NEWTON STRATIFICATION FOR POLYNOMIALS: THE OPEN STRATUM.

RÉGIS BLACHE AND ÉRIC FÉRARD

Abstract. In this paper we consider the Newton polygons of $L$-functions coming from additive exponential sums associated to a polynomial over a finite field $\mathbb{F}_q$. These polygons define a stratification of the space of polynomials of fixed degree. We determine the open stratum: we give the generic Newton polygon for polynomials of degree $d \geq 2$ when the characteristic $p$ is greater than $3d$, and the Hasse polynomial, i.e. the equation defining the hypersurface complementary to the open stratum.

0. Introduction

Let $k := \mathbb{F}_q$ be the finite field with $q := p^m$ elements, and for any $r \geq 1$, let $k_r$ denote its extension of degree $r$. If $\psi$ is a non trivial additive character on $\mathbb{F}_q$, then $\psi^r := \psi \circ \text{Tr}_{k_r/k}$ is a non trivial additive character of $k_r$, where $\text{Tr}_{k_r/k}$ denotes the trace from $k_r$ to $k$. Let $f \in k[X]$ be a polynomial of degree $d \geq 2$ prime to $p$; then for any $r$ we form the additive exponential sum

$$S_r(f, \psi) := \sum_{x \in k_r} \psi^r(f(x)).$$

To this family of sums, one associates the $L$-function

$$L(f, T) := \exp \left( \sum_{r \geq 1} S_r(f, \psi) T^r \right).$$

It follows from the work of Weil on the Riemann hypothesis for function fields in characteristic $p$ that this $L$-function is actually a polynomial of degree $d - 1$. Consequently we can write

$$L(f, T) = (1 - \theta_1 T) \cdots (1 - \theta_d T).$$

Another consequence of the work of Weil is that the reciprocal roots $\theta_1, \ldots, \theta_d$ are $q$-Weil numbers of weight 1, i.e. algebraic integers all of whose conjugates have complex absolute $q^{\frac{1}{d}}$. Moreover, for any prime $\ell \neq p$, they are $\ell$-adic units, that is $|\theta_i|_\ell = 1$.

A natural question is to determine their $q$-adic absolute value, or equivalently their $p$-adic valuation. In other words, one would like to determine the Newton polygon $NP_q(f)$ of $L(f, T)$ where $NP_q$ means the Newton polygon taken with respect to the valuation $v_q$ normalized by $v_q(q) = 1$ (cf. [9], Chapter IV for the link between the Newton polygon of a polynomial and the valuations of its roots). There is an elegant general answer to this problem when $p \equiv 1 \ [d]$, $p \geq 5$: then the Newton polygon $NP_q(f)$ has vertices (cf. [10], Theorem 7.5)

$$\left( n, \frac{n(n+1)}{2d} \right)_{1 \leq n \leq d-1}.$$
This polygon is often called the *Hodge polygon* for polynomials of degree \(d\), and denoted by \(HP(d)\).

Unfortunately, if we don’t have \(p \equiv 1 \mod d\), there is no such general answer. We know that \(NP_q(f)\) lies above \(HP(d)\). This polygon can vary greatly depending on the coefficients of \(f\), and it seems hopeless to give a general answer to the question above, as show the known examples (cf. [12] for degree 3 polynomials, [3] and [7] for degree 4 and degree 6 polynomials respectively). On the other hand, we have asymptotic results (cf. [11], [14]): in these papers, Zhu proves the one-dimensional case of Wan’s conjecture (cf. [13] Conjecture 1.12), i.e. that there is a Zariski dense open subset \(U\) of the space of polynomials of degree \(d\) over \(\overline{\mathbb{Q}}\) such that when \(p\) tends to infinity, for any \(f \in U\), the polygon \(NP_q(f)\) obtained from the reduction of \(f\) modulo a prime above \(p\) in the field defined by the coefficients of \(f\), we have \(\lim_{p \to \infty} NP_q(f) = HP(d)\).

A general result concerning Newton polygons is *Grothendieck’s specialization theorem*. In order to quote it, let us recall some results about crystals. Let \(L_\psi\) denote the *Artin–Schreier crystal*; this is an overconvergent *\(F\)-isocrystal over \(\mathbb{A}^1\)*) (cf. [4] 6.5), and for any polynomial \(f \in k[x]\) of degree \(d\), we have an overconvergent \(F\)-isocrystal \(f^*L_\psi\) with (cf. [2])
\[
L(f,T) = \det(1 - T\phi_\psi|H^1_{rig,c}(k^1/K,f^*L_\psi)) .
\]

Now if we parametrize the set of degree \(d\) monic polynomials without constant coefficient by the affine space \(k^{d-1}\), associating the point \((a_1, \ldots, a_{d-1})\) to the polynomial \(f(X) = X^d + a_{d-1}X^{d-1} + \cdots + a_1X\), we can consider the family of overconvergent \(F\)-isocrystals \(f^*L_\psi\). Now for a family of \(F\)-crystal \((\mathcal{M}, F)\) of rank \(r\) over a \(\mathbb{F}_p\)-algebra \(A\), we have Grothendieck’s specialization theorem (cf. [5], [8] Corollary 2.3.2)

*Let \(P\) be the graph of a continuous \(\mathbb{R}\)-valued function on \([0, r]\) which is linear between successive integers. The set of points in Spec \((A)\) at which the Newton polygon of \((\mathcal{M}, F)\) lies above \(P\) is Zariski closed, and is locally on Spec \((A)\) the zero-set of a finitely generated ideal.*

In other words, this theorem means that when \(f\) runs over polynomials of degree \(d\) over \(\mathbb{F}_q\), then there is a Zariski dense open subset \(U_{d,p}\) (the open stratum) of the (affine) space of these polynomials, and a generic Newton polygon \(GP(d, p)\) such that for any \(f \in U_{d,p}\), \(NP_q(f) = GP(d, p)\), and \(NP_q(f) \geq GP(d, p)\) for any \(f \in \mathbb{F}_q[X]\), \(f\) monic of degree \(d\) (where \(NP \geq NP'\) means \(NP\) lies above \(NP'\)).

The aim of this article is to determine explicitly both the generic polygon \(GP(d, p)\) and the associated Hasse polynomial \(H_{d,p}\), i.e. the exact polynomial such that \(U_{d,p}\) is the complementary of the hypersurface \(H_{d,p} = 0\). To be more precise, let \(p \geq 3d\) be a prime; a *normalized* polynomial of degree \(d\) over \(\mathbb{F}_q\) is \(f(x) = x^d + a_{d-2}x^{d-2} + \cdots + a_1x \in \mathbb{F}_q[x]\); we identify the space of normalized polynomials with the affine space \(k^{d-2}(\mathbb{F}_q)\). Then the generic polygon \(GP(d, p)\) has vertices \[
\left(\frac{n}{p-1}, \frac{Y_n}{p-1}\right)_{1 \leq n \leq d-1}, \quad Y_n := \min_{\sigma \leq N_\infty} \sum_{k=1}^n \frac{pk - \sigma(k)}{d},
\]
and we have \(NP_q(f) = GP(d, p)\) exactly when \(H_{d,p}(a_1, \ldots, a_{d-2}) \neq 0\), with \(H_{d,p}\) the Hasse polynomial, that we determine explicitly. Note that both \(GP(d, p)\) and \(H_{d,p}\) do not depend on \(q\), but only on \(p\).

