THE FIRST SLOPE CASE OF WAN'S CONJECTURE

JASPER SCHOLTEN AND HUI JUNE ZHU

ABSTRACT. Let $d \geq 2$ and p a prime coprime to d. For $f(x) \in (\mathbb{Z}_p \cap \mathbb{Q})[x]$, let $\mathrm{NP}_1(f \bmod p)$ denote the first slope of the Newton polygon of the L-function of the exponential sums $\sum_{x\in\mathbb{F}_{p^\ell}} \zeta_p^{\mathrm{Tr}_{\mathbb{F}_{p^\ell}/\mathbb{F}_p}(f(x))}$. We prove that there is a Zariski dense open subset $\mathcal{U}$ in the space $\mathbb{A}^d$ of degree-d monic polynomials over $\mathbb{Q}$ such that for all $f(x) \in \mathcal{U}$ we have $\lim_{p\to\infty} \mathrm{NP}_1(f \bmod p) = \frac{1}{d}$. This is a "first slope case" of a conjecture of Wan.

Let $d \geq 2$ be an integer and p a prime coprime to d. Let $\mathbb{A}^d$ be the set of all degree-d monic polynomials over $\mathbb{Q}$. For any $f(x) = x^d + a_{d-1}x^{d-1} + \ldots + a_0 \in (\mathbb{Z}_p \cap \mathbb{Q})[x]$ and for any integer $\ell \geq 1$ let $S_\ell(f) := \sum_{x\in\mathbb{F}_{p^\ell}} \zeta_p^{\mathrm{Tr}_{\mathbb{F}_{p^\ell}/\mathbb{F}_p}(f(x))}$. The L function of $f(x) \bmod p$ is defined by $L(f \bmod p; T) = \exp\left(\sum_{\ell=1}^{\infty} S_\ell(f)\frac{T^\ell}{\ell}\right)$. It is a theorem of Dwork-Bombieri-Grothendieck that $L(f \bmod p; T) = 1 + b_1T + \ldots + b_{d-1}T^{d-1} \in \mathbb{Z}[\zeta_p][T]$ for some p-th root of unity ζ_p in $\overline{\mathbb{Q}}$. Define the *Newton polygon* of $f \bmod p$, denoted by $\mathrm{NP}(f \bmod p)$, as the lower convex hull of the points $(\ell, \mathrm{ord}_p b_\ell)$ in $\mathbb{R}^2$ for $0 \leq \ell \leq d-1$ where we set $b_0 = 1$. It is exactly the p-adic Newton polygon of the polynomial $L(f \bmod p; T)$. Let $\mathrm{NP}_1(f \bmod p)$ denote its first slope. Define the *Hodge polygon* $\mathrm{HP}(f)$ as the convex hull in $\mathbb{R}^2$ of the points $(\ell, \frac{\ell(\ell+1)}{2d})$ for $0 \leq \ell \leq d-1$. It is proved that the Newton polygon is always lying above the Hodge polygon (see [3] [6] and [2]). The following conjecture was proposed by Wan in the Berkeley number theory seminar in the fall of 2000, a general form of which will appear in [7, Section 2.5].

Conjecture 1 (Wan). *There is a Zariski dense open subset $\mathcal{U}$ in $\mathbb{A}^d$ such that for all $f(x) \in \mathcal{U}$ we have* $\lim_{p\to\infty} \mathrm{NP}(f \bmod p) = \mathrm{HP}(f)$.

The cases $d = 3$ and 4 are proved in [6] and [4], respectively. It is also known that if $p \equiv 1 \bmod d$ then $\mathrm{NP}(f \bmod p) = \mathrm{HP}(f)$ for all $f \in \mathbb{A}^d$ (see [1]). In this paper we use an elementary method to prove the "first slope case" of this conjecture.

For any real number r let $\lceil r \rceil$ denote the least integer greater than or equal to r. For any integer N and for any Laurent polynomial $g(x)$ in one variable, we use $[g(x)]_{x^N}$ to denote the x^N-coefficient of $g(x)$.

