NEAL KOBLITZ

p-adic variation of the zeta-function over families of varieties defined over finite fields

Compositio Mathematica, tome 31, nº 2 (1975), p. 119-218
<http://www.numdam.org/item?id=CM_1975__31_2_119_0>

COMPOSITIO MATHEMATICA, Vol. 31, Fasc. 2, 1975, pag. 119–218
Noordhoff International Publishing
Printed in the Netherlands

P-ADIC VARIATION OF THE ZETA-FUNCTION OVER FAMILIES OF VARIETIES DEFINED OVER FINITE FIELDS

Neal Koblitz

Table of contents

Introduction

Let X be a scheme of finite type over a finite field $\mathbb{F}_q$ with $q = p^a$ elements. Let $N_s = \# X(\mathbb{F}_{q^s})$ be the number of $\mathbb{F}_{q^s}$-rational points on X. The p-adic study of the N_s is the outgrowth of the classical results of Warning and Ax on p-divisibility of the number of solutions of equations over finite fields.

PROPOSITION (Warning [60]): *Let $F(X_1, \ldots, X_n) \in \mathbb{Z}[X_1, \ldots, X_n]$ be a polynomial of degree $d < n$. Then the number of solutions of*

$$F(X_1, \ldots, X_n) \equiv 0 \pmod{p}$$

is divisible by p.

PROPOSITION (Ax [2]): *Let $F(X_1, \ldots, X_n) \in \mathbb{Z}[X_1, \ldots, X_n]$ be a polynomial of degree d. Let μ be the least nonnegative integer such that*

$$\mu \geqq \frac{n-d}{d}.$$

Let N be the number of solutions of

$$F(X_1, \ldots, X_n) = 0$$

in $(\mathbb{F}_q)^n$. Then

$$N \equiv 0 \pmod{q^\mu}.$$

All the information about the $N_s = \# X(\mathbb{F}_{q^s})$ is contained in the zeta-function

$$Z(X/\mathbb{F}_q; t) = \exp\left(\sum_{s=1}^{\infty} N_s t^s/s\right)$$

of X over $\mathbb{F}_q$, which Dwork [10] proved to be a rational function. For example:

PROPOSITION (Ax [2]): *Let X be a scheme of finite type over $\mathbb{F}_q$, and let μ be a positive integer. Then the following are equivalent:*

(i) *the reciprocal of every zero and pole of $Z(X/\mathbb{F}_q; t)$ is of the form q^μ (an algebraic integer);*

(ii) $N_s \equiv 0 \pmod{q^{s\mu}}$ *for all* $s \geqq 1$;
(iii) $Z(X/\mathbb{F}_q; t) \in \mathbb{Z}[[q^\mu t]]$.

Now suppose that X is proper and smooth, $\dim X = n$. Given any 'Weil cohomology' H^* in the sense of [29], the zeta-function is expressed as an alternating product of the characteristic polynomials of the action of the pth-power 'Frobenius' endomorphism F:

$$Z(X/\mathbb{F}_q; t) = \prod_i \det (1 - tF^a | H^i(X))^{(-1)^{i+1}}.$$

In the proper and smooth case, the zeta-function has certain basic properties, which were conjectured by Weil in 1949 and proved in the following form by Grothendieck (i), (ii), (iii) and Deligne (iv):

(i) For any prime $l \neq p$, we have

$$Z(X/\mathbb{F}_q; t) = \frac{P_1(t)P_3(t)\dots P_{2n-1}(t)}{P_0(t)P_2(t)\dots P_{2n}(t)},$$

where

$$P_i(t) = \prod_{j=1}^{b_i} (1 - \alpha_{ij} t) \in 1 + t\mathbb{Z}_l[t].$$

(ii) If X is obtained by reduction from a proper smooth scheme defined in characteristic 0, then $b_i = \deg P_i$ is the i-th topological Betti number of X.

(iii) (Functional Equation)

$$Z\left(X/\mathbb{F}_q; \frac{1}{q^n t}\right) = \pm t^\chi q^{n\chi/2} Z(X/\mathbb{F}_q; t), \qquad \text{where} \quad \chi = \sum (-1)^i b_i;$$

thus, if α_{ij} is a reciprocal root or pole, then so is q^n/α_{ij}.

(iv) The P_i in (i) are independent of l; $P_i(t) \in 1 + t\mathbb{Z}[t]$, i.e., the α_{ij} are algebraic integers; and

$$\text{(Riemann Hypothesis)} \ |\alpha_{ij}|_{\text{complex}} = q^{i/2}.$$

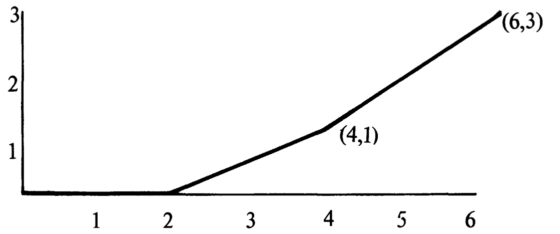
Note that the functional equation implies that all the α_{ij} are l-adic units for all primes $l \neq p$, because both α_{ij} and q^n/α_{ij} are algebraic integers. Thus, there remains the question of the p-adic ordinals of the α_{ij}. As mentioned above, in classical terms these p-adic ordinals correspond to p-divisibility properties of the N_s.

