f(x) \in F_q[x]$ is called a permutation polynomial over F_q if $f(x)$ induces a one-one map of F_q. $f(x)$ is called exceptional over F_q if $x - y$ is the only absolutely irreducible factor of $f(x) - f(y)$ over F_q. A fundamental result in the theory of permutation polynomials is the theorem of Cohen which asserts that any exceptional polynomial over F_q is a permutation polynomial over F_q. This result was conjectured by Davenport and Lewis [2]. It was first proved by MacCluer [4] in the case that $\deg(f) < 2p$. The general case of the Davenport-Lewis conjecture was proved by Cohen [1] using the deep method of algebraic number theory. In the case that the characteristic p is large compared to the degree of $f(x)$, a very elementary and ingenius proof was found by Williams [6], see also page 363-364 in [3] for an account.

In this note, we show that Williams' simple idea can be modified to give a general proof of Cohen's theorem. The reason that Williams' proof fails for small characteristics is that he directly worked over finite fields and the small characteristic p may kill the leading coefficient in Newton's formula about symmetric polynomials, thus fails to yield enough information. To avoid the difficulty, a natural idea is to try to lift Williams' proof to p-adic number fields. Our purpose here is to carry out this plan. A new idea in our proof is to lift the orthogonal relations

$$\sum_{i=1}^{q} a_i^k = 0, \quad 1 \le k \le w \tag{0.1}$$

over F_q to a p-adic number field with restricted residue classes on some of the a_i, where w is a positive integer smaller than $q - 1$. We believe that this type of lifting is useful to many problems over finite fields. Another example can be found in [5], where the lifting modulo p^2 is used.

1. The Lifting Lemma

Let F_q be the finite field of q elements, where $q = p^r$. Let Q_p be the field of p-adic rational numbers and let K be the unique unramified extension of Q_p of degree r. We are interested in lifting an equation together with its solutions over F_q to an equation with solutions over K. The most well-known such lifting is undoubtably the Teichmüller lifting. It lifts the solutions of the equation $x^q - x$ over F_q (which are the elements of F_q) to solutions of the equation $x^q - x$ over K. Let t_i $(1 \le i \le q)$ be the Teichmüller liftings of the elements of F_q. A fundamental property is that they satisfy the following orthogonal equations

$$\sum_{i=1}^{q} t_i^k = 0, \quad 1 \le k < q-1. \tag{1.1}$$

For applications to certain problems over finite fields, we need to consider a more general lifting with some of the variables restricted to certain residue classes. For convenience, we order the Teichmüller liftings t_i such that $t_q = 0$.

Lemma 1.1. Given an integer $1 \le w \le q-1$. There are uniquely determined convergent power series $x_1, \cdots, x_w$ in $K[[x_{w+1}, \cdots, x_q]]$ with p-adic integral coefficients such that

$$\sum_{i=1}^{q} (t_i + px_i)^k = 0, \quad 1 \le k \le w. \tag{1.2}$$

Recall that a p-adic power series is called convergent if its coefficients approach zero, equivalently, the power series is analytic on the closed unit disk. This lemma can be viewed as a special refined implicit function theorem. It can be proved using Hensel's lemma or the fixed point theorem in a p-adic Banach space.

Proof. Expanding (1.2), we get the system of equations

$$\sum_{i=1}^{q} (p\binom{k}{1} t_i^{k-1} x_i + p^2 \binom{k}{2} t_i^{k-2} x_i^2 + \cdots) = 0, \quad k = 1, \cdots, w. \tag{1.3}$$

This system can be rewritten as

$$\sum_{i=1}^{w} t_i^{k-1} x_i = -\sum_{i=w+1}^{q} t_i^{k-1} x_i - \frac{1}{pk} \sum_{i=1}^{q} (p^2 \binom{k}{2} t_i^{k-2} x_i^2 + p^3 \binom{k}{3} t_i^{k-3} x_i^3 + \cdots), \quad k = 1, \cdots, w. \tag{1.4}$$

