Finite Fields and Their Applications 41 (2016) 64–71

Contents lists available at ScienceDirect

Finite Fields and Their Applications

www.elsevier.com/locate/ffa

On a conjecture of Wan about limiting Newton polygons

Yi Ouyang, Jinbang Yang *

Wu Wen-Tsun Key Laboratory of Mathematics, School of Mathematical Sciences, University of Science and Technology of China, Hefei, Anhui 230026, PR China

ARTICLE INFO

Article history:
Received 24 October 2015
Received in revised form 25 February 2016
Accepted 12 May 2016
Available online 26 May 2016
Communicated by Daqing Wan

MSC:
primary 11T23
secondary 11L07, 11M38

Keywords:
Newton polygon
Hodge polygon
L-function
Zeta function

ABSTRACT

We show that for a monic polynomial $f(x)$ over a number field K containing a global permutation polynomial of degree > 1 as its composition factor, the Newton Polygon of $f \mod \mathfrak{p}$ does not converge for $\mathfrak{p}$ passing through all finite places of K. In the rational number field case, our result is the "only if" part of a conjecture of Wan about limiting Newton polygons.

1. Introduction and main results

Let K be a number field and $f(x)$ be a monic polynomial in $K[x]$ of degree $d \geq 1$. For a finite place $\mathfrak{p}$ of K, denote the completion of K at $\mathfrak{p}$ by $K_\mathfrak{p}$. Let $\mathcal{O}_\mathfrak{p}$ be the ring of $\mathfrak{p}$-adic integers and $k_\mathfrak{p}$ be the residue field. Then $k_\mathfrak{p}$ is a finite field of $q = q_\mathfrak{p} = p^h$

* Corresponding author.
E-mail addresses: yiouyang@ustc.edu.cn (Y. Ouyang), yjb@mail.ustc.edu.cn (J. Yang).

http://dx.doi.org/10.1016/j.ffa.2016.05.003
1071-5797/

elements for some rational prime $p = p_\mathfrak{p}$ and some positive integer $h = h_\mathfrak{p}$. Denote by $k_\mathfrak{p}^m$ the unique field extension of $k_\mathfrak{p}$ of degree m. Denote by $\Sigma_K := \Sigma_K(f)$ the set of finite places $\mathfrak{p}$ of K such that $f(x) \in \mathcal{O}_\mathfrak{p}[x]$ and $(d, p) = 1$. Note that almost all finite places of K are contained in Σ_K.

Let $\mathfrak{p}$ be a place in Σ_K. By modulo $\mathfrak{p}$, we get the reduction $\overline{f}$ of f, a polynomial over $k_\mathfrak{p}$. For a nontrivial character $\chi : \mathbb{F}_p \to \mu_p$, the L-function

$$L(\overline{f}, \chi, t) = L(\overline{f}/k_\mathfrak{p}, \chi, t) = \exp\left(\sum_{m=1}^{\infty} S_m(\overline{f}, \chi)\frac{t^m}{m}\right), \tag{1.1}$$

where $S_m(\overline{f}, \chi)$ is the exponential sum

$$S_m(\overline{f}, \chi) = S_m(\overline{f}/k_\mathfrak{p}, \chi) = \sum_{x \in k_\mathfrak{p}^m} \chi(\mathrm{Tr}_{k_\mathfrak{p}^m/\mathbb{F}_p}(\overline{f}(x))), \tag{1.2}$$

is a polynomial of t of degree $d-1$ over $\mathbb{Q}_p(\zeta_p)$ by well-known theorems of Dwork–Bombieri–Grothendieck and Adolphson–Sperber [1]. The q-adic Newton polygon $\mathrm{NP}_\mathfrak{p}(f)$ of this L-function does not depend on the choice of the nontrivial character χ.