In the cases considered in this paper there is only one 'interesting' polynomial P_i in $Z(X/\mathbb{F}_q; t)$. If X is a complete intersection this is the polynomial P_n, corresponding to middle dimensional cohomology. If X is an abelian variety it is P_1, corresponding to $H^1(X)$. In such a case the p-adic picture of the zeta-function is given by the 'Newton polygon' of P_n (resp. P_1). The Newton polygon of a polynomial

$$P(t) = \sum_{i=0}^{b} a_i t^i \in 1 + t\mathbb{Z}[t]$$

is defined as the convex hull of the points $(i, v_q(a_i))$, $i = 0, \ldots, b$, where v_q is the p-adic valuation normalized so that $v_q(q) = 1$.

The 'unit root' part of the Newton polygon is the segment with zero slope. Its length equals the number of p-adic unit reciprocal roots of P. In general, the horizontal length of a segment of slope a/b equals the number of reciprocal roots of P having $v_q = a/b$. In the case of the zeta-function of a complete intersection or an abelian variety, the functional equation imposes the following symmetry on the Newton polygon: $0 \leqq a/b \leqq n$, and the segments of slope a/b and $n-(a/b)$ have the same length. Here is a typical Newton polygon (here $n = 1$, $b = 6$, i.e., X is a curve of genus 3):



A second constraint on the Newton polygon is that its vertices are integral lattice points, i.e., the number of roots with $v_q = c$ is a multiple of the denominator of c (cf. Manin, [34], Theorem 4.1, or Katz, [27], Theorem 2).

A third constraint is imposed by the following special case of a theorem of Mazur [36] (the 'Katz conjecture'):

Proposition: *Let $X/\mathbb{F}_q$ be a projective smooth complete intersection of dimension n. Then the Newton polygon of P_n lies on or above the Newton polygon of*

$$\prod_{i=0}^{n} (1-q^i t)^{h_0^{i,n-i}}, \qquad \text{where } h_0^{i,n-i} = \dim_{\mathbb{F}_q} H^{n-i}(X, \Omega^i_{X/\mathbb{F}_q}) - \delta_{i,n-i}.$$

It turns out that the unit root part of P_n is most easily studied, thanks to the Katz congruence formula [21]:

$$Z(X/\mathbb{F}_q; t) \equiv \prod_{i=0}^{n} \det (1-tF^a|H^i(X, \mathcal{O}_X))^{(-1)^{i+1}} \qquad (\text{mod } p),$$

where $H^i(X, \mathcal{O}_X)$ is the Čech cohomology of X with coefficients in the structure sheaf (abbreviated $H^i(\mathcal{O}_X)$ from now on), and F is the Frobenius, the 'p-linear' vector space map induced by $f \mapsto f^p$ on the structure sheaf ('p-linear' means $F(af+bg) = a^p F(f) + b^p F(g)$). Thus, the unit root part of the Newton polygon of P_n corresponds to the 'semisimple' part of the vector space $H^n(\mathcal{O}_X)$ under the action of the p-linear map F. (Recall that two exact functors are defined on the category of pairs (V, F), where V is a k-vector space, k a field of characteristic p, and F is a p-linear endomorphism:

$$\text{'nilpotent part':} \qquad V \rightsquigarrow V_{\text{nilp}} = \bigcup_{n=1}^{\infty} \ker (F^n|V),$$

$$\text{'semisimple part':} \qquad V \rightsquigarrow V_{\text{ss}} = \bigcap_{n=1}^{\infty} \text{span of im } (F^n|V).$$

When k is a perfect field, we have $V = V_{\text{nilp}} \oplus V_{\text{ss}}$ with F nilpotent on V_{nilp} and bijective on V_{ss}, and $\dim (V_{\text{ss}})$ is called the 'stable rank' of F.) The action of F on $H^n(\mathcal{O}_X)$ is classically known as the Hasse-Witt matrix (see, e.g., [32]). Thus, the number of p-adic unit reciprocal roots of P_n is equal to the stable rank $r(X)$ of the Hasse-Witt matrix.

The following questions will be investigated in this paper:

(1) As X varies over certain families (hypersurfaces of given dimension and degree, complete intersections of given dimension and multidegree, curves of given genus), does $r(X)$ generically attain the maximal possible value $p_g(X) = h_0^{0,n} = \dim H^n(\mathcal{O}_X)$?

(2) If $X \subset \mathbb{P}^N$ is fixed and H is a varying hypersurface of degree d, then how does the generic value of $r(X \cdot H)$ compare with $p_g(X \cdot H)$, especially as $d \to \infty$? When does X satisfy the 'invertibility conjecture' of Grothendieck-Miller, which asserts that generically $r(X \cdot H) = p_g(X \cdot H)$ if $d \gg 0$?

In answering questions (1) and (2), an essential role is played by the convenient fact that the Katz congruence formula expresses the unit root part as a *coherent cohomology* phenomenon.

(3) How are various moduli spaces (principally polarized abelian varieties, genus g curves) stratified by the stable rank r?

(4) What can be said about the refinement of this stratification according to the entire Newton polygon?

I wish to thank Professors B. Dwork, P. Deligne, B. Mazur, W. Messing, D. Mumford, and A. Ogus for many valuable discussions, ideas, and corrections. I am especially grateful to my adviser, Professor Nicholas M. Katz, for suggesting the problem and giving me constant help throughout my work on the subject.