Theorem 2. *Let $d \geq 2$ and p a prime coprime to d. Let $f(x)$ be a degree-d monic polynomial in $(\mathbb{Z}_p \cap \mathbb{Q})[x]$. Suppose $\left[f(x)^{\lceil \frac{p-1}{d} \rceil}\right]_{x^{p-1}} \not\equiv 0 \bmod p$. If $p > \frac{d}{2} + 1$ then* $\mathrm{NP}_1(f \bmod p) = \lceil \frac{p-1}{d} \rceil / (p-1)$.

Date: February 1, 2002.

1991 *Mathematics Subject Classification.* 11L, 14H, 14M.

Key words and phrases. Artin-Schreier curves, exponential sums, Newton polygon, Hodge polygon, zeta and L functions over finite fields, Wan's Conjecture.

Proof. Suppose $p > \frac{d}{2}+1$. For $k \geq 0$ let $c_k := \sum_{x=0}^{p-1}\binom{f(x)}{k}$. Then

$$c_k \equiv \sum_{0\leq n\leq \deg\binom{f(x)}{k}} \left[\binom{f(x)}{k}\right]_{x^n} \sum_{\bar{x}\in\mathbb{F}_p} \bar{x}^n \bmod p, \tag{1}$$

where 0^0 is defined as 1. Note that if k is an integer such that $0 \leq k < \lceil \frac{p-1}{d} \rceil$ then $k < \frac{p-1}{d}$, and consequently $\deg \binom{f(x)}{k} = dk < p-1$.

If $\frac{d}{2}+1 < p < d$ then $\lceil\frac{p-1}{d}\rceil = 1$ and $d\lceil\frac{p-1}{d}\rceil < 2(p-1)$. If $p > d$ then $d\lceil\frac{p-1}{d}\rceil \leq d\frac{p+d-2}{d} < 2(p-1)$. So for all $p > \frac{d}{2}+1$ we have $\deg\binom{f(x)}{\lceil\frac{p-1}{d}\rceil} = d\lceil\frac{p-1}{d}\rceil < 2(p-1)$.

Consider the elementary fact that $\sum_{\bar{x}\in\mathbb{F}_p}\bar{x}^n = 0$ if $(p-1)\nmid n$ or $n=0$, and $\sum_{\bar{x}\in\mathbb{F}_p}\bar{x}^n = -1$ otherwise. Combining with the estimates on $\deg\binom{f(x)}{k}$ above, it follows from (1) that $c_k = 0$ for $k < \lceil\frac{p-1}{d}\rceil$ and

$$c_{\lceil\frac{p-1}{d}\rceil} \equiv -\frac{1}{\lceil\frac{p-1}{d}\rceil!}\left[f(x)^{\lceil\frac{p-1}{d}\rceil}\right]_{x^{p-1}} \not\equiv 0 \bmod p.$$

We abbreviate NP_1 for $\mathrm{NP}_1(f \bmod p)$ in this proof. Let $\pi = \zeta_p - 1$, so $\mathrm{ord}_p(\pi) = \frac{1}{p-1}$. Then $S_1(f) = \sum_{\bar{x}\in\mathbb{F}_p}(1+\pi)^{f(\bar{x})} \equiv \sum_{k=0}^{p-2} c_k\pi^k \bmod p$, hence

$$\mathrm{NP}_1 \leq \mathrm{ord}_p(S_1(f)) = \lceil\tfrac{p-1}{d}\rceil/(p-1). \tag{2}$$