The above results improve recent works of Scholten-Zhu (cf. [11]) and Zhu (cf. [11], [14]). In [11], Scholten and Zhu determine the first generic slope and the polynomials having this slope, and our work is a generalization of this result to
the whole Newton polygon. In [13], the generic Newton polygon is determined, but its $n$-th vertex depends on an intricated constant $\varepsilon_n$; moreover, Zhu doesn’t need to give the exact equation defining $U_{d,p}$ since she just wants to prove its non emptyness.

We use $p$-adic cohomology, following the works of Dwork, Robba and others. To be more precise, we use Washnitzer-Monsky spaces of overconvergent series $H^1(A)$; one can define a linear operator $\beta$ on $H^1(A)$ and a differential operator $D$ with finite index on this space such that $\beta$ and $D$ commute up to a power of $p$. Then the linear map $\pi = \beta^{-1} \beta \beta^{-2} \ldots \beta$ (for the Frobenius on the quotient $H^1(A)/DH^1(A)$ has characteristic polynomial (almost) equal to $L(f,T)$. Using a monomial basis of $H^1(A)/DH^1(A)$, we are able to give congruences for the coefficients of the matrix $M := \text{Mat}_B(\pi)$ in terms of the coefficients of a lift of $f$. We deduce congruences for the minors of $N := \text{Mat}_B(\pi)$, i.e. for the coefficients of the function $L(f,T)$.

The paper is organized as follows: in section 1, we recall the results from $p$-adic cohomology we use, reducing the calculation of the $L$-function to the calculation of the characteristic polynomial. In section 2, the generic Newton polygon is determined, $\pi$ be the Frobenius; it is the generator of $\text{Gal}(K_m/Q_p)$ which acts on $\mathcal{T}_m$ as the $p$th power map. Finally we denote by $C_p$ a completion of a fixed algebraic closure $\overline{Q}_p$ of $Q_p$. Let $\pi \in C_p$ be a root of the polynomial $X^r - 1 + p$. It is well known that $Q_p(\pi) = Q_p(\zeta_p)$ is a totally ramified extension of degree $p - 1$ of $Q_p$. We shall frequently use the valuation $v := v_{\pi}$, normalized by $v_{\pi}(\pi) = 1$, instead of the usual $p$-adic valuation $v_p$, or the $q$-adic valuation $v_q$.

1. $p$-adic differential operators and exponential sums.

In this section, we recall well known results about $p$-adic differential operators, and their application to the evaluation of the $L$-function of exponential sums. The reader interested in more details and the proofs should refer to [10].

We denote by $Q_p$ the field of $p$-adic numbers, and by $K_m$ its $p$-adic valuation ring.

Let $\pi \in C_p$ be a root of the polynomial $X^{r-1} + p$. It is well known that $Q_p(\pi) = Q_p(\zeta_p)$ is a totally ramified extension of degree $p - 1$ of $Q_p$. We shall frequently use the valuation $v := v_{\pi}$, normalized by $v_{\pi}(\pi) = 1$, instead of the usual $p$-adic valuation $v_p$, or the $q$-adic valuation $v_q$.

1.1. Index of $p$-adic differential operators of order 1. In this paragraph, we denote by $\Omega$ an algebraically closed field containing $C_p$, complete under a valuation extending that of $C_p$, and such that the residue class field of $\Omega$ is a transcendental extension of the residue class field of $C_p$. For any $\omega \in \Omega$, $r \in R$, we denote by $B(\omega ; r^+)$ (resp. $B(\omega ; r^-)$) the closed (resp. open) ball in $\Omega$ with center $\omega$ and radius $r$.

Let $f(X) := a_d X^d + \cdots + a_1 X$, $a_d \neq 0$ be a polynomial of degree $d$, prime to $p$, over the field $\mathbb{F}_q$, and let $g(x) := a_d X^d + \cdots + a_1 X \in \mathcal{O}_m[X]$ be the polynomial whose
coefficients are the Teichmüller lifts of those of $f$. Let $A := B(0, 1^+) \setminus B(0, 1^-)$. We consider the space $\mathcal{H}^1(A)$ of overconvergent analytic functions on $A$.

Define the function $H := \exp(\pi g(X))$; note that since $X \mapsto \exp(\pi X)$ has radius of convergence 1, $H$ is not an element of $\mathcal{H}^1(A)$. Now let $D$ be the differential operator (where a function acts on $\mathcal{H}^1(A)$ by multiplication)

$$D := X \frac{d}{dX} - \pi X g'(X) \left(= H^{-1} \circ X \frac{d}{dX} \circ H\right).$$

Since $H$ is not in $\mathcal{H}^1(A)$, $D$ is injective in $\mathcal{H}^1(A)$. Thus the index of $D$ in $\mathcal{H}^1(A)$ is the dimension of its cokernel. By [10] Proposition 5.4.3 p226), this dimension is $d$.

On the other hand, since $D$ can be seen as a differential operator acting on $\mathbb{C}_p[X, \frac{1}{X}]$, Theorem 5.6 of [10] ensures that a complementary subspace of $D \mathbb{C}_p[X, \frac{1}{X}]$ in $\mathbb{C}_p[X, \frac{1}{X}]$ is also a complementary subspace of $D \mathcal{H}^1(A)$ in $\mathcal{H}^1(A)$. Now an easy calculation gives, for any $n \in \mathbb{Z}$

$$DX^{n-d} = (n-d)X^{n-d} + \pi \sum_{i=1}^{d} i a_i X^{i+n-d},$$

and since this function is clearly in $D \mathcal{H}^1(A)$, we get, for $n \geq d$

$$X^n \equiv -\frac{n-d}{\pi} X^{n-d} - \sum_{i=1}^{d-1} i a_i X^{i+n-d} \; [D \mathcal{H}^1(A)],$$

and for $n < 0$, $X^n \equiv -\frac{n}{\pi} \sum_{i=1}^{d} i a_i X^{i+n} \; [D \mathcal{H}^1(A)]$. Thus $B := \{1, \ldots, X^{d-1}\}$ forms a basis of a complementary subspace of $D \mathcal{H}^1(A)$ in $\mathcal{H}^1(A)$, and for every $n \in \mathbb{Z}$, $X^n$ can be written uniquely as

$$X^n \equiv \sum_{i=0}^{d-1} a_{ni} X^i \; [D \mathcal{H}^1(A)],$$

for some $a_{ni} \in K_n(\pi)$, $1 \leq i \leq d-1$. We need more precise estimates for these coefficients and their $\pi$-adic valuations

**Lemma 1.1.** We have the relations

i) $a_{ni} = \delta_{ni}$ if $0 \leq n \leq d - 1$,

ii) $v(a_{ni}) \geq -\left[\frac{n-1}{d}\right]$ for $n \geq d$ and $i = 1$

iii) $a_{ni} = 0$ for any $n > 0$.

**Proof.** Part i) is trivial, and part ii) is just Lemma 7.7 in [10]. It remains to show part iii); from the discussion above the lemma and the definition of the $a_{ni}$, we get for any $n \geq d$

$$a_{n0} = -\frac{n-d}{\pi} a_{n-d,0} - \sum_{i=1}^{d-1} i a_i a_{i+n-d,0}.$$

Thus $a_{n0} = 0$ from part i), and the result follows recursively.