I. Generic invertibility of the Hasse-Witt matrix

1. *Hypersurface sections and their Hasse-Witt*

Let $X \subset \mathbb{P}_k^N$, where $k = \mathbb{F}_q$, be an arbitrary n-dimensional closed subscheme, corresponding to a homogeneous ideal $I \subset k[X_0, \ldots, X_n]$. Let $\bar{k}$ be an algebraic closure of k, and let $\bar{X} = X x_k \bar{k}$, $\bar{I} = I \otimes_k \bar{k}$, $\bar{\mathbb{P}}^N = \mathbb{P}_{\bar{k}}^N$. Let $S_d \approx \bar{\mathbb{P}}^v$, where $v = v_{N,d} = \binom{N+d}{N} - 1$, be the projective space of hypersurfaces H of degree d in $\bar{\mathbb{P}}^N$. Let S_d have homogeneous coordinates $(Y_0, \ldots, Y_v)$.

We are interested in hypersurfaces H whose equation h is not a zero divisor in $\mathcal{O}_{\bar{X}}$, i.e., for which no irreducible component of $\bar{X}$ has h vanishing at all of its points. Such H are said to 'intersect properly' with $\bar{X}$. In terms of ideals, this means we want to eliminate from S_d those h contained in any of the associated primes P_i of $\bar{I}$ (i.e., the minimal primes, corresponding to maximal points of $\bar{X}$; we have $\bar{I} = \bigcap P_i^{m_i}$). Take some $P \in \{P_i\}$ having homogeneous generators $g_u \in \bar{k}[X_0, \ldots, X_N]$ of degrees d_u, respectively. We first replace $\{g_u\}$ by $\{h_j\}_{j=0}^m$, where the h_j run through all products of the g_u with monomials of degree $d - d_u$, and we leave out a g_u if $d_u > d$. Then $h \in P$ if and only if there exist $a_0, \ldots, a_m \in \bar{k}$ such that $h = \sum_{j=0}^m a_j h_j$. That is, we want to eliminate from S_d the image of the morphism

$$\bar{\mathbb{P}}^m \to S_d$$

given on closed points by

$$(a_0, \ldots, a_m) \mapsto \text{hypersurface with equation } \sum a_j h_j.$$

This image is closed. Moreover, it does not contain all of S_d: take a point $x \in \bar{X}$ in the component corresponding to the prime ideal P, and take the point in S_d corresponding to a hypersurface H which does not contain x; then, since all the h_j vanish at x, it follows that the equation of H is *not* of the form $\sum a_j h_j$. Thus, let $Y \subset S_d$ be the nonempty Zariski open set consisting of hypersurfaces which intersect properly with $\bar{X}$.

Recall that the Hasse-Witt matrix of an n-dimensional variety X is defined as the action of the Frobenius F on $H^n(\mathcal{O}_X)$. However, when considering high degree hypersurface sections $\bar{X} \cdot H$ of a fixed variety X, we modify the definition of the Hasse-Witt of the section as follows. Under a mild assumption on X which we shall always make – namely, the Cohen-Macaulay condition – it will follow that the restriction

$$\mathcal{O}_{\bar{X}} \xrightarrow{j} \mathcal{O}_{\bar{X} \cdot H}$$

induces

$$\begin{cases} j^* : H^i(\mathcal{O}_{\bar{X}}) \xrightarrow{\sim} H^i(\mathcal{O}_{\bar{X} \cdot H}), & i < n-1 \\ j^* : H^{n-1}(\mathcal{O}_{\bar{X}}) \hookrightarrow H^{n-1}(\mathcal{O}_{\bar{X} \cdot H}). \end{cases}$$

So if F fails to act bijectively on $H^{n-1}(\mathcal{O}_{\bar{X}})$, then it also fails to act bijectively on $H^{n-1}(\mathcal{O}_{\bar{X} \cdot H})$, which is the middle dimensional cohomology of the $(n-1)$-dimensional variety $\bar{X} \cdot H$, *for any* H. Hence, if we are to have any hope of generic invertibility for high degree sections, we must consider only the 'truly variable' part of $H^*(\mathcal{O}_{\bar{X} \cdot H})$ and define the Hasse-Witt of a hypersurface section of any fixed variety X as the action of F on

$$H^{n-1}(\mathcal{O}_{\bar{X} \cdot H})/j^*(H^{n-1}(\mathcal{O}_{\bar{X}})).$$

Note that for high degree sections $\bar{X} \cdot H$ the map

$$j^* : H^{n-1}(\mathcal{O}_{\bar{X}}) \hookrightarrow H^{n-1}(\mathcal{O}_{\bar{X} \cdot H})$$

is far from surjective, since, as we shall see, dim $H^{n-1}(\mathcal{O}_{\bar{X} \cdot H})$ grows with order $D \cdot d^n/n!$, where D is the 'degree' of $\bar{X}$ (i.e., the number of intersection points with the intersection of n hyperplanes in general position).

Katz [23] proved that, for a fixed Cohen-Macaulay variety X and for generic H of degree $d \gg 0$, the Hasse-Witt matrix of $\bar{X} \cdot H$ has positive stable rank, i.e.,

$$\dim_{\bar{k}} (H^{n-1}(\mathcal{O}_{\bar{X} \cdot H})/j^* H^{n-1}(\mathcal{O}_{\bar{X}}))_{ss} > 0$$

– in other words, the action of F is not nilpotent – and he conjectured that much stronger estimates are possible.