Let $\mathrm{HP}(f)$ be a convex polygon with break points

$$\left\{\left(i, \frac{i(i+1)}{2d}\right) \middle| \, 0 \le i \le d.\right\},$$

which only depends on the degree of f. Adolphson and Sperber [2] proved that $\mathrm{NP}_\mathfrak{p}(f)$ lies above $\mathrm{HP}(f)$ and that $\mathrm{NP}_\mathfrak{p}(f) = \mathrm{HP}(f)$ if $p \equiv 1 \mod d$. Obviously, there are infinitely many $\mathfrak{p} \in \Sigma_K$ such that $p \equiv 1 \mod d$, thus if $\lim_{\mathfrak{p}\in\Sigma_K} \mathrm{NP}_\mathfrak{p}(f)$ exists, then $\lim_{\mathfrak{p}\in\Sigma_K} \mathrm{NP}_\mathfrak{p}(f) = \mathrm{HP}(f)$.

Recall that a global permutation polynomial (GPP) over K is a polynomial $P(x) \in K[x]$ such that $x \mapsto \overline{P}(x)$, where $\overline{P}$ is the reduction of P modulo $\mathfrak{p}$, is a permutation on $k_\mathfrak{p}$ for infinitely many places $\mathfrak{p} \in \Sigma_K$.

In 1999, D. Wan proposed a conjecture, whose complete version in [16, Chapter 5] and [4, Conjecture 6.1] is as follows:

Conjecture 1.1 *(Wan). Let f be a non-constant monic polynomial in $\mathbb{Q}[x]$. Then f contains a GPP over $\mathbb{Q}$ of degree > 1 as its composition factor if and only if $\lim_{\mathfrak{p}\in\Sigma_\mathbb{Q}} \mathrm{NP}_\mathfrak{p}(f)$ does not exist.*

In this note, we give a proof of the "only if" part of Wan's conjecture. Moreover, we get the following main result.

Theorem 1.2. *Let f be a non-constant monic polynomial in $K[x]$. If f contains a GPP over K of degree > 1 as its composition factor, then $\lim_{\mathfrak{p}\in\Sigma_K} \mathrm{NP}_\mathfrak{p}(f)$ does not exist.*

Remark. The "If" part of Conjecture 1.1 is much harder. So far, we know the following results:

(1) polynomials of small degree. This is shown by Sperber [13] and Hong [8,9].
(2) polynomials of the form $x^d + ax^s$. This is proved by Yang [16], Zhu [17,18], Liu–Niu [11] and Ouyang–Zhang [12].
(3) polynomials of the form $P(x^s)$. This can be deduced by Blache–Férard–Zhu's results in [4].
(4) the general case. This is proved in Zhu [17].

Remark. If we replace $\mathbb{Q}$ in Conjecture 1.1 by any number field K, then the "if" part does not hold in general. We give an example here. Let ℓ be a prime number greater than 3. Let $K = \mathbb{Q}(\zeta_\ell)$ and $f(x) =$ the Dickson polynomial $D_\ell(x, 1)$. By Lemma 2.5, f is not a permutation polynomial for all $k_\mathfrak{p}$ with $\mathfrak{p} \nmid 3\ell\omega$. Thus f is not a GPP over K. By Lemma 2.5, one can easily check that f is a GPP over $\mathbb{Q}$. Theorem 1.2 implies that $\lim_{p \in \Sigma_\mathbb{Q}} \mathrm{NP}_p(f)$ does not exist. By Proposition 2.3, $\lim_{\mathfrak{p} \in \Sigma_K} \mathrm{NP}_\mathfrak{p}(f)$ also does not exist.

2. Preliminary

2.1. Zeta functions and L-functions of exponential sums

We fix a rational prime p, a positive integer h and let $q = p^h$. Let C be a curve over $\mathbb{F}_q$. The Zeta function of C

$$Z(C, t) = \exp\left(\sum_{m=1}^{\infty} N_m(C)\frac{t^m}{m}\right) \tag{2.1}$$

is a rational function over $\mathbb{Q}$, where

$$N_m(C) = \#C(F_{q^m})$$

is the number of $\mathbb{F}_{q^m}$-rational points of C. If C is smooth and proper, by Weil [15], $Z(C, t)$ is of the form $\frac{P_C(t)}{(1-t)(1-qt)}$, where $P_C(t)$ is a polynomial of t of degree $2g(C)$ over $\mathbb{Z}$ and $g(C)$ is the genus of C. Denote the q-adic Newton polygon of $P_C(t)$ by $\mathrm{NP}_q(C)$.