Assume first that $p > 2$. Then one checks that the second term on the right side has p-adic integral coefficients which are divisible by p. Since $t_i \neq 0$ for $i < q$, we have $t_i^0 = 1$. Thus, the coefficient matrix on the left side is the $w \times w$ Vandermonde matrix formed from $t_1, \cdots, t_w$. The determinant is a p-adic unit since $t_1, \cdots, t_w$ are not congruent to each other modulo p. Solving the "linear system" (1.4), we conclude that (1.4) is equivalent to a system of the form

$$x_k = f_k(x_{w+1}, \cdots, x_q) + pg_k(x_1, \cdots, x_q), \quad 1 \leq k \leq w, \tag{1.5}$$

where the f_k and g_k are polynomials with p-adic integral coefficients. Thus, (1.5) defines a contraction map. By successive iterations or the fixed point theorem in a p-adic Banach space, there are uniquely determined power series $x_1, \cdots, x_w$ in $K[[x_{w+1}, \cdots, x_q]]$ with p-adic integral coefficients satisfying (1.2).

We now treat the case when $p = 2$. The proof is a little more subtle. We claim that the system (1.4) is equivalent to a system of the following form

$$\sum_{i=1}^{w} t_i^{k-1} x_i = f_k(x_{w+1}, \cdots, x_q) + 2g_k(x_1, \cdots, x_q), \tag{1.6}$$

where the f_k and g_k are polynomials with p-adic integral coefficients. If k is odd, then the second term on the right side of (1.4) has p-adic integral coefficints which are divisible by $p = 2$. Thus, the kth equation in (1.4) has the form of the kth equation in (1.6). If k is even, write $k = 2k_1$. The kth equation in (1.4) can be written as

$$\begin{aligned} \sum_{i=1}^{w} t_i^{k-1} x_i = &- \sum_{i=w+1}^{q} t_i^{k-1} x_i - (k-1) \sum_{i=1}^{q} t_i^{k-2} x_i^2 \\ &- \frac{1}{pk} \sum_{i=1}^{q} (p^3 \binom{k}{3} t_i^{k-3} x_i^3 + \cdots), \quad k = 1, \cdots, w. \end{aligned} \tag{1.7}$$

One checks that the third term on the right side of (1.7) has p-adic integral coefficints which are divisible by $p = 2$. To prove the claim, we need to prove that $\sum_{i=1}^{w} t_i^{k-2} x_i^2$ can be written as an expresssion similar to the right side of (1.6). Now, $k = 2k_1$. We have

$$\begin{aligned} \sum_{i=1}^{w} t_i^{k-2} x_i^2 &= (\sum_{i=1}^{w} t_i^{k_1-1} x_i)^2 + \sum_{i=1}^{w} t_i^{k-2} x_i^2 - (\sum_{i=1}^{w} t_i^{k_1-1} x_i)^2 \\ &= (\sum_{i=1}^{w} t_i^{k_1-1} x_i)^2 + 2f(x_1, \cdots, x_w), \end{aligned} \tag{1.8}$$

where f is polynomial with p-adic integral coefficients. Using equation (1.8) and induction on k, we conclude that the claim is true. As the case for $p > 2$, (1.6) defines a contraction map. The lemma then follows from the fixed point theorem. The proof is complete.

Corollary 1.2. Given an integer $1 \leq w \leq q-1$ and p-adic integers $a_{w+1}, \cdots, a_q$ in K. There are uniquely determined p-adic integers $a_1. \cdots, a_w$ in K such that

$$\sum_{i=1}^{q} (t_i + pa_i)^k = 0, \quad 1 \leq k \leq w. \tag{8}$$

The existence of the a_i $(1 \leq i \leq w)$ follows directly from the lemma. The uniqueness follows from the proof of the lemma. If we choose $w = q-1$ and $a_q = 0$, then Corollary 1.2 is reduced to the Teichmüller liftings.

2. Permutation Polynomials

In this section, we lift Williams' proof to characteristic zero and thus give a simple proof of Cohen's theorem.

Theorem 2.1. If $f(x)$ is exceptional over F_q, then $f(x)$ is a permutation polynomial over F_q.