1.2. **L-functions of exponential sums as characteristic polynomials.** We define the power series $\theta(X) := \exp(\pi X - \pi X^p)$; this is a splitting function in Dwork’s terminology (cf. [9] p55). Its values at the points of $T_1$ are $p$-th roots of unity; in other words this function represents an additive character of order $p$. It is well known that $\theta$ converges for any $x$ in $\mathbb{C}_p$ such that $v_p(x) > -\frac{1}{p^2}$, and in particular $\theta \in \mathcal{H}^1(A)$. We will need the following informations on the coefficients of the power series $\theta$

**Lemma 1.2.** Set $\theta(X) := \sum_{i \geq 0} b_i X^i$; then we have

i) $b_i = \frac{a_i}{\pi}$ if $0 \leq i \leq p - 1$;
\(\text{ii) } v(b_i) \geq i \text{ for } 0 \leq i \leq p^2 - 1; \)
\(\text{iii) } v(b_i) \geq \left(\frac{p-1}{p}\right) i \text{ for } i \geq p^2.\)

We define the functions \(F(X) := \prod_{i=1}^{d} \theta(a_iX^i) := \sum_{n \geq 0} h_nX^n, \) and \(G(X) := \prod_{i=0}^{m-1} F^{\tau^i}(X^{p^i}); \) since \(\theta\) is overconvergent, \(F\) and \(G\) also, and we get \(G \in \mathcal{H}^1(A).\)

Consider the mapping \(\psi_q\) defined on \(\mathcal{H}^1(A)\) by \(\psi_q(f)(x) := \frac{1}{q} \sum_{z \equiv q} f(z);\) if \(f(X) = \sum b_nX^n,\) then \(\psi_q(f)(x) = \sum b_nX^n.\) Let \(\alpha := \psi_q \circ G;\) as operators on \(\mathcal{H}^1(A), D\) and \(\alpha\) commute up to a factor \(q,\) and we get a commutative diagram with exact rows

\[
0 \longrightarrow \mathcal{H}^1(A) \overset{D}{\longrightarrow} \mathcal{H}^1(A) \overset{\alpha}{\longrightarrow} \mathcal{H}^1(A)/D\mathcal{H}^1(A) \longrightarrow 0
\]

Let \(L^*(f, T)\) be the \(L\)-function associated to the sums \(S_r^*(f) := \sum_{x \in k^x} \psi_r(f(x));\)
Dwork’s trace formula (cf [10]) gives the following

\[
L^*(f, T) = \frac{\det(1 - T\alpha)}{\det(1 - qT\alpha)} = \det(1 - T\overline{\alpha}).
\]

We have thus rewritten the \(L\)-function associated to the family of exponential sums as the characteristic polynomial of an endomorphism in a \(p\)-adic vector space.

Let \(\beta\) be the endomorphism of \(\mathcal{H}^1(A)\) defined by \(\beta = \psi_p \circ F;\) then \(\tau^{-1} \circ \beta\) commutes with \(D\) up to a factor \(p,\) and passes to the quotient, giving an endomorphism \(\tau^{-1} \circ \beta\)

Let \(M := Mat\{\overline{\beta}\} \text{ (resp. } N)\) be the matrix of \(\overline{\beta} \text{ (resp. } \overline{\alpha})\) in the basis \(B,\) and \(m_{ij} \text{ (resp. } n_{ij}), 0 \leq i, j \leq d - 1\) be the coefficients of \(M \text{ (resp. } N).\) From the description of \(F,\) we can write \(m_{ij} = h_{pi-j} + \sum_{n \geq d} h_{np-j} a_n\) (cf [10] 7.10). Since we have \(h_0 = 1,\) \(h_n = 0\) for negative \(n,\) we see from Lemma 1.2 iii) that \(m_{00} = 1,\) and \(m_{ij} = 0\) for \(1 \leq j \leq d - 1.\) Since \(N = M^{r-1} \ldots M,\) the same is true for the \(n_{ij};\) thus the space \(W' = \text{Vect}(X, \ldots, X^{d-1})\) is stable under the action of \(\overline{\alpha}, \text{ (resp. } \overline{\beta})\) induces a morphism from \(W'\) to \(W'^r\) and the matrix \(\Gamma\) (resp. \(A\)) defined by \(\Gamma := (m_{ij})_{1 \leq i, j \leq d-1},\) (resp. \(A := (n_{ij})_{1 \leq i, j \leq d-1}\)) is the matrix of the restriction of \(\overline{\beta} \text{ (resp. } \overline{\alpha})\) with respect to the basis \(\{X, \ldots, X^{d-1}\}.\) These matrices satisfy \(A = \Gamma r^{d-1} \ldots \Gamma,\) and \(\det(1 - T\overline{\alpha}) = (1 - T) \det(I_{d-1} - T \Gamma) = (1 - T) \det(I_{d-1} - T T^{r-1} \ldots \Gamma).\) Finally, since we assumed \(f(0) = 0,\) we have \(S_r^*(f) = S_r(f) - 1\) for any \(r \geq 1,\) and \(L^*(f, T) = (1 - T)L(f, T).\) From this we deduce the following result, which we will use to evaluate the valuations of the coefficients of the \(L\)-function associated to \(f.\)

**Proposition 1.1.** Let \(\Gamma\) be as above; then we have

\[
L(f, T) = \det(I_{d-1} - TT^{r-1} \ldots \Gamma).
\]

**Remark 1.1.** We have chosen to work over a ring of overconvergent series, the Washnitzer-Monsky dagger space; one can check that if \(K := \mathcal{K}_m(\gamma)\) is the totally
ramified extension of $K_m$ containing a fixed root of $X^d - \pi$, then the space $W' \otimes K$ with $W'$ as above is isomorphic to the space $H_0(SK_{\ast}(B, D))$ constructed in [1], and under this isomorphism the operator $\alpha$ corresponds to $H_0(\alpha)$ there. Moreover, these spaces are isomorphic to the first rigid cohomology group $H^1_{\text{rig,c}}(k_f/K, f^*\mathcal{L}_0)$ (cf. [2]).

2. CONGRUENCES FOR THE COEFFICIENTS AND THE MINORS OF THE MATRIX $\Gamma$.

In this section, we express the “principal parts” of the coefficients $m_{ij}$ in terms of certain coefficients of the powers of the lifting $g$ of the polynomial $f$. Then we use these results to give the principal parts of the coefficients of the $L$-function.

2.1. The coefficients. Recall that we can express the coefficients $m_{ij}$ from the coefficients $h_n$ of the power series $F$ and the $a_{ni}$ in the following way

$$m_{ij} = h_{ni-j} + \sum_{n \geq d} h_{np-j}a_{ni}.$$

We begin by a congruence on the coefficients of $F$.

**Notation.** Let $P$ be a polynomial; we denote by $\{P\}_n$ its coefficient of degree $n$.

**Lemma 2.1** Assume $p \geq d$, and let $0 \leq n \leq (p-1)d$; then we have the following congruence for the coefficients of the power series $F$

$$h_n = \sum_{k=\lfloor \frac{n}{d} \rfloor}^{p-1} \{g^k\}_n \pi^k n! \left[ \frac{n}{d} \right],$$

where $\lfloor r \rfloor$ is the least integer greater or equal than $r$.