Let g be a polynomial in $\mathbb{F}_q[x]$ of degree d with $(d, p) = 1$. The fraction field of the integral domain $\mathbb{F}_q[x, y]/(y^p - y - g)$, denoted by L_g, is a Galois extension of $\mathbb{F}_q(x)$, which is the function field of $\mathbb{P}^1_{\mathbb{F}_q}$. So $C(g)$, the normalization of $\mathbb{P}^1_{\mathbb{F}_q}$ in L_g, is a Galois cover of $\mathbb{P}^1_{\mathbb{F}_q}$ with Galois group isomorphic to $\mathbb{F}_p$. The Zeta function of the $C(g)$ admits the following decomposition

$$Z(C(g), t) = \prod_{\chi:\mathbb{F}_p \to \mu_p} L(g, \chi, t), \quad P_{C(g)}(t) = \prod_{\chi \neq 1} L(g, \chi, t).$$

Hence the study of the polynomial $P_{C(g)}(t)$ reduces to the study of $L(g, \chi, t)$ for nontrivial characters χ.

For polygon P, denote by $\mathrm{Len}(P, \lambda)$ the horizontal length of the segment of slope λ. As the Newton polygon $\mathrm{NP}_{\mathfrak{p}}(f)$ of $L(\overline{f}, \chi, t)$ is independent of the choice of $\chi \neq 1$, we have the following result:

Lemma 2.1. *For any λ, $\mathrm{Len}(\mathrm{NP}_q(C(\overline{f})), \lambda) = (p-1)\mathrm{Len}(\mathrm{NP}_{\mathfrak{p}}(f), \lambda)$.*

By [7, Corollary 5.2.6], if $P_C(t) = \prod_{i=1}^{2g(C)}(1-\alpha_i t)$, then $P_{C/\mathbb{F}_{q^n}}(t) = \prod_{i=1}^{2g(C)}(1-\alpha_i^n t)$. By the same method there, one has the following result.

Lemma 2.2. *Write $L(g, \chi, t)$ in the form $(1-\alpha_1 t)(1-\alpha_2 t)\cdots(1-\alpha_{d-1}t)$. For any $n \geq 1$, we have*

$$S_m(g, \chi) = -(\alpha_1^m + \alpha_2^m + \cdots + \alpha_{d-1}^m)$$

and

$$L(g/\mathbb{F}_{q^n}, \chi, t) = (1-\alpha_1^n t)(1-\alpha_2^n t)\cdots(1-\alpha_{d-1}^n t).$$

In particular, the q-adic Newton polygon of $L(g, \chi, t)$ is the same as the q^n-adic Newton polygon of $L(g/\mathbb{F}_{q^n}, \chi, t)$.

Proposition 2.3. *Let L/K be a finite extension of number fields and $\mathfrak{P}$ a place of L above $\mathfrak{p}$ a place of K. Then*

$$\mathrm{NP}_{\mathfrak{p}}(f) = \mathrm{NP}_{\mathfrak{P}}(f).$$

In particular, $\lim_{\mathfrak{p}\in\Sigma_K} \mathrm{NP}_{\mathfrak{p}}(f)$ exists if and only if $\lim_{\mathfrak{P}\in\Sigma_L} \mathrm{NP}_{\mathfrak{P}}(f)$ exists.

Proof. By definition, $\mathrm{NP}_{\mathfrak{p}}(f)$ is the q-adic Newton polygon of $L(\overline{f}/k_{\mathfrak{p}}, \chi, t)$ and $\mathrm{NP}_{\mathfrak{P}}(f)$ is the $q^{[k_{\mathfrak{P}}:k_{\mathfrak{p}}]}$-adic Newton polygon of $L(\overline{f}/k_{\mathfrak{P}}, \chi, t)$. By Lemma 2.2, we have $\mathrm{NP}_{\mathfrak{p}}(f) = \mathrm{NP}_{\mathfrak{P}}(f)$. □

We also need the following result about the divisibility of Zeta functions of curves.