Denote the horizontal length of the first-slope-segment of $\mathrm{NP}(f \bmod p)$ by ℓ. From the fact the Newton polygon is above the Hodge polygon it follows that $\frac{\ell(\ell+1)}{2d} \leq \ell\mathrm{NP}_1$. Combining this with the inequality in (2) yields

$$\ell+1 \leq \tfrac{2d}{p-1}\lceil\tfrac{p-1}{d}\rceil. \tag{3}$$

If $\frac{2d}{3}+1 < p \leq d+1$ then $\lceil\frac{p-1}{d}\rceil = 1$ and (3) implies $\ell+1 < 3$, hence $\ell = 1$. If $\frac{4d}{3}+1 < p < 2d$ then $\lceil\frac{p-1}{d}\rceil = 2$ and (3) again implies $\ell = 1$. If $2d < p$ then $\ell+1 \leq \frac{2d}{p-1}\lceil\frac{p-1}{d}\rceil \leq \frac{2d(p+d-2)}{(p-1)d} < \frac{3p-4}{p-1} < 3$ so $\ell = 1$. If $\frac{d}{2}+1 < p \leq \frac{2d}{3}+1$ then $\lceil\frac{p-1}{d}\rceil = 1$ and $\ell+1 \leq \frac{2d}{p-1} < 4$, so $\ell \leq 2$. If $d+1 < p \leq \frac{4d}{3}+1$ then $\lceil\frac{p-1}{d}\rceil = 2$ and $\ell+1 \leq \frac{4d}{p-1} < 4$, so again $\ell \leq 2$.

We remark that the y-coordinates of bending points of $\mathrm{NP}(f \bmod p)$ are integral multiples of $\frac{1}{p-1}$ because $L(f \bmod p; T) \in \mathbb{Z}[\zeta_p][T]$. The Hodge polygon bound gives $\mathrm{NP}_1 \geq \frac{1}{d}$. So if $\ell = 1$ then $(p-1)\mathrm{NP}_1$ is an integer $\geq \frac{p-1}{d}$, hence $\mathrm{NP}_1 \geq \lceil\frac{p-1}{d}\rceil/(p-1)$. If $\ell = 2$ then $2(p-1)\mathrm{NP}_1$ is an integer $\geq \frac{3(p-1)}{d}$, hence $\mathrm{NP}_1 \geq \left\lceil\frac{3(p-1)}{d}\right\rceil/(2(p-1))$. We have seen that this case only occurs for $\frac{d}{2}+1 < p \leq \frac{2d}{3}+1$ or $d+1 < p \leq \frac{4d}{3}+1$, which implies $\left\lceil\frac{3(p-1)}{d}\right\rceil = 2$, $\lceil\frac{p-1}{d}\rceil = 1$ or $\left\lceil\frac{3(p-1)}{d}\right\rceil = 4$, $\lceil\frac{p-1}{d}\rceil = 2$ respectively, and consequently $\left\lceil\frac{3(p-1)}{d}\right\rceil/(2(p-1)) = \left\lceil\frac{(p-1)}{d}\right\rceil/(p-1)$. This proves the theorem. □

Theorem 3. *Let $d \geq 2$. Let $\mathcal{U}$ be the set of all monic polynomials $f(x) = x^d + a_{d-1}x^{d-1} + \cdots + a_0$ in $\mathbb{A}^d$ such that $[f(x)^{\lceil\frac{p-1}{d}\rceil}]_{x^{p-1}} \not\equiv 0 \bmod p$ for all but finitely many primes p. Then $\mathcal{U}$ is Zariski open and dense in $\mathbb{A}^d$. For every $f(x) \in \mathcal{U}$ we have*

$$\lim_{p\to\infty} \mathrm{NP}_1(f \bmod p) = \frac{1}{d}. \tag{4}$$

Proof. Let r be any integer with $1 \leq r \leq d-1$ and $\gcd(r,d)=1$. Let r' be the least non-negative residue of $1-r \bmod d$. Let $h := \prod_{\substack{1\leq r\leq d-1\\ \gcd(r,d)=1}} h_r$, where

$$h_r := \left[\sum_{\ell=0}^{r'} \binom{\frac{r'-1}{d}}{\ell}(A_{d-1}x^{-1}+\ldots+A_0x^{-d})^\ell\right]_{x^{-r'}} \in \mathbb{Q}[A_0,\ldots,A_{d-1}].$$

By the hypothesis on r and r', we see that $-1 < \frac{r'-1}{d} < 1$ and $\frac{r'-1}{d} \neq 0$, and hence $[h_r]_{A_{d-1}^{r'}} = \binom{\frac{r'-1}{d}}{r'} \neq 0$ for every r. Therefore the polynomial h is not zero.