**Proof.** From the definition of $F$, we get

$$h_n = \sum_{m_1+\cdots+md=n} a_1^{m_1} \cdots a_d^{m_d} b_{m_1} \cdots b_{m_d}.$$

Since $m_1 + \cdots + md = n$, we get $d(m_1 + \cdots + md) \geq n$, and $m_1 + \cdots + md \geq \lfloor \frac{n}{d} \rfloor$; on the other hand we clearly have $m_1 + \cdots + md \leq n$, and we write

$$h_n = \sum_{k=\lfloor \frac{n}{d} \rfloor}^{p-1} h_{n,k}, \quad h_{n,k} = \sum_{m_1+\cdots+md=n} a_1^{m_1} \cdots a_d^{m_d} b_{m_1} \cdots b_{m_d}.$$

From Lemma 1.2 ii), since $n < pd \leq p^2$, we have $m_i < p^2$, and $v(b_{m_i}) \geq m_i$; thus $v(h_{n,k}) \geq k$, and $h_n = \sum_{k=\lfloor \frac{n}{d} \rfloor}^{p-1} h_{n,k} \left[ \frac{n}{d} \right]$. Since $k \leq p-1$, the same is true for the $m_i$ appearing in the expression of $h_{n,k}$: from Lemma 1.2 i), we know the $b_{m_i}$ explicitly, and we get

$$h_{n,k} = \sum_{m_1+\cdots+md=n} \frac{a_1^{m_1} \cdots a_d^{m_d}}{m_1! \cdots md!} = \pi^k \sum_{m_1+\cdots+md=n} \binom{k}{m_1, \ldots, m_d} a_1^{m_1} \cdots a_d^{m_d},$$

where $\binom{k}{m_1, \ldots, m_d} := \frac{k!}{m_1! \cdots md!}$ denotes a multinomial coefficient. On the other hand, developing the polynomial $g^k$ yields

$$p^k(X) = \left( \sum_{i=1}^{d} a_i X^i \right)^k = \sum_{m_1+\cdots+md=k} \binom{k}{m_1, \ldots, m_d} a_1^{m_1} \cdots a_d^{m_d} X^{\sum im_i},$$

and we get the result.

We now give a congruence on the coefficients $m_{ij}$ of $\Gamma$.
Proposition 2.1 Assume that $p \geq d + 3$. Let $1 \leq i, j \leq d - 1$; we have 

$$m_{ij} \equiv h_{pi-j} \pmod{p}[π].$$

Proof. From the expression of $m_{ij}$, we are reduced to show that for any $n \geq d$, we have $v(h_{np-j}a_{ni}) \geq p$. Assume first that $n \leq p$; from the expression of $h_n$, we see that the $m_i$ appearing in $h_{np-j}$ are all less than $p^{d-1}$, and we have $v(h_{np-j}) \geq \frac{np-j}{d}$. Let $d \leq n < d + i$; from Lemma 1.1, we have $v(a_{ni}) \geq -\left\lfloor \frac{n-i}{d} \right\rfloor \geq 0$, and $v(h_{np-j}a_{ni}) \geq \frac{np-j}{d} \geq p - 1$. On the other hand, if $n \geq d + i$, $v(a_{ni}) \geq -\left\lfloor \frac{n-i}{d} \right\rfloor \geq \frac{i-n}{d}$, and $v(h_{np-j}a_{ni}) \geq \frac{np-j}{d} + \frac{i-n}{d} = \frac{n(p-1)+i-j}{d} \geq p - 1 + \frac{i(p-1)+i-j}{d} > p - 1$ since $p \geq d$.

Suppose now that $n > p$; in this case we have $v(h_{np-j}) \geq \frac{np-j}{d} \left(\frac{p-1}{p}\right)^2$ (cf [10] Lemma on p242). Thus

$$v(h_{np-j}a_{ni}) \geq \frac{np-j}{d} \left(\frac{p-1}{p}\right)^2 \cdot \frac{n-i}{d} = \frac{n}{d} \left(\frac{(p-1)^2}{p} - 1\right) - \frac{1}{d} \left(\frac{(p-1)^2}{p} j - i\right).$$

We have $\left(\frac{p-1}{p}\right)^2 j - i \leq d$, thus $v(h_{np-j}a_{ni}) \geq \frac{n}{d} \left(\frac{(p-1)^2}{p} - 1\right) - 1$. Since $n > p$, we get $\frac{n}{d} > 1$ and $v(h_{np-j}a_{ni}) > \frac{p^2-3p+1}{d} - 1 > p - 1$ for $p \geq d + 3$.

Corollary 2.1 Assume that $p \geq d + 3$. Let $1 \leq i, j \leq d - 1$; we have

$$m_{ij} \equiv \left\lfloor g^{(\frac{n-i}{d})} \right\rfloor_{pi-j} \pmod{p}[π] \left(\frac{p-1}{p}\right)^{\frac{i-n}{d}} \frac{\pi^k}{k!}.$$

Another consequence of the above evaluations is a congruence on exponential sums associated to polynomials over the prime field: since $S_1(f)$ is the trace of the matrix $Γ$, we deduce from proposition 2.1.

Corollary 2.2 Assume $p \geq d + 3$, and let $f \in F_p[X]$ be a polynomial of degree $d$; then we have the following congruence on the exponential sum $S_1(f)$

$$S_1(f) \equiv \sum_{k=\left\lfloor \frac{n}{d} \right\rfloor}^{p-1} \sum_{i=1}^{d-1} \left\lfloor g^k \right\rfloor_{pi-j} \pmod{p}[π].$$

2.2. The minors. Our aim here is to give estimates for the principal parts of certain minors of the matrix $Γ$. Recall the following expression of a characteristic polynomial

$$\det(I_d - TΓ) = 1 + \sum_{n=1}^{d-1} M_n T^n,$$

where $M_n = \sum_{1 \leq u_1 < \cdots < u_n \leq d-1} \sum_{\sigma \in S_n} \text{sgn}(\sigma) \prod_{i=1}^{n} m_{u_i, u_i(\sigma)}$ is the sum of the $n \times n$ minors centered on the diagonal of $Γ$. We use the results of paragraph 2.1 to give a congruence for the coefficients $M_n$.

Definition 2.1 i) Set $Y_n := \min_{\sigma \in S_n} \sum_{k=1}^{n} \left\lfloor \frac{bk - \sigma(k)}{d} \right\rfloor$, and

$$\Sigma_n := \{\sigma \in S_n, \sum_{k=1}^{n} \left\lfloor \frac{bk - \sigma(k)}{d} \right\rfloor = Y_n\}. $$

ii) For every $1 \leq i \leq d - 1$, set $j_i$ be the least positive integer congruent to $pi$ modulo $d$, and for every $1 \leq n \leq d - 1$, let $B_n := \{1 \leq i \leq n, \ j_i \leq n\}$. 
Note that since $p$ is coprime to $d$, the map $i \mapsto j_i$ is an element of $S_{d-1}$, the $d-1$-th symmetric group. We can use the set $B_n$ to describe $\Sigma_n$ precisely.

**Lemma 2.2.** Let $1 \leq n \leq d-1$; we have $\Sigma_n = \{ \sigma \in S_n, \sigma(i) \geq j_i, \forall i \in B_n \}$, and $Y_n = \sum_{k=1}^{n} \left[ \frac{pk}{d} \right] - \#B_n$.