Proposition 2.4 *([3, Proposition 5]). Let X, Y be two smooth separated complete curves over $\mathbb{F}_q$. If there is some finite $\mathbb{F}_q$-morphism $\pi: Y \to X$, then*

$$P_X(t) \mid P_Y(t).$$

2.2. Global permutation polynomials and Dickson polynomials

Let a be an element in a commutative ring R. For any $n \geq 1$, the Dickson polynomial of the first kind associated to a of degree n, denote by $D_n(x, a)$, is the unique polynomial over R such that

$$D_n\left(x + \frac{a}{x}, a\right) = x^n + \frac{a^n}{x^n}. \tag{2.2}$$

One can easily check that

$$D_n(x, 0) = x^n \tag{2.3}$$

and

$$D_{mn}(x, a) = D_m(D_n(x, a), a^n). \tag{2.4}$$

Lemma 2.5. *Let $a \in \mathbb{F}_q$ and n be a positive integer.*

1). *If $a = 0$, then $D_n(x, 0) = x^n$ is a permutation polynomial of $\mathbb{F}_q$ if and only if $(n, q - 1) = 1$.*
2). *If $a \neq 0$, then $D_n(x, a)$ is a permutation polynomial of $\mathbb{F}_q$ if and only if $(n, q^2 - 1) = 1$.*

Proof. Due to [5], see [10, Theorem 7.16] for quick reference. □

Proposition 2.6 *(Fried–Turnwald). Let f be a GPP over K. Then f is a composition of linear polynomials $\alpha_i x + \beta_i \in K[x]$ and the Dickson polynomials $D_{n_j}(x, a_j)$, where $a_j \in K$ and n_j are positive integers.*

Proof. See [6, Theorem 2] or [14, Theorem 2]. □

3. Proof of main result

We first show

Proposition 3.1. *Suppose that f contains $D_n(x, a)$ as a composition factor. Then for $\mathfrak{p} \in \Sigma_K$ such that*

(1) *$a \in \mathcal{O}_\mathfrak{p}$;*
(2) *$\mathfrak{p} \nmid 3n\omega$, where ω is the number of the roots of unity in K;*
(3) *$D_n(x, \overline{a})$ is a permutation polynomial on $k_\mathfrak{p}$,*

there exists $v_0 \in \mathbb{Q}$ such that $\mathrm{Len}(\mathrm{NP}_\mathfrak{p}(f), v_0) \geq 2$ and hence the gap between $NP_\mathfrak{p}(f)$ and $\mathrm{HP}(f)$ is at least $\frac{1}{2d}$.

Proof. Write f in the form $f_1 \circ D_n(x,a) \circ f_3$. As $D_n(x,\overline{a})$ is a permutation polynomial on $k_{\mathfrak{p}}$, by Lemma 2.5, $(n, q-1) = 1$. As $\mathfrak{p} \nmid \omega$, the reduction induces an inclusion $\mu_K \subset \mu_{k_{\mathfrak{p}}}$, and hence $\omega \mid q-1$. So we have $(n,\omega) = 1$. By (2.4), we may assume that n is an odd prime number. Set $e = 1$ if $\overline{a} = 0$ and otherwise $e = 2$. By Lemma 2.5, we have $(q^e - 1, n) = 1$. As n is an odd prime number, $(q^{(n-1)s+1})^e \equiv q^e \not\equiv 1 \mod n$ and so $((q^{(n-1)s+1})^e - 1, n) = 1$. Using Lemma 2.5 again, $D_n(x,\overline{a})$ is permutation polynomial of $k_{\mathfrak{p}}^m$, where $m = (n-1)s + 1$ and s is a non-negative integer. For these m and any nontrivial character $\chi : \mathbb{F}_p \to \mu_p$, we have that

$$S_m(\overline{f}_1, \chi) = S_m(\overline{f}_1 \circ D_n(x,\overline{a}), \chi). \tag{3.1}$$