For every prime $p \equiv r \bmod d$ we have $\lceil \frac{p-1}{d} \rceil = \frac{p-1+r'}{d} \equiv \frac{r'-1}{d} \bmod p$. So

$$\begin{aligned}
\left[f(x)^{\lceil \frac{p-1}{d}\rceil}\right]_{x^{p-1}} &= \left[(x^{-d}f(x))^{\lceil \frac{p-1}{d}\rceil}\right]_{x^{-r'}}\\
&= \left[(1+a_{d-1}x^{-1}+\cdots+a_0x^{-d})^{\lceil \frac{p-1}{d}\rceil}\right]_{x^{-r'}}\\
&= \left[\sum_{\ell=0}^{r'}\binom{\lceil\frac{p-1}{d}\rceil}{\ell}(a_{d-1}x^{-1}+\cdots+a_0x^{-d})^\ell\right]_{x^{-r'}}\\
&\equiv h_r(a_0,\ldots,a_{d-1}) \bmod p.
\end{aligned}$$

Thus $f(x) \in \mathcal{U}$ if and only if $h(a_0,\ldots,a_{d-1}) \not\equiv 0 \bmod p$ for all but finitely many p. The latter is equivalent to $h(a_0,\ldots,a_{d-1}) \neq 0$. But we already know that h is a non-zero polynomial, so $\mathcal{U}$ must be Zariski dense in $\mathbb{A}^d$.

Let $f(x) \in \mathcal{U}$. Then there exists an integer N such that for all $p > N$ we have $\mathrm{NP}_1(f \bmod p) = \frac{\lceil \frac{p-1}{d}\rceil}{p-1}$ by Theorem 2. Therefore, for every $f(x) \in \mathcal{U}$ we have (4) holds. □

Acknowledgments. We thank Bjorn Poonen for invaluable contribution to the proof of Theorem 3. We also thank the referees for comments. The research of Hui June Zhu was partially supported by a grant of Bjorn Poonen from the David and Lucile Packard Foundation.

References

[1] Alan Adolphson; Steven Sperber: p-adic estimates for exponential sums and the theorem of Chevalley-Warning, *Ann. Sci. Ecole Norm. Sup. (4),* **20** (1987), 545–556.

[2] Alan Adolphson; Steven Sperber: Newton polyhedra and the degree of the L-function associated to an exponential sum, *Invent. Math.* **88** (1987), 555–569.

[3] Enrico Bombieri: On exponential sums in finite fields. *American J. Mathematics,* **88** (1966), 71–105.

[4] Shaofang Hong: Newton polygons of L functions associated with exponential sums of polynomials of degree four over finite fields, *Finite fields and their applications.* **7** (2001), 205–237.

[5] Jasper Scholten; Hui June Zhu: Slope estimates of Artin-Schreier curves, electronic preprint available online at `http://xxx.lanl.gov/abs/math.AG/0105005`, 2001.

[6] Steven Sperber: On the p-adic theory of exponential sums, *American J. Math.,* **109** (1986), 255–296.

[7] Daqing Wan: An introduction to the theory of Newton polygons for L-functions of exponential sums, To appear. Preprint available at `http://www.math.uci.edu/~dwan/Overview.html`.

Mathematisch Instituut, Katholieke Universiteit Nijmegen, Postbus 9010, 6500 GL Nijmegen. The Netherlands.

E-mail address: `scholten@sci.kun.nl`

Department of mathematics, University of California, Berkeley, CA 94720-3840. The United States.
E-mail address: zhu@alum.calberkeley.org