**Proof.** It is easily seen that for any $1 \leq j \leq j_i - 1$, we have $\left[ \frac{p(j-1)}{d} \right] = \left[ \frac{pj}{d} \right]$, and for $j_i \leq j \leq n$, $\left[ \frac{p(j-1)}{d} \right] = \left[ \frac{p(j)}{d} \right] - 1$. From this we deduce

$$
\sum_{k=1}^{n} \left[ \frac{pk}{d} - \sigma(k) \right] = \sum_{k=1}^{n} \left[ \frac{pk}{d} \right] - \#\{1 \leq k \leq n, \sigma(k) \geq j_k \}.
$$

Now we have the inclusion $\{1 \leq k \leq n, \sigma(k) \geq j_k \} \subset B_n$. Finally the set $\{ \sigma \in S_n, \sigma(i) \geq j_i, \forall i \in B_n \}$ is not empty, since $i \mapsto j_i$ is an injection from $B_n$ into $\{1, \ldots, n\}$; we get $Y_n = \sum_{k=1}^{n} \left[ \frac{pk}{d} \right] - \#B_n$, and that the permutations reaching this minimum are exactly the ones with $\sigma(i) \geq j_i$ for all $i \in B_n$. This is the desired result.

We are now ready to give a congruence for the coefficients $M_n$ of the polynomial $\det(I_{d-1} - TT)$.

**Definition 2.2.** Recall that we have set $g(X) = \sum_{i=1}^{d} a_i X^i$. For any $1 \leq n \leq d-1$ let $P_n$ be the polynomial in $\mathbb{Z}[X_1, \ldots, X_d]$ defined by

$$P_n(a_1, \ldots, a_d) := \sum_{\sigma \in \Sigma_n} \text{sgn}(\sigma) \prod_{i=1}^{n} \left[ g\left( \frac{\sum_{j \neq i} a_j}{d} \right) \right]_{\sigma(i)}.$$ 

**Lemma 2.3** Let $1 \leq u_1 < \cdots < u_n = n + s$ and $1 \leq v_1 < \cdots < v_n = n + t$ be integers; then we have the following inequality

$$
\sum_{k=1}^{n} \left[ \frac{pu_k - v_k}{d} \right] \leq Y_n + \left( \left[ \frac{p}{d} \right] - 1 \right) t - s.
$$

**Proof.** We first rewrite the sum as in the proof of lemma 2.2

$$
\sum_{k=1}^{n} \left[ \frac{pu_k - v_k}{d} \right] = \sum_{k=1}^{n} \left[ \frac{pu_k}{d} \right] - \#\{v_i, v_i \geq j_{u_i} \}.
$$

We know that there are $\#B_n$ integers in $\{1, \ldots, n\}$ such that $j_i \leq n$; thus there are at most $\#B_n + s$ integers in $\{1, \ldots, n\}$ such that $j_i \leq n + s$ since $i \mapsto j_i$ is a bijection. On the other hand, there are at most $t$ elements in $\{n + 1, \ldots, n + t\}$ such that $j_i \leq n + s$; thus the set $\{v_i, v_i \geq j_{u_i} \}$ contains at most $\#B_n + s + t$ elements, and we get

$$
\sum_{k=1}^{n} \left[ \frac{pu_k - v_k}{d} \right] \geq \sum_{k=1}^{n} \left[ \frac{pu_k}{d} \right] - \#B_n - s - t
\geq \sum_{k=1}^{n} \left[ \frac{pu_k}{d} \right] + \left[ \frac{pu_k}{d} \right] - \#B_n - s - t
\geq Y_n + \left( \left[ \frac{p}{d} \right] - 1 \right) t - s.
$$

Now for any $a, b \geq 0$ we have $[a + b] \geq [a] + [b]$, and the sum above is greater than $Y_n + \left[ \frac{p}{d} \right] - t - s$. Moreover, $[ab] \geq [a][b]$, and the sum is greater than $Y_n + \left( \left[ \frac{p}{d} \right] - 1 \right) t - s$. This proves the lemma.

**Proposition 2.2** Assume $p \geq 3d$; then for any $1 \leq n \leq d-1$, we have

$$M_n = \frac{P_n(a_1, \ldots, a_d)}{\prod_{i \in B_n} \left[ \frac{a_i}{d} \right] ! \prod_{i \in B_n} \left( \left[ \frac{a_i}{d} \right] - 1 \right) !} \pi Y_n \left[ \pi Y_{n+1} \right].$$
Lemma 3.1

If the map \( i \mapsto k_{m-1} \) is not injective, we have:

\[
S' := \sum_{\sigma \in S_n} \text{sgn}(\sigma) \prod_{i=1}^{n} m_{k_{m-1}, u_{\sigma(i)}} = 0.
\]
Proof. Assume that \( k_{m-1,i} = k_{m-1,j} \) for some \( i \neq j \). Then \( \sigma \mapsto \sigma' = \sigma \circ (i,j) \) is a bijection from \( A_n \) to \( S_n \setminus A_n \), and we write

\[
S' = \sum_{\sigma \in A_n} \left( \text{sgn}(\sigma) \prod_{l=1}^{n} m_{k_{m-1}u_{\sigma(i)}} + \text{sgn}(\sigma') \prod_{l=1}^{n} m_{k_{m-1}u_{\sigma'(i)}} \right);
\]

Since \( \text{sgn}(\sigma') = -\text{sgn}(\sigma) \), the sum above is zero for any \( \sigma \).

Thus we can write \( k_{m-1,i} = \theta_{m-1}(i) \) for some injective map \( \theta_{m-1} : \{1, \ldots, n\} \to \{1, \ldots, d - 1\} \). Let \( I_n \) be the set of such maps. We get a new expression for \( S \) (where the first sum is taken over \( 1 \leq i \leq m - 2, 1 \leq j \leq n \))

\[
S_U = \sum_{1 \leq k_{ij} \leq d - 1} \sum_{\theta_{m-1} \in I_n} \sum_{\sigma \in S_n} \text{sgn}(\sigma) \prod_{i=1}^{n} m_{k_{ij}u_{\sigma(i)}} \prod_{i=1}^{n} m_{k_{m-1}u_{\sigma(i)}}
\]

Now we show that each of the maps \( \theta_j : i \mapsto k_{ji} \) must be in \( I_n \):

**Lemma 3.2** Assume that the maps \( \theta_j : i \mapsto k_{ji} \) are in \( I_n \) for any \( 1 \leq t < l \leq m - 1 \), but that the map \( i \mapsto k_{ti} \) is not injective; then we have the equality:

\[
S'' := \sum_{(\theta_{t+1}, \ldots, \theta_{m-1}, \sigma) \in I_n^{m-t-1} \times S_n} \text{sgn}(\sigma) \prod_{i=1}^{n} m_{k_{ti}u_{\theta_{t+1}(i)}} \cdots m_{k_{m-1}u_{(i)\sigma(i)}} = 0.
\]

Proof. Assume that \( k_{ti} = k_{tj} \) for \( i \neq j \); consider the disjoint union

\[
I_n^{m-t-1} \times S_n = I_n^{m-t-1} \times A_n \times I_n^{m-t-1} \times S_n \setminus A_n.
\]

The map \( (\theta_{t+1}, \ldots, \theta_{m-1}, \sigma) \mapsto (\theta_{t+1} \circ (i,j), \ldots, \theta_{m-1} \circ (i,j), \sigma \circ (i,j)) \) is a bijection from \( I_n^{m-t-1} \times A_n \) to \( I_n^{m-t-1} \times S_n \setminus A_n \). Since \( k_{ti} = k_{tj} \) and \( \text{sgn}(\sigma) = -\text{sgn}(\sigma \circ (i,j)) \), the terms in \( S'' \) coming from \( (\theta_{t+1}, \ldots, \theta_{m-1}, \sigma) \) and \( (\theta_{t+1} \circ (i,j), \ldots, \theta_{m-1} \circ (i,j), \sigma \circ (i,j)) \) cancel each other and we are done.