Assume that

$$L(\overline{f}_1, \chi, t) = (1-\alpha_1 t)(1-\alpha_2 t)\cdots(1-\alpha_{d_1-1} t)$$

and

$$L(\overline{f}_1 \circ D_n(x,\overline{a}), \chi, t) = (1-\beta_1 t)(1-\beta_2 t)\cdots(1-\beta_{nd_1-1} t),$$

where d_1 is the degree of f_1. Lemma 2.2 implies that

$$S_m(\overline{f}_1, \chi) = -(\alpha_1^m + \alpha_2^m + \cdots + \alpha_{d_1-1}^m)$$

and

$$S_m(\overline{f}_1 \circ D_n(x,\overline{a}), \chi) = -(\beta_1^m + \beta_2^m + \cdots + \beta_{nd_1-1}^m).$$

By (3.1), we have an equality of power series

$$\sum_{m=(n-1)s+1} (\alpha_1^m + \alpha_2^m + \cdots + \alpha_{d_1-1}^m) t^m = \sum_{m=(n-1)s+1} (\beta_1^m + \beta_2^m + \cdots + \beta_{nd_1-1}^m) t^m.$$

Hence

$$\sum_{i=1}^{d_1-1} \frac{\alpha_i t}{1-(\alpha_i t)^{n-1}} = \sum_{i=1}^{nd_1-1} \frac{\beta_i t}{1-(\beta_i t)^{n-1}}.$$

Comparing the poles on both sides, there exist $1 \le i < j \le nd_1 - 1$ such that

$$\beta_i^{n-1} = \beta_j^{n-1}.$$

Denote by v_0 the q-adic valuation of β_i (and of β_j). Then

$$\mathrm{Len}(\mathrm{NP}_{\mathfrak{p}}(f_1 \circ D_n(x,a)), v_0) \ge 2.$$

Denote $C' = C(\overline{f}_1 \circ D_n(x, \overline{a}))$, by Lemma 2.1,

$$\mathrm{Len}(\mathrm{NP}_q(C'), v_0) \geq 2(p-1).$$

Denote $C = C(f)$, one can check that

$$k_{\mathfrak{p}}(C') = k_{\mathfrak{p}}(x, y') \text{ and } k_{\mathfrak{p}}(C) = k_{\mathfrak{p}}(x, y),$$

where $(y')^p - y' = \overline{f}_1 \circ D_n(x, \overline{a})$ and $y^p - y = f(x)$. The embedding

$$k_{\mathfrak{p}}(x, y') \to k_{\mathfrak{p}}(x, y)$$

sending x to $\overline{f_3}$ and y' to y induces a non-constant morphism

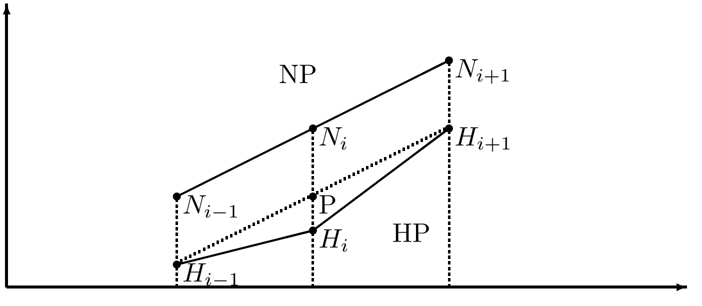
$$\pi : C \to C'$$

of complete smooth curves. By Proposition 2.4,

$$\mathrm{Len}(\mathrm{NP}_q(C), v_0) \geq \mathrm{Len}(\mathrm{NP}_q(C'), v_0) \geq 2(p-1).$$

Using Lemma 2.1 again, we have

$$\mathrm{Len}(\mathrm{NP}_{\mathfrak{p}}(f), v_0) \geq 2.$$



As in the above diagram, we assume that $N_{i-1}N_i$ and N_iN_{i+1} are of the same slope. The slopes of $H_{i-1}H_i$ and H_iH_{i+1} are $\frac{i}{d}$ and $\frac{i+1}{d}$, respectively. As the HP is below the NP, we know that $N_{i\pm 1}$ is above $H_{i\pm 1}$. Hence the middle point N_i of $N_{i-1}N_{i+1}$ is above P that of $H_{i-1}H_{i+1}$. So we have

$$|N_iH_i| \geq |PH_i| \geq \frac{1}{2d}. \quad \square$$

Proof of main result. Write f in the form $f_1 \circ f_2 \circ f_3$, where f_2 is a GPP over K of degree > 1. As every composition factor of a GPP is still a GPP, by Proposition 2.6, we can assume that $f_2 = D_n(x, a)$ is a GPP over K, where $a \in K$ and $n \in \mathbb{Z}_{>1}$.

