<table>
<thead>
<tr>
<th>著者</th>
<th>Atsumi Tsuyoshi</th>
</tr>
</thead>
<tbody>
<tr>
<td>期刊名</td>
<td>Reports of the Faculty of Science, Kagoshima University</td>
</tr>
<tr>
<td>巻</td>
<td>38</td>
</tr>
<tr>
<td>頁</td>
<td>83-88</td>
</tr>
<tr>
<td>URL</td>
<td><a href="http://hdl.handle.net/10232/815">http://hdl.handle.net/10232/815</a></td>
</tr>
</tbody>
</table>
A note on planar polynomials

<table>
<thead>
<tr>
<th>著者</th>
<th>Atsumi Tsuyoshi</th>
</tr>
</thead>
<tbody>
<tr>
<td>雑誌名</td>
<td>城崎大学理学部紀要</td>
</tr>
<tr>
<td>卷</td>
<td>38</td>
</tr>
<tr>
<td>頁</td>
<td>83-88</td>
</tr>
<tr>
<td>URL</td>
<td><a href="http://hdl.handle.net/10232/00006299">http://hdl.handle.net/10232/00006299</a></td>
</tr>
</tbody>
</table>
A note on planar polynomials

Tsuyoshi Atsumi
Department of Mathematics and Computer Science
Faculty of Science, Kagoshima University
Kagoshima 890-0065, Japan

September 29, 2005

Abstract

The following conjecture is well-known.

Conjecture. Let $p$ be an odd prime ($p \geq 5$). Let $f(x)$ be a polynomial over $F_{p^2}$ of degree at most $p^2 - 1$. Assume that $f(x)$ is a planar polynomial over $F_{p^2}$. Then $f(x)$ is a quadratic polynomial.

In this short note we shall prove that in a special case the conjecture is true.

Keywords. finite field, planar polynomial, permutation polynomial

1 Introduction and Summary

In order to prove the conjecture for a special case we shall establish the following main theorem, which is an extension of the proof in Lemma 6 in [4].

Theorem 1. Let $F_q$ be the finite field with $q = p^k$ elements where $p$ is a prime, and let $f(x)$ be a planar polynomial over $F_{p^s}$ of degree $s \geq 3$. Let $u$ be a positive integer such that

$$u \leq \frac{q-1}{s} < u + 1. \quad (1)$$

Set $n = 2u$. Then

$$\binom{n}{u} (-1)^{n-u} \binom{us}{ns - (q-1)} = 0$$

in $F_q$. 
By using the above theorem and its proof we shall also prove the following two propositions.

**Proposition 1.** Let \( p \equiv 1 \pmod{4} \) be a prime. Then there are no planar polynomials over \( F_{p^2} \) of degree \( 4p + 3 \).

Proposition 1 is a special case of our conjecture.

**Proposition 2.** Let \( p \) be an odd prime (\( p \geq 5 \)). Let \( f(x) \) be a polynomial over \( F_p \) of degree at most \( p - 1 \). Assume that \( f(x) \) is a planar polynomial over \( F_p \). Then \( f(x) \) is a quadratic polynomial.


Here we shall give several definitions. A polynomial \( g \in F_q[x] \) is called a permutation polynomial of \( F_q \) (see [5]) if the associated polynomial function \( g : c \mapsto f(c) \) from \( F_q \) into \( F_q \) is a permutation of \( F_q \). A polynomial \( f \in F_q[x] \) is called a planar polynomial over \( F_q \) (see [2]) if \( f(x + d) - f(x) \) is a permutation polynomial of \( F_q \) for each \( d \in F_q^* (= F_q - \{0\}) \).

For \( g, h(\neq 0) \in F_q[x] \), there exist \( q, r \in F_q[x] \) with \( g = qh + r \) and either \( r = 0 \) or \( \deg r < \deg h \). Then \( r \) is called the reduction of \( g \) (mod \( h \)).

### 2 Preliminaries

**Theorem 2.** Let \( F_q \) be a finite field of order \( q = p^k \). If \( g \in F_q[x] \) is a permutation polynomial of \( F_q \), then the following two conditions holds:

(i) \( g \) has exactly one root in \( F_q \)

(ii) for each integer \( t \) with \( 1 \leq t \leq q - 2 \), the reduction of \( g(x)^t \pmod{x^q-x} \) has degree \( \leq q - 2 \).

**Remark.** The above theorem is part of Hermite’s Criterion [5, p. 349].

Let \( f(x) \) be a planar polynomial over \( F_q \) of degree at most \( q - 1 \), where \( q = p^k (p \geq 5, k \geq 1) \). Let \( h(x) = f(x) - f(0) \). Then this \( h(x) \) is also a planar polynomial. So we may assume that

\[
f(x) = \sum_{m=1}^{s} c_m x^m, c_s \neq 0, \deg(f(x)) = s < q. \tag{2}
\]

For integer \( n(0 < n < q - 1) \), we have

\[
(f(x + d) - f(x))^n = g_{q-1}(d)x^{q-1} + g_{q-2}(d)x^{q-2} + \cdots \pmod{x^q - x}, \tag{3}
\]
where \( g_{q-1}(d), g_{q-2}(d), \ldots \) are polynomials in \( d \) and their degree are at most \( q - 1 \) because \( d^q = d \) for all \( d \in F_q \).