Summing up, we get a new expression for \( S_U \)

\[
S_U = \sum_{(\theta_1, \ldots, \theta_{m-1}) \in I_n^{m-1} \times S_n} \text{sgn}(\sigma) \prod_{i=1}^{n} m_{\theta_{i}u_{\theta_{i}(i)}} \cdots m_{\theta_{m-1}u_{\sigma(i)}}.
\]

We are ready to prove the following:

**Proposition 3.1** Assume that \( p \geq 3d \); then for any \( 1 \leq n \leq d - 1 \), we have:

\[
\mathcal{M}_n = \sum_{(\sigma, \theta_1, \ldots, \theta_{m-1}) \in S_n^m} \text{sgn}(\sigma) \prod_{i=1}^{n} m_{\theta_{i}u_{\theta_{i}(i)}} \cdots m_{\theta_{m-1}u_{\sigma(i)}} \left[ \pi^{mY_n + 1} \right].
\]

Proof. Let \( V \) be the valuation of \( m_{\theta_{i}u_{\theta_{i}(i)}} \cdots m_{\theta_{m-1}u_{\sigma(i)}} \); from Corollary 2.1 (note that since \( d \geq 2 \) and \( p \geq 3d \) we have \( p \geq d + 3 \)), we get:

\[
V \geq \sum_{i=1}^{n} \left[ \frac{pu_{i} - \theta_{i}(i)}{d} \right] + \cdots + \left[ \frac{ph_{m-1}(i) - u_{\sigma(i)}}{d} \right]
\]

Assume that \( 1 \leq u_1 < \cdots < u_n = n + t_0 \), and \( 1 \leq \theta_{i}(1) < \cdots < \theta_{i}(n) = n + t_i \), \( 1 \leq i \leq m - 1 \); then we have from lemma 2.3

\[
V \geq Y_n + \left( \left[ \frac{d}{p} \right] - 1 \right) t_0 - t_1 + \cdots + y_n + \left( \left[ \frac{d}{p} \right] - 1 \right) t_{m-1} - t_0
\]

Assume that one of the \( t_i \) is nonzero; from the hypothesis on \( p \), we have \( V \geq mY_n + 1 \), and this term doesn’t appear in the congruence. Thus the only terms remaining
are those with \( \{u_1, \ldots, u_n\} \), \( \theta_i(\{1, \ldots, n\}) \) all equal to \( \{1, \ldots, n\} \), and this is the desired result.

We are now ready to show the main result of this section; we use the notations of section 2:

**Proposition 3.2** Assume that \( p \geq 3d; \) then for any \( 1 \leq n \leq d - 1 \), we have the congruence:

\[
\mathcal{M}_n \equiv \frac{N_{K_m/Q_p}(P_n(a_1, \ldots, a_d))}{(\prod_{i \not\in B_n} q^{-m}) \prod_{i \in B_n} ((q^m) - 1)!} \mathfrak{m}^{mY_n}[\pi^mY_{n+1}].
\]

**Proof.** We rewrite the sum in proposition 3.1: set \( \sigma_0 = \theta_1, \sigma_1 = \theta_2 \circ \theta_1^{-1}, \ldots, \sigma_{m-1} = \sigma \circ \theta_{m-1}^{-1}; \) we get

\[
\mathcal{M}_n \equiv \sum_{(\sigma_0, \ldots, \sigma_{m-1}) \in S_n^m} \text{sgn}(\sigma_0 \circ \cdots \circ \sigma_{m-1}) \prod_{i=1}^n m^{m_{i\sigma_0(i)} - m_{i\sigma_1(i)}} \cdots m^{m_{i\sigma_{m-1}(i)}} [\pi^mY_{n+1}]
\]

\[
\equiv \prod_{i=0}^{m-1} \sum_{\sigma_i \in S_n} \text{sgn}(\sigma_i) \prod_{j=1}^n m^{m_{j\sigma_i(j)}} = \prod_{i=0}^{m-1} \left( \sum_{\sigma_i \in S_n} \text{sgn}(\sigma_i) \prod_{j=1}^n m^{m_{j\sigma_i(j)}} \right)^\tau [\pi^mY_{n+1}].
\]

Finally we know from Proposition 2.2 that

\[
\left( \sum_{\sigma \in \Sigma_n} \text{sgn}(\sigma) \prod_{j=1}^n m_{j\sigma(j)} \right)^\tau \equiv \frac{\prod_{i \in B_n} q^{-m}[\pi]! \prod_{i \not\in B_n} ((q^m) - 1)!} {\prod_{i \not\in B_n} q^{-m}[\pi]! \prod_{i \not\in B_n} ((q^m) - 1)!} \mathfrak{m}^{mY_n}[\pi^mY_{n+1}],
\]

and the theorem is an immediate consequence of the congruences above.

### 4. Generic Newton polygons

In this section we use the results above to determine the generic Newton polygon \( GNP(d, q) \) associated to polynomials of degree \( d \) over \( \mathbb{F}_q \). We determine the Zariski dense open subset \( U \) in \( \mathbb{A}^{d-1} \), the space of monic polynomials of degree \( d \) without constant coefficient, such that for any \( f \in U \) we have \( N_{p}(f, \mathbb{F}_q) = GNP(d, q) \), giving an explicit polynomial, the Hasse polynomial \( G_{d,p} \) in \( \mathbb{F}_p[X_1, \ldots, X_d] \) such that \( U = D(G_{d,p}) \).

#### 4.1. Hasse polynomials

In this section, we study the polynomials which appear when expressing the principal parts of the minors \( M_n \) in terms of the coefficients of the original polynomial.

**Definition 4.1.** Recall that for \( g(X) = \sum_{i=1}^d a_iX^i \), we have set

\[
P_n(a_1, \ldots, a_d) := \sum_{\sigma \in \Sigma_n} \text{sgn}(\sigma) \prod_{i=1}^n \left( g^\frac{\tau_{\sigma^i(i)}}{d} \right)^{\pi_{\sigma(i)}}.
\]

We denote by \( P_n \in \mathbb{F}_p[X_1, \ldots, X_d] \) the reduction modulo \( p \) of \( P_n \), and let \( P_{d,p} := \prod_{i=1}^d P_i \).

Our next task is to ensure that the polynomial \( P_{d,p} \) is non zero; in order to prove this, we consider the monomials in \( P_{d,p} \) of minimal degree and exhibit one that appear (with non zero coefficient) exactly once when \( \sigma \) describes \( \Sigma_n \).