2. *Flatness and base-changing*

We first need a few lemmas. The first lemma asserts the flatness and properness of the families of varieties that are the primary concern of this chapter.

(1) Let $Y_1 = Y \subset S_d$ be the moduli space of hypersurfaces in $\bar{\mathbb{P}}^N$ which intersect properly with a fixed variety $\bar{X} \subset \bar{\mathbb{P}}^N$. Let

$$h \in \bar{k}[X_0, \ldots, X_N, Y_0, \ldots, Y_v]$$

be the 'generic' form of degree d in $\bar{k}[X_0, \ldots, X_N]$ whose coefficient of the i-th monomial term ($i = 0, 1, \ldots, \binom{N+d}{N}-1$) is the corresponding Y_i. Now h defines a hypersurface H in $\bar{\mathbb{P}}^N \times S_d \approx \bar{\mathbb{P}}^N \times \bar{\mathbb{P}}^v$, since it is homogeneous of degree d in the first set of variables and degree 1 in the second set. Let $M_1 = H \cdot (\bar{X} \times Y_1)$, and let $M_1 \to Y_1$ be the morphism induced by the projection of $\bar{X} \times Y_1$ onto the second factor.

(2) For any fixed multidegree $(d_1, \ldots, d_r) \in \mathbb{Z}^r_+$, $r \geqq 0$, let

$$Y_2 = S_{d_1, d_2, \ldots, d_r} \subset S_{d_1} \times S_{d_2} \times \ldots \times S_{d_r}$$

be the nonempty Zariski open set of r-tuples of hypersurfaces $H_i \subset \bar{\mathbb{P}}^N$ of degree d_i which intersect properly, i.e., such that $H_1 \cdot H_2 \cdots H_r$ is a complete intersection. This condition is equivalent to requiring that, for $i = 1, 2, \ldots, r$, the equation of H_i is not a zero divisor in $\mathcal{O}_{H_1 \cdot H_2 \cdots H_{i-1}}$ ($= \mathcal{O}_{\bar{\mathbb{P}}^N}$ if $i = 1$). For each fixed $i = 1, 2, \ldots, r$, let $v_i = \binom{N+d_i}{N}-1$, and let h_i be the form in

$$\bar{k}[X_0, \ldots, X_N, Y_{10}, \ldots, Y_{1v_1}, Y_{20}, \ldots, Y_{2v_2}, \ldots, Y_{r0}, \ldots, Y_{rv_r}]$$

which is the sum of the degree d_i monomials in the X's with coefficient the corresponding Y_{ij}, $j = 1, \ldots, v_i$. (The $Y_{i'j}$ with $i' \neq i$ do not appear in h_i.) Let $M' \subset \bar{\mathbb{P}}^N \times S_{d_1} \times S_{d_2} \times \ldots \times S_{d_r}$ be the closed subvariety defined by the ideal $(h_1, \ldots, h_r)$, let $M_2 = M' \cdot (\bar{\mathbb{P}}^N \times Y_2)$, and let $M_2 \to Y_2$ be the morphism induced by the projection of $\bar{\mathbb{P}}^N \times Y_2$ onto the second factor.

Lemma 1: *The families $M_i \to Y_i$, $i = 1, 2$, are proper and flat.*

Proof: (1) $M_1 \to Y_1$.

The morphism $M_1 \hookrightarrow \bar{X} \times Y_1$ is obtained by restriction of the closed immersion $H \hookrightarrow \overline{\mathbb{P}}^N \times \overline{\mathbb{P}}^\nu$ and so is itself a closed immersion:

$$\begin{tikzcd} & H \arrow[r, hook] & \overline{\mathbb{P}}^N \times \overline{\mathbb{P}}^\nu \\ M_1 = H \cdot (\bar{X} \times Y_1) \arrow[ur, hook] \arrow[rr, hook] & & \bar{X} \times Y_1 \arrow[u, hook] \end{tikzcd}$$

The morphism $M_1 \to Y_1$ is the composition of two closed immersions and one projection:

$$M_1 \to \bar{X} \times Y_1 \to \overline{\mathbb{P}}^N \times Y_1 \to Y_1.$$

The third map $\overline{\mathbb{P}}^N \times Y_1 \to Y_1$ is proper because $\overline{\mathbb{P}}^N$ is proper over $\bar{k}$. Since all three morphisms are proper, $M_1 \to Y_1$ is also proper.

As for flatness, by [3], ch. 2, § 3, Proposition 15, it suffices to verify that the localization B_x of $\mathcal{O}_{M_1}$ at any closed point $x \in M_1$ is flat over the localization A_y of $\mathcal{O}_{Y_1}$ at the closed point $y \in Y_1$, where $x \mapsto y$. If B'_x denotes the localization of $\mathcal{O}_{\bar{X} \times Y_1}$ at $x \in M_1 = H \cdot (\bar{X} \times Y_1) \subset \bar{X} \times Y_1$, then:

1. since $\mathcal{O}_{\bar{X} \times Y_1}$ is flat (in fact, free) over $\mathcal{O}_{Y_1}$, it follows that B'_x is flat over A_y;

