A note on planar polynomials

著者	Atsumi Tsuyoshi
journal or publication title	鹿児島大学理学部紀要=Reports of the Faculty of Science, Kagoshima University
volume	38
page range	83-88
URL	http://hdl.handle.net/10232/815

A note on planar polynomials

Rep. Fac. Sci., Kagoshima Univ.,
No. 38, pp. 83~88 (2005)

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^k} of degree $s \geq 3$. Let u be a positive integer such that*

$$u \leq \frac{q-1}{s} < u + 1. \tag{1}$$

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.*

Remark. Proposition 2 is proved by Hiramine [4], Gluck[3] and Rónyai and Szönyi[7] independently

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 $g \pmod h$.

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* $d^i x^{q-1}$ $(0 \le i \le q-1)$ *in (3) is* 0.

Proof. By Theorem 2 the coefficient of x^{q-1} of the reduction of $(f(x+d) - f(x))^n \pmod{x^q - x}$ 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 $q-1$.

□

Lemma 2. *Suppose* $q - 1 < ns \le 2(q-1)$. *The coefficient of* $d^{ns-(q-1)}x^{q-1}$ *in* $(f(x+d) - f(x))^n$ *is* $c_s^n \sum_{l=0}^{n} \binom{n}{l}(-1)^{n-l}\binom{ls}{ns-(q-1)}$.

Proof.

$$\begin{aligned}(f(x+d)-f(x))^n &= (c_s(x+d)^s + \cdots + c_1(x+d) - c_s x^s - \cdots c_1 x)^n \\ &= \sum_{p_1+\cdots+q_s=n, 0\le p_1,\ldots,q_s\le n} \frac{n!}{p_1!\cdots p_s! q_1!\cdots q_s!}(c_1(x+d)^1)^{p_1}\cdots \\ &\quad (c_s(x+d)^s)^{p_s}(-c_1x^1)^{q_1}\cdots(-c_s x^s)^{q_s}\end{aligned}$$

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
$\binom{1p_1}{i_1}x^{p_1-i_1}d^{i_1}\cdots\binom{sp_s}{i_s}x^{sp_s-i_s}d^{i_s}x^{q_1}\cdots x^{q_s}$ in $(x+d)^{1p_1}\cdots(x+d)^{sp_s}x^{1q_1}\cdots x^{sq_s}$.
Since

$$\begin{aligned}&\binom{1p_1}{i_1}x^{p_1-i_1}d^{i_1}\cdots\binom{sp_s}{i_s}x^{sp_s-i_s}d^{i_s}x^{q_1}\cdots x^{q^s} \\ &= \binom{1p_1}{i_1}\cdots\binom{sp_s}{i_s}x^{p_1+\cdots+sp_s+q_1+\cdots+sq_s-(i_1+\cdots+i_s)}d^{i_1+\cdots+i_s}\end{aligned}$$

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

Clearly we have $p_1 + \cdots + q_s = n, \quad p_1 + \cdots + sp_s + q_1 + \cdots + sq_s \le ns$. These imply that

$$p_1 + \cdots + sp_s + q_1 + \cdots + sq_s - (ns - (q-1)) = q - 1$$

holds if and only if

$$p_s + q_s = n, p_{s-1} = 0, p_{s-2} = 0, \cdots, q_1 = 0 \tag{4}$$

hold.

By (4) we proved that when we write

$$\begin{aligned}(f(x+d)-f(x))^n &= \sum_{p_s+q_s=n} \frac{n!}{p_s!q_s!}(c_s(x+d)^s)^{p_s}(-c_sx^s)^{q_s} \\ &+ \sum_{p_1+\cdots+q_s=n, 0\le p_1,\ldots,q_s\le n, p_s+q_s\neq n} \frac{n!}{p_1!\cdots p_s!q_1!\cdots q_s!}(c_1(x+d)^1)^{p_1}\cdots \\ &\quad (c_s(x+d)^s)^{p_s}(-c_1x^1)^{q_1}\cdots(-c_sx^s)^{q_s}\end{aligned}$$

, 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

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

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

Lemma 3 (Lucas' Theorem). *Let p be a prime number, and let $m = a_0 + a_1p + \cdots + a_vp^v$, $n = b_0 + b_1p + \cdots + b_vp^v$, where $0 \le a_i$, $b_i < p$ for $i = o, \ldots, v$. 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 $s \ge 3$. Then

$$2 \le n \le \frac{2(q-1)}{s} < q-1. \tag{5}$$

From (1) and (5) we see that

$$q-1 < ns \le 2(q-1). \tag{6}$$

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

Lemma 4.

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

Proof. (i) The case $l < u$. That is, $l+1 \le u$. This and (1) show that $ns-(q-1)-sl = 2us-(q-1)-ls \ge us+s-(q-1) = (u+1)s-(q-1) > 0$. Thus

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

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

$$ns-(q-1) \le q-1. \tag{8}$$

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

$$q \le ls \le ns \le 2(q-1). \tag{9}$$

Let $ls = a_0 + a_1 p + \cdots + a_k p^k$ and $ns-(q-1) = b_0 + b_1 p + \cdots + b_k p^k$ 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 $(0 \le j \le k-1)$. 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. □

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. □

Proof of Proposition 3

Proof. Assume $s \ge 3$. 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. □

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 $p^2-1 = (p-1)/4(4p+3)+(p-1)/4$, $us = \{(p-1)/4\}(4p+3) = (p-1)p+(3/4)(p-1)$,and $ns-(p^2-1) = (p-1)p+(p-1)/2$. So by Lucas' Theorem $\binom{us}{ns-(p^2-1)} \neq 0$. $\binom{n}{u} \neq 0$ because $n = (p-1)/2$. So

$$\binom{n}{u}(-1)^{n-u}\binom{su}{ns-(p^2-1)} \not\equiv 0 \pmod{p}. \tag{13}$$

This contradicts Theorem 1.

□

References

[1] P. J. Cameron, *Combinatorics: Topics Techniques Algorithms* (Cambridge University Press, 1994).

[2] R. Coulter and R. Matthews, Planar functions and planes of Lenz-Barlotti class II, *Des. Codes Cryptogr.*, **10** (1997) 167–184.

[3] D. Gluck, A note on permutation polynomials and finite geometries, *Discrete Math.*, **80**(1990) 97–100.

[4] Y. Hiramine, A conjecture on affine planes of prime order, *J. of Combin. Theory Ser. A* **52**(1989), 44–50.

[5] R. Lidl and H. Niederreiter, *Finite Fields* Encyclopedia Math. Appl., Addison-Wesley, Reading, **20**(1983)(now distributed by Cambridge University Press).

[6] M. J. Kallaher, *Affine Planes with Transitive Collineation Groups* (North-Holland, New york/Amsterdam/Oxford, 1982).

[7] L. Rónyai and T. Szönyi, Planar functions over finite fields, *Combinatorica*, **9** (3) (1989), 315–320.

[8] S. Wolfram, *Mathematica : A System for Doing Mathematics by Computer* (Addison -Wesley, 1988).