**Lemma 4.1** For any \( 1 \leq n \leq d - 1 \), we have \( P_n \neq 0 \) in \( \mathbb{F}_p[X_1, \ldots, X_d] \). Moreover this polynomial is homogeneous of degree \( Y_n \).
Proof. The polynomial \((a_1, \ldots, a_d) \mapsto \left\{ g_{\bar{m}-\sigma(i)} \right\}_{\bar{m}-\sigma(i)} \) contains a unique monomial of maximal degree in \(X_d\), which is \(X_d \left\{ g_{\bar{m}-\sigma(i)} \right\}_{\bar{m}-\sigma(i)} \), where \(\bar{m}\) stands for the least nonnegative integer congruent to \(n\) modulo \(d\), and we set \(X_0 = 1\). Moreover it's coefficient is 1 if \(\bar{m} - \sigma(i) = 0\), and \(\left\{ g_{\bar{m}-\sigma(i)} \right\}\) else: in any case it is non zero modulo \(p\). Thus \(\prod_{i=1}^{n} \left\{ g_{\bar{m}-\sigma(i)} \right\}_{\bar{m}-\sigma(i)} \) contains a unique monomial of maximal degree in \(X_d\) with nonzero coefficient, which is \(X_d^{\sum_{i=1}^{n} \left\{ \frac{\bar{m}-\sigma(i)}{d} \right\}} \prod_{i=1}^{n} X_{\bar{m}-\sigma(i)}\).

On the other hand, we have \(\left\{ \frac{\bar{m} - j}{d} \right\} = \left\{ \frac{\bar{m}}{d} \right\}\) if \(1 \leq j \leq j_i\), and \(\left\{ \frac{\bar{m} - j}{d} \right\} = \left\{ \frac{\bar{m}}{d} \right\} - 1\) if \(j \geq j_i + 1\). Thus the degree in \(X_d\) of a monomial of \(P_n\) is maximal for those \(\sigma\) such that \(\sigma(i) \leq j_i\). From Lemma 2.2, we see that the monomials in \(P_n\) of maximal degree in \(X_d\) come from the \(\sigma\) such that for any \(i \in B_n\), \(\sigma(i) = j_i\) (note that such \(\sigma\) exist since \(i \mapsto j_i\) is injective on \(B_n\)). If \(\Sigma^+ \subset \Sigma\) is the set of these permutations, we get that the monomials in \(P_n\) of maximal degree in \(X_d\) are the

\[
X_d^{\sum_{i=1}^{n} \left\{ \frac{\bar{m}}{d} \right\}} \prod_{i \notin B_n} X_{\bar{m}-\sigma(i)} = X_d^{\sum_{i=1}^{n} \left\{ \frac{\bar{m}}{d} \right\}} \prod_{i \notin B_n} X_{j_i - \sigma(i)},
\]

with \(\sigma \in \Sigma^+\), and that there is exactly \#\(\Sigma^+\) such monomials in \(P_n\) (remind that for \(i \notin B_n\), \(\sigma \in \Sigma^+\), we have \(\bar{m} = j_i > n\), and \(\bar{m} - \sigma(i) = j_i - \sigma(i)\)).

We now construct \(\sigma_0 \in \Sigma^+\) such that the associated monomial cannot be obtained from any other \(\sigma \in \Sigma^+\). For \(i \in B_n\), we must have \(\sigma_0(i) = j_i\) from the definition of \(\Sigma^+\). Let \(i_0 \in \{1, \ldots, n\} \setminus B_n\) be such that \(j_{i_0}\) is maximal, and set \(\sigma_0(i_0) = \min \{\{1, \ldots, n\} \setminus \{j, i \in B_n\}\}\). Then we continue the same process, with \(i_1 \neq i_0\), \(i_1 \notin B_n\) such that \(j_{i_1}\) is maximal, and \(\sigma_0(i_1)\) minimal among the remaining possible images. The permutation \(\sigma_0\) is clearly well defined, and unique. Let \(\sigma \in \Sigma^+\) be such that \(\prod_{i \notin B_n} X_{j_i - \sigma(i)} = \prod_{i \notin B_n} X_{j_i - \sigma_0(i)}\). Consequently here exists \(i \notin B_n\) such that \(j_i - \sigma(i) = j_{i_0} - \sigma_0(i_0)\); from the construction we must have \(j_i = j_{i_0}\), thus \(i = i_0\), and \(\sigma(i_0) = \sigma_0(i_0)\). Following this process, we get \(\sigma = \sigma_0\). Finally the monomial \(X_d^{\sum_{i=1}^{n} \left\{ \frac{\bar{m}}{d} \right\}} \prod_{i \notin B_n} X_{j_i - \sigma_0(i)}\) appears just once in \(P_n\), with coefficient \(\prod_{i \notin B_n} \left\{ \frac{\bar{m} - \sigma_0(i)}{d} \right\}\) and this gives the first assertion.

To prove the second assertion, remark that from the proof of Lemma 2.1, \((a_1, \ldots, a_d) \mapsto \left\{ g_{\bar{m}-\sigma(i)} \right\}_{\bar{m}-\sigma(i)}\) is homogeneous of degree \(\left\{ \frac{\bar{m} - \sigma(i)}{d} \right\}\); thus from the definition of \(\Sigma_n\), we get the result.

Lemma 4.2 i) We have \(P_{d,p}(X_1, \ldots, X_{d-1}, 1) \neq 0\) in \(\mathbb{F}_p[X_1, \ldots, X_{d-1}]\). Moreover this polynomial has degree less or equal than \(\frac{d-1}{2}\) \(\left\lceil \frac{d}{2} \right\rceil \left( \frac{d}{2} + 1 \right)\); ii) we have \(P_{d,p}(X_1, \ldots, X_{d-2}, 0, 1) \neq 0\) in \(\mathbb{F}_p[X_1, \ldots, X_{d-1}]\). Moreover this polynomial has degree less or equal than \(\frac{d-1}{2}\) \(\left\lceil \frac{d}{2} \right\rceil \left( \frac{d}{2} + 1 \right)\).

Proof. i) The non vanishing is obvious from Lemma 4.1, since dehomogenizing a non zero homogeneous polynomial with respect to any of its variables yields a non zero polynomial.

We now show the assertion on the degree; consider the polynomial \((a_1, \ldots, a_d) \mapsto \left\{ g_{\bar{m}} \right\}_{\bar{m}}\). From the proof of Lemma 2.1, its monomials are among the \(X_1^{m_1} \ldots X_d^{m_d}\) with \(m_1 + \cdots + dm_d = k\), and \(m_1 + \cdots + m_d = \left\lfloor k \right\rfloor\). Multiplying the second equality by \(d\) and substracting the first we get \((d-1)m_1 + \cdots + m_{d-1} = d\left\lfloor \frac{k}{d} \right\rfloor - k \leq d - 1\); consequently \(m_1 + \cdots + m_{d-1} \leq d - 1\), and the degree in \(X_1, \ldots, X_{d-1}\) of the above polynomial is at most \(d - 1\). From the definition of \(P_n\), its degree in the first \(d - 1\)
variables is at most \( n(d - 1) \), and finally the degree of \( P_{d,p}(X_1, \ldots, X_{d-1}, 1) \) is at most \( \frac{d-1}{2} \left( \left\lfloor \frac{d}{2} \right\rfloor + 1 \right) \).

\( \text{ii) } \) The non vanishing follows from the proof of Lemma 4.1. Remark that from the construction of \( \sigma_0 \), we must have, for \( i \notin B_n, j_i - \sigma_0(i) \leq d - 2 \); thus the monomial constructed in the proof doesn’t contain \( X_{d-1} \), and the result follows. In order to give a bound for the degree, we use the same technique that in the proof of \( i \), remarking that now we take \( m_{d-1} = 0 \), and consequently \( m_1 + \cdots + m_{d-1} \leq \frac{d^2}{12} \).