For the a and n, by definition of GPP, there are infinitely many $\mathfrak{p} \in \Sigma_K$ satisfying the three conditions in Proposition 3.1. For those $\mathfrak{p}$, by Proposition 3.1, the gap between $NP_{\mathfrak{p}}(f)$ and $\mathrm{HP}(f)$ is at least $\frac{1}{2d}$. However, for places $\mathfrak{p}$ such that $p_{\mathfrak{p}} \equiv 1 \mod d$, we know $NP_{\mathfrak{p}}(f) = \mathrm{HP}(f)$. So the limit does not exist. □

Acknowledgments

Research is partially supported by National Key Basic Research Program of China (Grant No. 2013CB834202) and National Natural Science Foundation of China (Grant Nos. 11171317 and 11571328).

References

[1] A. Adolphson, S. Sperber, Newton polyhedra and the degree of the L-function associated to an exponential sum, Invent. Math. 88 (1987) 555–569.
[2] A. Adolphson, S. Sperber, Exponential sums and Newton polyhedra: cohomology and estimates, Ann. Math. 130 (1989) 367–406.
[3] Y. Aubry, M. Perret, Divisibility of zeta functions of curves in a covering, Arch. Math. 82 (2004) 205–213.
[4] R. Blache, E. Férard, H.J. Zhu, Hodge–Stickelberger polygons for L-functions of exponential sums of $P(x^s)$, Math. Res. Lett. 15 (5) (2008) 1053–1071.
[5] 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. Math. 11 (1–6) (1896/1897) 65–120, 161–183.
[6] M. Fried, On a conjecture of Schur, Mich. Math. J. 17 (1970) 41–55.
[7] D.M. Goldschmidt, Algebraic Functions and Projective Curves, Graduate Texts in Mathematics, vol. 215, Springer-Verlag, New York, ISBN 0-387-95432-5, 2003, xvi+179 pp.
[8] S. Hong, Newton polygons of L-functions associated with exponential sums of polynomials of degree four over finite fields, Finite Fields Appl. 7 (2001) 205–237.
[9] S. Hong, Newton polygons for L-functions of exponential sums of polynomials of degree six over finite fields, J. Number Theory 97 (2002) 368–396.
[10] R. Lidl, H. Niederreiter, Finite Fields, Encyclopedia of Mathematics and its Applications, vol. 20, Addison–Wesley Publishing Company, Reading, MA, 1983.
[11] C. Liu, C. Niu, Generic twisted T-adic exponential sums of binomials, Sci. China Math. 54 (5) (2011) 865–875.
[12] Y. Ouyang, S. Zhang, Newton polygons of L-functions of polynomials x^d+ax^{d-1} with $p \equiv -1 \mod d$, Finite Fields Appl. 37 (2016) 285–294.
[13] S. Sperber, On the p-adic theory of exponential sums, Am. J. Math. 108 (1986) 255–296.
[14] G. Turnwald, On Schur's conjecture, J. Aust. Math. Soc. A 58 (3) (1995) 312–357.
[15] A. Weil, Numbers of solutions of equations in finite fields, Bull. Am. Math. Soc. 55 (1949) 497–508.
[16] R. Yang, Newton polygons of L-functions of polynomials of the form $x^d + \lambda x$, Finite Fields Appl. 9 (1) (2003) 59–88.
[17] H.J. Zhu, p-adic variation of L functions of one variable exponential sums. I, Am. J. Math. 125 (3) (2003) 669–690.
[18] H.J. Zhu, Generic A-family of exponential sums, J. Number Theory 143 (2014) 82–101.