2. we have the exact sequence

$$0 \to B'_x \xrightarrow{h} B'_x \to B_x \to 0,$$

where the first map is multiplication by the restriction of the equation of H to B'_x. Let $k = A_y/m_y$ be the residue field at y. Tensoring with k gives

$$0 = \mathrm{Tor}_1^{A_y}(B'_x, k) \to \mathrm{Tor}_1^{A_y}(B_x, k) \xrightarrow{\partial} B'_x \otimes k \to B'_x \otimes k \to B_x \otimes k \to 0.$$

But, by the definition of Y_1, h is not a zero divisor in the structure sheaf of the fibre over any closed point $y \in Y_1$. Thus, the map

$$B'_x \otimes k \xrightarrow{h} B'_x \otimes k$$

is injective, and

$$\mathrm{Tor}_1^{A_y}(B_x, k) = 0.$$

This implies flatness of B_x over A_y by the 'local criterion for flatness' (cf. [48]): If $R \to S$ is a local homomorphism of Noetherian local rings and m is the maximal ideal of R, then S is flat over R if and only if

$\mathrm{Tor}_1^R(S, R/m) = 0.$

(2) $M_2 \to Y_2$.

The morphism $M_2 \to Y_2$ is the composition of the morphisms

$$M_2 \to \bar{\mathbb{P}}^N \times Y_2 \to Y_2,$$

where the first is a closed immersion, and so $M_2 \to Y_2$ is proper.

We prove flatness by induction on r. If $r = 1$, we have the special case $X = \mathbb{P}^N$ of the first part of this lemma. Suppose that $r > 1$ and flatness holds for $r-1$.

Let $\tilde{Y}$ be the Y_2 for $r-1$, i.e., the moduli space of complete intersections of multidegree $(d_1, \ldots, d_{r-1})$ in $\bar{\mathbb{P}}^N$. Let $\tilde{M}$ be the closed subvariety of $\bar{\mathbb{P}}^N \times S_{d_1} \times \ldots \times S_{d_r}$ defined by the ideal $(h_1, \ldots, h_{r-1})$. Let $\tilde{M}'$ be the closed subvariety of

$$\bar{\mathbb{P}}^N \times S_{d_1} \times \ldots \times S_{d_{r-1}}$$

defined by the ideal $(h_1, \ldots, h_{r-1})$. (Recall that $h_1, \ldots, h_{r-1}$ do not involve the coordinates $Y_{r0}, \ldots, Y_{rv_r}$ of S_{d_r}.) Let

$$M^* = \tilde{M} \cdot (\bar{\mathbb{P}}^N \times \tilde{Y} \times S_{d_r}) = [\tilde{M}' \cdot (\bar{\mathbb{P}}^N \times \tilde{Y})] \times S_{d_r}.$$

The expression in brackets is the M_2 for $r-1$. Hence, the induction assumption and the fact that flatness is preserved under change of base imply flatness of the morphism

$$M^* \to \tilde{Y} \times S_{d_r}$$

induced by the projection $\bar{\mathbb{P}}^N \times \tilde{Y} \times S_{d_r} \to \tilde{Y} \times S_{d_r}$. The morphism $M^* \to \tilde{Y} \times S_{d_r}$ remains flat when restricted to the Zariski open set over $Y_2 \subset \tilde{Y} \times S_{d_r}$. That is, the following morphism is flat:

$$\tilde{M} \cdot (\bar{\mathbb{P}}^N \times Y_2) \to Y_2.$$

Now $M_2 = M' \cdot (\bar{\mathbb{P}}^N \times Y_2)$ is the closed subvariety of $\tilde{M} \cdot (\bar{\mathbb{P}}^N \times Y_2)$ given by the equation h_r. We are hence in the same situation as in part (1) of this lemma. Namely, we must prove flatness of a morphism whose local ring B_x at any point is the quotient of multiplication by h_r in a flat local ring B'_x:

$$0 \to B'_x \xrightarrow{h_r} B'_x \to B_x \to 0.$$

The rest of the proof is identical to the proof of the first part of the lemma. QED

LEMMA 2: *Suppose that for some positive integer d*

$$H^i(X, \mathcal{O}_X(-d)) = 0 \qquad \text{for } i < n.$$

Then the cohomology along the fibers of the structure sheaf of the family of properly intersecting hypersurface sections parametrized by $Y_1 \subset S_d$ is locally free on Y_1, and its formation commutes with change of base. That is, the cohomology of the hypersurface section corresponding to a point $y \in Y_1$ is naturally isomorphic to the restriction to the fibre of the cohomology of the family.

PROOF: Let f denote the morphism $M_1 \to Y_1$. Let $\mathcal{F} = \mathcal{O}_{M_1}$. By Lemma 1, we may apply the base-changing theorems in Mumford, [42], p. 50–51, which give the following information:

(a) For each $i \geqq 0$, the function $Y_1 \to \mathbb{Z}$ given by

$$y \mapsto \dim_{\bar{k}(y)} H^i(M_{1_y}, \mathcal{F}_y)$$

is upper semicontinuous on Y_1.

(b) The function $Y_1 \to \mathbb{Z}$ given by

$$y \mapsto \chi(\mathcal{F}_y) = \sum_{i=0}^{\infty} (-1)^i \dim_{\bar{k}(y)} H^i(M_{1_y}, \mathcal{F}_y)$$

is constant on Y_1.