This ends the proof.

**Definition 4.2.** We define the Hasse polynomial for polynomials of degree \( d \) \( G_{d,p} \) in \( \mathbb{F}_q[X_1, \ldots, X_{d-1}] \) as

\[
G_{d,p}(X_1, \ldots, X_{d-1}) := P_{d,p}(X_1, \ldots, X_{d-1}, 1),
\]

and the Hasse polynomial for normalized polynomials of degree \( d \), \( H_{d,p} \) in \( \mathbb{F}_q[X_1, \ldots, X_{d-2}] \) as

\[
H_{d,p}(X_1, \ldots, X_{d-2}) := P_{d,p}(X_1, \ldots, X_{d-2}, 0, 1),
\]

### 4.2. The generic Newton polygon

We use the results of the paragraph above to show that for any monic polynomial of degree \( d \) over \( \mathbb{F}_q \), its Newton polygon is above a generic Newton polygon, and that most polynomials have their Newton polygon attaining the generic Newton polygon.

We identify the set of normalized monic polynomials of degree \( d \) such that \( f(0) = 0 \) with affine \( d - 2 \) space \( \mathbb{A}^{d-2} \) by associating the point \((a_1, \ldots, a_{d-2})\) to the polynomial \( f(X) = X^d + a_1X^{d-1} + \cdots + a_{d-2}X + a_1X \).

**Definition 4.3.** Set \( Y_0 := 0 \). We define the generic Newton polygon of exponential sums associated to polynomials of degree \( d \) in \( \mathbb{F}_q, \text{GNP}(d, \mathbb{F}_q) \), as the lowest convex hull of the points

\[
\left\{ \left( n, \frac{Y_n}{p-1} \right) \right\}_{0 \leq n \leq d-1}.
\]

We are ready to prove the main result of this paper.

**Theorem 4.1.** Let \( p \geq 3d \) be a prime, and \( f \in \mathbb{F}_q[X] \) a normalized polynomial of degree \( d \). Then we have \( \text{NP}_q(f, \mathbb{F}_q) = \text{GNP}(d, q) \) if and only if the coefficients of \( f \) belong to the Zariski dense open subset \( U := D(H_{p,d}) \). Moreover for any polynomial of degree \( d \) over \( \mathbb{F}_q \), the associated Newton polygon is above the generic Newton polygon.

**Proof.** Recall from Proposition 1.1 that for any polynomial of degree \( d \) we have

\[
L(f, T) = \det(I_{d-1} - TT^{m-1} \cdots I) = \sum_{n=0}^{d-1} \mathcal{M}_n T^n.
\]

Thus the Newton polygon \( \text{NP}_q(f, \mathbb{F}_q) \) is the lower convex hull of the set of points

\[
\{(n, v_q(\mathcal{M}_n)), 0 \leq n \leq d - 1\}.
\]

On the other hand we have, from Proposition 3.2

\[
\mathcal{M}_n = \frac{N_{k,m/\mathbb{Q}_p}(\bar{P}_n(a_1, \ldots, a_d))}{(\prod_{i \in B_n} \left\lfloor \frac{a_i}{d} \right\rfloor ! \prod_{i \notin B_n} \left\lfloor \frac{a_i}{d} \right\rfloor !^{-1})} \pi^m Y_n \left[ \pi^m Y_{n+1} \right].
\]

and we get \( v_q(\mathcal{M}_n) = \frac{Y_n}{p-1} \) if and only if \( P_n(a_1, \ldots, a_{d-2}, 0, 1) \neq 0 \) in \( \mathbb{F}_q \). Moreover, the Newton polygon is symmetric: if it has a slope of length \( l \) and slope \( s \) it has a segment of the same length and slope \( 1 - s \). Thus, in order to show that \( \text{NP}_q(f, \mathbb{F}_q) \) coincides with \( \text{GNP}(d, q) \), it is sufficient to show that the first \( \left\lfloor \frac{d}{2} \right\rfloor \) vertices of \( \text{NP}_q(f, \mathbb{F}_q) \) coincide with the ones of \( \text{GNP}(d, q) \). From Definition 4.1,
this is true exactly when $P_{d,p}(\alpha_1, \ldots, \alpha_{d-2}, 0, 1) \neq 0$; this is the desired result. The last assertion is an easy consequence of the discussion above.

**Remark 4.1.** Let us show that we have $NP(f) = HP(d)$ for any $f$ of degree $d$ when $p \equiv 1 \mod d$; in this case we get $\Sigma_n = \{Id\}$ for any $n$, $Y_n = (p-1)^{n(n+1)/2}$, and $GNP(d, q) = HP(d)$; moreover $P_n(X_1, \ldots, X_d) = cX_d^{Y_n}$, for some $c \in F_p^\times$, and $H_{d,p}$ is a nonzero polynomial of degree 0. In this case we get that $U_{d,p}$ is the whole $A^{d-2}$, as stated above.

**References**

[1] A. Adolphson, S. Sperber, Exponential sums and Newton polyhedra: cohomology and estimates, Ann. Math. 130 (1989), 367-406.
[2] P. Bourgeois, Annulation et pureté des groupes de cohomologie rigide associés à des sommes exponentielles, C. R. Acad. Sci. Paris 328 (1999), 681-686.
[3] B. Dwork, On the zeta function of an hypersurface, Publ. Math. I.H.E.S. 12 (1962), 5-68.
[4] Y. Etesse, B. Le Stum, Fonctions $L$ associées aux $F$-isocristaux surconvergents I, Math. Ann. 296 (1993), 557-576.
[5] A. Grothendieck, Groupes de Barsotti-Tate et cristaux de Dieudonné, Séminaire de mathématiques supérieures, Université de Montréal, Les presses de l'université de Montréal, 1974.
[6] S. Hong, Newton polygons of $L$-functions associated with exponential sums of polynomials of degree four over finite fields, Finite Fields and Applications 7 (2001), 205-237.
[7] S. Hong, Newton polygons for $L$-functions of exponential sums of polynomials of degree six over finite fields, Journal of Number Theory 97 (2002), 368-396.
[8] N. Katz, Slope filtration of $F$-crystals, Astérisque 63 (1979), 113-164.
[9] N. Koblitz, $p$-adic numbers, $p$-adic analysis and zeta functions, GTM 58, Springer-Verlag 1984.
[10] P. Robba, Index of $p$-adic differential operators III. Application to twisted exponential sums. Astérisque 119-120 (1984), 191-266.
[11] J. Scholten, H. J. Zhu, First slope case of Wan’s conjecture, Finite Fields and Applications 8 (2002), 414-419.
[12] S. Sperber, On the $p$-adic theory of exponential sums, Amer. J. Math. 109 (1986), 255-296.
[13] D. Wan, Variation of $p$-adic Newton polygons for $L$-functions of exponential sums, Asian J. Math. 8 (2004), 427-474.
[14] H. J. Zhu, $p$-adic variation of $L$-functions of one variable exponential sums, I. American Journal of Mathematics 125 (2003), 669-690.
[15] H. J. Zhu, Asymptotic variation of $L$-functions of one-variable exponential sums, J. Reine Angew. Math., 572 (2004), 219-233.