Then,

**Lemma 1.** \( g_{q-1}(d) = 0. \) That is, the coefficient of \( d^i x^{q-1} \) \((0 \leq i \leq q - 1)\) in (3) is 0.

**Proof.** By Theorem 2 the coefficient of \( x^{q-1} \) of the reduction of \((f(x + d) - f(x))^n \mod x^q \) is 0. So for all \( d \in F_q^* \), \( g_{q-1}(d) = 0. \) Clearly \( g_{q-1}(0) = 0. \) Thus \( g_{q-1}(d) = 0 \) because the degree of \( g_{q-1}(d) \) is at most \( q - 1. \)

\( \square \)

**Lemma 2.** Suppose \( q - 1 < ns \leq 2(q - 1). \) The coefficient of \( d^{ns-(q-1)} x^{q-1} \) in \((f(x + d) - f(x))^n \) is \( c^n_0 \sum_{k=0}^{n} \binom{n}{k} (-1)^{n-k} \binom{\frac{ns}{q} - 1}{k} \).

**Proof.**

\[
(f(x + d) - f(x))^n = (c_0(x + d)^s + \cdots + c_1(x + d) - c_2 x^s - \cdots c_1 x)^n
\]

\[
= \sum_{p_1 + \cdots + q_s = n, 0 \leq p_1, \ldots, q_s \leq n} \frac{n!}{p_1! \cdots p_s! q_1! \cdots q_s!} (c_1(x + d)^{p_1} \cdots (c_2(x + d)^{q_s}(-c_1 x^{p_1 - 1})^q \cdots (-c_2 x)^{q_s})^{q_s}
\]

Here we shall find the terms involving \( d^{ns-(q-1)} x^{q-1} \) in the above polynomial. For this purpose we consider the term

\[
\binom{1}{i_1} x^{p_1-i_1} d^{i_1} \cdots \binom{sp_s}{i_s} x^{p_s-i_s} d^{i_s} x^{q_1} \cdots x^{q_s}
\]

in \((x + d)^{p_1} \cdots (x + d)^{sp_s} x^{q_1} \cdots x^{q_s}. \)

Since

\[
\binom{1}{i_1} \binom{sp_s}{i_s} = \binom{1}{i_1} \cdots \binom{sp_s}{i_s} x^{p_1+i+s_1+\cdots+i_s} x^{q_1} \cdots x^{q_s}
\]

\((p_1 \geq i_1 \geq 0, \cdots, sp_s \geq i_s \geq 0), \) so if we find \( p_1, \cdots, p_s, q_1, \cdots, q_s \) satisfying \( i_1 + \cdots + i_s = ns -(q-1) \) and \( p_1 + \cdots + sp_s + q_1 + \cdots + q_s = (ns -(q-1)) = q-1, \) then we know the terms involving \( d^{ns-(q-1)} x^{q-1} \) in the above polynomial.

Clearly we have \( p_1 + \cdots + q_s = n, \) \( p_1 + \cdots + sp_s + q_1 + \cdots + q_s \leq ns. \)

These imply that

\[
p_1 + \cdots + sp_s + q_1 + \cdots + q_s = (ns -(q-1)) = q-1
\]

holds if and only if

\[
p_s + q_s = n, p_{s-1} = 0, p_{s-2} = 0, \cdots, q_1 = 0
\]

(4)
hold.

By (4) we proved that when we write

\[
(f(x + d) - f(x))^n = \sum_{p_s + q_s = n} \frac{n!}{p_s^s q_s^s} (c_s(x + d)^s)^{p_s} (-c_s x^s)^{q_s}
\]

\[
+ \sum_{p_1 + \cdots + p_q = n, 0 \leq p_1, \ldots, q_s \leq n, p_s + q_s \neq n} \frac{n!}{p_1! \cdots p_q! q_1! \cdots q_q!} (c_1(x + d)^1)^{p_1} \cdots (c_s(x + d)^s)^{p_s} (-c_s x^s)^{q_s}
\]

, then the terms involving \(d^{ns-(q-1)x^{q-1}}\) appear in the first part of the RHS of the above equation.

Here we note

\[
\sum_{p_s + q_s = n} \frac{n!}{p_s^s q_s^s} (c_s(x + d)^s)^{p_s} (-c_s x^s)^{q_s} = (c_s(x + d)^s - c_s x^s)^n.
\]

Thus the coefficient of \(d^{ns-(q-1)x^{q-1}}\) in \((f(x + d) - f(x))^n\) is \(c_s^n \sum_{i=0}^{n} \binom{n}{i} (-1)^{n-i} \binom{n}{i}(\frac{d}{n})^{i}(q-1)^{n-i}(\frac{d}{n^{q-1}})\).

\[\square\]

**Lemma 3 (Lucas' Theorem).** Let \(p\) be a prime number, and let \(m = a_0 + a_1p + \cdots + a_v p^v\), \(n = b_0 + b_1p + \cdots + b_v p^v\), where \(0 \leq a_i, b_i < p\) for \(i = 0, \ldots, v\). Then

\[
\binom{m}{n} \equiv \prod_{i=0}^{v} \binom{a_i}{b_i} \pmod{p}.
\]

A proof of Lucas' Theorem can be found in [1, pp. 28].