(c) If, for some $i \geqq 0$,

$$y \mapsto \dim_{\bar{k}(y)} H^i(M_{1_y}, \mathcal{F}_y)$$

is a constant function, then the direct image sheaf $R^i r_*(\mathcal{F})$ is a locally free sheaf on Y_1, and for all $y \in Y_1$ the natural map

$$\mathcal{E} \underset{\mathcal{O}_{Y_1}}{\otimes} \bar{k}(y) \to H^i(M_{1_y}, \mathcal{F}_y)$$

is an isomorphism.

If y is a closed point in Y_1, then

$$\mathcal{F}_y = \mathcal{F} \underset{\mathcal{O}_{Y_1}}{\otimes} \bar{k}(y) = \mathcal{O}_{\bar{X} \cdot H_y}$$

corresponds to taking specific values in $\bar{k}$ for the coefficients of h to obtain a hypersurface $H_y \subset \bar{\mathbb{P}}^N$.

Suppose that X and d are such that

$$H^i(X, \mathcal{O}_X(-d)) = 0 \qquad \text{for } i < n.$$

For example, this is true for

$$\{X \text{ a complete intersection, any } d > 0\},$$

or

$$\{X \text{ a Cohen-Macaulay scheme, all } d \gg 0\}$$

(cf. [14], XII, § 1.4). Then

$$H^i(\bar{X}, \mathcal{O}_{\bar{X}}(-d)) = H^i(X, \mathcal{O}_X(-d)) \underset{k}{\otimes} \bar{k} = 0 \qquad \text{for } i < n.$$

Now for y a closed point in Y_1 the sequence

$$0 \to \mathcal{O}_{\bar{X}}(-d) \xrightarrow{h_y} \mathcal{O}_{\bar{X}} \to \mathcal{O}_{\bar{X}\cdot H_y} \to 0$$

is exact. The resulting long exact cohomology sequence gives

$$H^i(\mathcal{O}_{\bar{X}}) \xrightarrow{\sim} H^i(\mathcal{O}_{\bar{X}\cdot H_y}) \qquad \text{for } i < n-1.$$

Hence the function $Y_1 \to \mathbb{Z}$ given by

$$y \mapsto \dim_{\bar{k}(y)} H^i(M_{1_y}, \mathscr{F}_y), \qquad i < n-1,$$

is constant on closed points of Y_1, and hence, by (a), is constant on Y_1. By (b), the function

$$y \mapsto \dim_{\bar{k}(y)} H^{n-1}(M_{1_y}, \mathscr{F}_y)$$

is also constant on Y_1. Hence we have the conclusion in (c) for all i, and Lemma 2 is proved.

Lemma 3: *Let $F : V \to V$ be a p-linear endomorphism of an m-dimensional vector space V over a perfect field of characteristic p. Then*

$$V_{ss} = F^m V.$$

PROOF: Since $V = V_{ss} \oplus V_{\text{nilp}}$, we immediately reduce to the case $V = V_{\text{nilp}}$. But then, if $F^iV \neq (0)$, $i \geqq 0$, we have

$$F^{i+1}V = F(F^iV) \subsetneqq F^iV.$$

Thus, $\dim F^iV \leqq m-i$, $i = 0, 1, \ldots, m$, and $F^mV = (0)$. QED

For any closed point $y \in Y_1$, consider the semisimple part of $V = H^{n-1}(\mathcal{O}_{\bar{X} \cdot H_y})$ under the action of the Frobenius F. Let $m = \dim V$, and let $m_{ss} = \dim V_{ss}$. Let $Y^0 = \operatorname{Spec} A$ be an affine open neighborhood of y over which $\mathscr{E} = R^{n-1}f_*(\mathscr{F})$ is free (for example, without loss of generality we may take

$$A = \bar{k}[Y_1/Y_0, Y_2/Y_0, \ldots, Y_v/Y_0]_g, \qquad \text{where } g \in \bar{k}[Y_1/Y_0, \ldots, Y_v/Y_0]).$$

That is,

$$\tilde{A}^m \simeq \mathscr{E}|Y^0.$$

(For any A-module we let the tilde denote the associated sheaf over Spec A.)

We claim that for closed points y' in some (perhaps smaller) neighborhood Y' of y, we have

$$\dim_{\bar{k}} H^{n-1}(\mathcal{O}_{\bar{X} \cdot H_{y'}})_{ss} \geqq m_{ss}. \ (*)$$

Now the action of F^m on $\mathscr{E}|Y^0 \approx \tilde{A}^m$ is given by an $m \times m$ matrix with entries in A. Consider the map

$$F^m_{m_{ss}} : \textstyle\bigwedge^{m_{ss}} A^m \to \bigwedge^{m_{ss}} A^m$$

induced by F^m on the m_{gg}-th exterior product. By Lemmas 1 and 2, the left side of (*) equals

$$\dim (\operatorname{im} (F^m|\mathscr{E} \otimes_{\mathcal{O}_{Y^0}} \bar{k}(y'))).$$

For any point $y' \in Y^0$ this dimension is $\geqq m_{ss}$ if and only if

$$F^m_{m_{ss}} \otimes \bar{k}(y') \neq 0.$$

The set

$$Y' = \{y' \in Y^0 | F^m_{m_{ss}} \otimes \bar{k}(y') \neq 0\}$$

is open because $F^m_{m_{ss}}$, being an endomorphism of a free finitely generated A-module, is given by a matrix with entries in A, so that $Y^0 - Y'$ is the set of common zeros of all these entries. Since $Y' \ni y$, Y' is a neighborhood of y in which (*) holds.