Proof. Let $f(x)$ be an exceptional polynomial of degree n over F_q. Then, $x - y$ is the only absolutely irreducible factor of $f(x) - f(y)$. Let N_f be the number of solutions of $f(x) - f(y) = 0$ over F_q. Then, $N_f = q + O_n(1)$. Let the value set $\{f(c) : c \in F_q\}$ have V_f elements with multiplicities m_i $(1 \leq i \leq V_f)$. Then,

$$\sum_{i=1}^{V_f} m_i = q, \ \ \sum_{i=1}^{V_f} m_i^2 = N_f = q + O_n(1). \tag{2.1}$$

From this equation and the Cauchy-Schwarz inequality

$$(\sum_{i=1}^{V_f} 1)(\sum_{i=1}^{V_f} m_i^2) \geq (\sum_{i=1}^{V_f} m_i)^2 = q^2, \tag{2.2}$$

we deduce that $V_f = q - O_n(1)$.

To prove Theorem 2.1, we may assume that q is large. If q is small, then $f(x)$ is also exceptional over some large finite extension F_{q^s}. Applying Theorem 2.1 to the large field F_{q^s}, we conclude $f(x)$ is a permutation polynomial over F_{q^s}, hence a permutation polynomial over F_q.

Write $V_f = q - w$, where w is a non-negative integer. We need to prove that $w = 0$. Assume that $w \geq 1$. We want to derive a contradiction. Let $F(x)$ be a fixed lifting of $f(x)$ to $K[x]$. Write

$$F(x) = c_0 + c_1 x + \cdots + c_n x^n, \quad c_i \in K. \tag{2.3}$$

Let the t_i be the Teichmüller liftings of the elements in F_q. By the definition of w, we can reorder the sequence $\{F(t_i)\}$ as $\{b_i\}$ such that $b_{w+1}, \cdots, b_q$ are the representatives of the residue classes modulo p of the sequence $\{F(t_i)\}$. By assuming $f(x) = 0$, we may assume that b_q is divisible by p. Now, applying Corollary 1.2 we find that there are p-adic integers $a_1, \cdots, a_w$ in K such that

$$\sum_{i=1}^{w} a_i^k + \sum_{i=w+1}^{q} b_i^k = 0, \quad 1 \leq k \leq w. \tag{2.4}$$

Furthermore, none of the a_i is congruent to any b_j.

Since q is large, we may assume that $wn < q - 1$. Then, for all $1 \leq k \leq w$,

$$F^k(x) = c_0(k) + c_1(k)x + \cdots + c_{wn}(k)x^{wn}. \tag{2.5}$$

This equation and the orthogonal relations for the Teichmüller liftings imply that

$$\sum_{i=1}^{q} b_i^k = \sum_{i=1}^{q} F^k(t_i) = 0, \quad ,1 \leq k \leq w.$$

Thus, we have

$$\begin{aligned} \sum_{i=1}^{w} a_i^k &= \sum_{i=1}^{w} a_i^k + \sum_{i=1}^{q} b_i^k \\ &= (\sum_{i=1}^{w} a_i^k + \sum_{i=w+1}^{q} b_i^k) + \sum_{i=1}^{w} b_i^k \\ &= \sum_{i=1}^{w} b_i^k, \quad 1 \leq k \leq w. \end{aligned} \tag{2.6}$$

From this equation and Newton's formula about symmetric polynomials, we deduce that the two polynomials $\prod_{i=1}^{w}(x-a_i)$ and $\prod_{i=1}^{w}(x-b_i)$ have the same coefficients (note that we are in characteristic zero). Thus, their roots $\{a_i\}$ and $\{b_i\}$ are the same. This contradicts with the fact that none of the a_i is congruent to any b_j. The theorem is proved.

References

[1]. S.D. Cohen, The distribution of polynomials over finite fields, Acta Arith, 17(1970), 255-271.

[2]. H. Davenport and D.J. Lewis, Notes on congruences (I), Quart. J. Math, 14(1963), 51-60.

[3]. R. Lidl and H. Niederreiter, Finite Fields, Addison-Wesley Publishing Company, 1983.

[4]. C.R. MacCluer, On a conjecture of Davenport and Lewis concerning exceptional polynomials, Acta Arith., 12(1967), 289-299.

[5]. D. Wan, On a problem of Niederreiter and Robinson about finite fields, J. Austral. Math. Soc. Ser A, 41(1986), 336-338.

[6]. K.S. Williams, On exceptional polynomials, Canad. Math. Bull., 11(1968), 279-282.