### 3 Proofs of Theorem 1 and Propositions 1, 2

We start to prove Theorem 1.

From assumption \(s \geq 3\). Then

\[
2 \leq n \leq \frac{2(q-1)}{s} < q - 1.
\] (5)

From (1) and (5) we see that

\[
q - 1 < ns \leq 2(q-1).
\] (6)

So by Lemma 2, the coefficient of \(d^{ns-(q-1)x^{q-1}}\) is \(c_s^n \sum_{i=0}^{n} \binom{n}{i} (-1)^{n-i} \binom{n}{i}(\frac{d}{n^{q-1}})\).
Lemma 4.

\[ c_s^n \sum_{i=0}^{n} \binom{n}{l} (-1)^{n-i} \binom{ls}{ns - (q-1)} = c_s^n \binom{n}{u} (-1)^{n-u} \binom{su}{ns - (q-1)}. \]

Proof. (i) The case \( l < u \). That is, \( l + 1 \leq u \). This and (1) show that

\[ ns - (q-1) - sl = 2us - (q-1) - ls \geq us + s - (q-1) = (u+1)s - (q-1) > 0. \]

Thus

\[ \binom{ls}{ns - (q-1)} = 0. \tag{7} \]

(ii) The case \( l > u \). That is, \( l \geq u + 1 \). This and (1) show that \( q - 1 \geq ls - (ns - (q-1)) = (q-1) - (2us - ls) \geq (q-1) - us > 0 \). So \( \binom{ls}{ns - (q-1)} \) exists. Since \( ns \leq 2(q-1) \) we see

\[ ns - (q-1) \leq q - 1. \tag{8} \]

By (1) \( q - 1 < (u+1)s \leq ls \). This and (8) show that

\[ q \leq ls \leq ns \leq 2(q-1). \tag{9} \]

Let \( ls = a_0 + a_1p + \cdots + a_kp^k \) and \( ns - (q-1) = b_0 + b_1p + \cdots + b_kp^k \) be the base-\( p \) expansions of \( ls \) and \( ns - (q-1) \), where \( p^k = q \). Then (8) and (9) show that \( a_k = 1 \) and \( b_k = 0 \). Since \( ls - q < ns - (q-1) \), we have \( a_j < b_j \) for some \( j \) (\( 0 \leq j \leq k - 1 \)). By Lucas' Theorem this shows that

\[ \binom{ls}{ns - (q-1)} \equiv 0 \pmod{p} \tag{10} \]

(iii) The case \( l = u \). By (1) \( us - (ns - (q-1)) = us - 2us + (q - 1) = (q - 1) - us > 0 \). So

\[ \binom{us}{ns - (q-1)} \tag{11} \]

does not vanish.

From (7) and (10) the lemma follows. \( \square \)

By Lemmas 1, 2 and 8 \( c_s^n \binom{n}{u} (-1)^{n-u} \binom{us}{ns - (q-1)} = 0 \). Since \( \binom{n}{u} (-1)^{n-u} \binom{us}{ns - (q-1)} \neq 0 \). Thus \( c_s = 0 \), contrary to (2) We complete the proof of Theorem 1. \( \square \)

Proof of Proposition 3

Proof. Assume \( s \geq 3 \). Put \( q = p \) in Theorem 1. Here we note \( n \not\equiv 0 \pmod{p} \) because \( n < p - 1 \). So we see that

\[ \binom{n}{u} (-1)^{n-u} \binom{su}{ns - (p-1)} \not\equiv 0 \pmod{p}. \tag{12} \]

This forces \( s = 2 \) by using Theorem 1. we are done. \( \square \)
Proof of Proposition 2

Proof. Let \( f(x) \) be a planar polynomial over \( F_{p^2} \) of degree \( 4p + 3 \). Put \( q = p^2 \)
in Theorem 1. As \( p^3 - 1 = (p-1)/4(4p+3) + (p-1)/4 \), \( us = \{(p-1)/4\}(4p+3) = (p-1)p + (3/4)(p-1) \), and \( ns - (p^2 - 1) = (p-1)p + (p-1)/2 \). So by
Lucas' Theorem \( (n)_u^{us \over (n_s - (p^2 - 1))} \neq 0 \). \( {n \choose u} \neq 0 \) because \( n = (p - 1)/2 \). So

\[
{n \choose u}(-1)^{n-u} {su \over n_s - (p^2 - 1)} \neq 0 \pmod{p}. \tag{13}
\]

This contradicts Theorem 1.

\[
\square
\]

References