Finally, because

$$j^* : H^{n-1}(\mathcal{O}_{\bar{X}}) \hookrightarrow H^{n-1}(\mathcal{O}_{\bar{X} \cdot H_{y'}})$$

is injective, it follows that the stable and nilpotent ranks of

$$H^{n-1}(\mathcal{O}_{\bar{X} \cdot H_{y'}})/j^* H^{n-1}(\mathcal{O}_{\bar{X}})$$

under the Frobenius – that is, of the Hasse-Witt – differ by constants independent of $H_{y'}$ from the stable and nilpotent ranks of $H^{n-1}(\mathcal{O}_{\bar{X} \cdot H_{y'}})$. Hence we have proved:

LEMMA 4: *If $X \subset \mathbb{P}^N_k$ is a projective Cohen-Macaulay scheme (resp. a complete intersection) and if for some hypersurface $H_0 \subset \mathbb{P}^N_{\bar{k}}$ of degree $d \gg 0$ (resp. $d > 0$) which intersects properly with $\bar{X} = X \times_k \bar{k}$ the nilpotent rank of the Hasse-Witt matrix (the 'defect') of $\bar{X} \cdot H_0$ is given by $e(X, H_0)$, then for general H (i.e., for all H in a nonempty Zariski open set of the space S_d of hypersurfaces of degree d in $\mathbb{P}^N_{\bar{k}}$) the defect of $\bar{X} \cdot H$ is $\leqq e(X, H_0)$.*

3. *Degree of a generically reduced projective scheme*

We next discuss how to assign a degree D to an arbitrary n-dimensional projective scheme $\bar{X} \subset \bar{\mathbb{P}}^N$ all of whose n-dimensional irreducible components are reduced, and how to bound $\dim_{\bar{k}} H^n(\mathcal{O}_{\bar{X}})$ in terms of n and D.

Let X^0 be the union in $\bar{X}$ of all n-dimensional components of $\bar{X}$. Then the closed immersion $i : X^0 \hookrightarrow \bar{X}$ gives an exact sequence of sheaves on $\bar{X}$

$$0 \to K \to \mathcal{O}_{\bar{X}} \to i_* \mathcal{O}_{X^0} \to 0,$$

where the kernel K has support of dimension $< n$. Then the resulting long exact cohomology sequence gives

$$0 = H^n(K) \to H^n(\mathcal{O}_{\bar{X}}) \to H^n(i_* \mathcal{O}_{X^0}) \to 0,$$

so that lower dimensional components may be ignored in estimating $\dim_{\bar{k}} H^n(\mathcal{O}_{\bar{X}})$.

If $\bar{X}$ is reduced and irreducible, then from Šafarevič ([51], ch. 1, §6.5) we know how to define $\deg \bar{X}$. Namely, let $\mathbb{P}^*$ be the dual projective space of hyperplanes in $\bar{\mathbb{P}}^N$. Let

$$S \subset \mathbb{P}^* \times \overset{n+1 \text{ times}}{\cdots} \times \mathbb{P}^* \times \bar{X}$$

be the closed subvariety defined by the incidence relation: a closed point $(l_1, \ldots, l_{n+1}, x) \in S$ if and only if $l_1(x) = \ldots = l_{n+1}(x) = 0$. Let

$$\pi : S \to \mathbb{P}^* \times \overset{n+1 \text{ times}}{\cdots} \times \mathbb{P}^*$$

be the projection. Then $\pi(S)$ turns out to have codimension one in $\mathbb{P}^* \times \overset{n+1 \text{ times}}{\cdots} \times \mathbb{P}^*$ and so is given by a reduced polynomial homogeneous of some fixed degree D in each of $n+1$ sets of $N+1$ variables. By definition, $\deg \bar{X} = D$.

If we choose hyperplanes $(H_1, \ldots, H_n)$ in the nonempty Zariski open subset of $\mathbb{P}^* \times \overset{n \text{ times}}{\cdots} \times \mathbb{P}^*$ in which H_i intersects properly with

$$\bar{X} \cdot H_1 \cdot H_2 \ldots H_{i-1} \;(= \bar{X} \text{ if } i = 1) \qquad \text{for } i = 1, 2 \ldots, n,$$

then $\bar{X} \cdot H_1 \ldots H_n$ consists of $\leqq D$ points, and consists of precisely D reduced points for $(H_1, \ldots, H_n)$ in a nonempty Zariski open subset of $\mathbb{P}^* \times \overset{n \text{ times}}{\cdots} \times \mathbb{P}^*$ (cf. [51]).

If $\bar{X} \subset \bar{\mathbb{P}}^N$ is an arbitrary n-dimensional projective scheme all of whose n-dimensional irreducible components $X_1, \ldots, X_m$ are reduced, then we define

$$\deg \bar{X} = \sum_{i=1}^{m} \deg X_i.$$

Equivalently, we may define $\deg \bar{X}$ as the number of points of intersection of $\bar{X}$ with the intersection of n general hyperplanes, since the intersection of n general hyperplanes misses both the lower dimensional components of $\bar{X}$ and also all intersections $X_i \cdot X_j$ of different n-dimensional irreducible components. Thus

$$\deg \bar{X} = \deg X^0.$$

We further note that

$$\deg \bar{X} \cdot H_1 \ldots H_r = \deg \bar{X}$$

for $r \leqq n$ general hyperplanes $H_1, \ldots, H_r$.

Finally, we shall need a slight generalization of the method for determining $\deg \bar{X}$ by intersection with general hyperplanes. Namely, let $P \subset \bar{\mathbb{P}}^N$ be a linear subspace disjoint from $\bar{X}$, and let $P^* \subset \mathbb{P}^*$ be the linear subspace of $\mathbb{P}^*$ whose points correspond to hyperplanes containing P. The exact same reasoning as for $(H_1, \ldots, H_n) \in \mathbb{P}^* \times \overset{n \text{ times}}{\cdots} \times \mathbb{P}^*$ will show that the intersection of general $(H_1, \ldots, H_n) \in P^* \times \overset{n \text{ times}}{\cdots} \times P^*$ meets $\bar{X}$ in D reduced points. We are now ready for

LEMMA 5: *If $\bar{X} \subset \bar{\mathbb{P}}^N$ $(X \subset \mathbb{P}_k^N, \bar{X} = X \times_k \bar{k})$ is an arbitrary n-dimensional projective scheme all of whose n-dimensional irreducible components are reduced, and if $D = \deg \bar{X}$, then*

$$\dim_k H^n(\mathcal{O}_X) = \dim_{\bar{k}} H^n(\mathcal{O}_{\bar{X}}) \leqq \binom{D-1}{n+1}.$$

PROOF: As mentioned above, we may assume that $\bar{X}$ is an equidimensional projective variety of dimension n. We use the following

FACT: There exists a finite birational morphism

$$\varphi : \bar{X} \to X',$$

where $X' \subset \bar{\mathbb{P}}^{n+1}$ is a hypersurface of degree D.

This fact is essentially proved in Mumford, [44], p. 373–378, using a projection φ from a subspace P disjoint from $\bar{X}$. The only new assertion here is that $\deg X' = \deg \bar{X}$. But, as noted above, the hyperplanes used to determine $\deg \bar{X}$ may be chosen generically from among those containing P. In addition, the n general hyperplanes in $\bar{\mathbb{P}}^{n+1}$ used to determine $\deg X'$ may be chosen so that their intersection misses the closed subvariety of X' where the birational morphism φ is not an isomorphism. Thus, $\deg X' = \deg \bar{X}$.

So let $\varphi : \bar{X} \to X'$ be as in the above fact. We have the short exact sheaf sequence

$$0 \to \mathcal{O}_{X'} \to \varphi_* \mathcal{O}_{\bar{X}} \to Q \to 0,$$

where the quotient sheaf Q has support of dimension $\leqq n-1$, since φ is birational. Then we have exactness of

$$H^n(\mathcal{O}_{X'}) \to H^n(\varphi_* \mathcal{O}_{\bar{X}}) \to H^n(Q) = 0,$$

so that

$$\begin{aligned}\dim_k H^n(\mathcal{O}_X) &= \dim_{\bar{k}} H^n(\mathcal{O}_{\bar{X}}) = \dim_{\bar{k}} H^n(\varphi_* \mathcal{O}_{\bar{X}}) \text{ (since } \bar{X} \to X' \text{ is finite)} \\ &\leqq \dim_{\bar{k}} H^n(\mathcal{O}_{X'}) = \dim_{\bar{k}} H^{n+1}(\mathcal{O}_{\bar{\mathbb{P}}^{n+1}}(-D)) = \binom{D-1}{n+1}\end{aligned}$$

(cf. Serre, [54], p. 258). QED

4. *X-regular sequences*

Let $X \subset \mathbb{P}_k^N$ be a projective scheme, with k any field for the duration of this section. If $H_1, H_2, \ldots, H_d$ are hypersurfaces in $\mathbb{P}^N$ with equations $h_1, \ldots, h_d$, we say that $H_1, \ldots, H_d$ is an *X-regular sequence* if in any affine open set Spec R of X, for any $i_1 < i_2 < \ldots < i_j, j \geqq 1$, multiplication by h_{i_j} is injective in $R/(h_{i_1}, \ldots, h_{i_{j-1}})$ ($= R$ if $j = 1$). The definition of an X-regular sequence may be restated: for any $i_1 < i_2 < \ldots < i_j$, H_{i_j} intersects properly with $X \cdot H_{i_1} \cdot H_{i_2} \ldots H_{i_{j-1}}$ ($= X$ if $j = 1$).

LEMMA 6: *If X is an arbitrary projective scheme, then there exists a constant C depending only on X such that for any sequence of hyperplanes $H_1, H_2, \ldots, H_d$ which is X-regular*:

$$\dim H^i(\mathcal{O}_{X \cdot H_1 \cdot H_2 \cdots H_d}) \leqq C \qquad \text{for all } i, d \geqq 0.$$

PROOF: We prove by induction on d that for all $i \geqq 0$ and all $j \geqq 0$ there exists a constant $C_{d,i,j}$ independent of the hyperplanes $H_1, \ldots, H_d$ such that

$$(*) \qquad \dim H^i(X \cdot H_1 \cdot H_2 \cdots H_d, \mathcal{O}_{X \cdot H_1 \cdot H_2 \cdots H_d}(-j)) \leqq C_{d,i,j}.$$

Since $H^i(\mathcal{O}_{X \cdot H_1 \cdots H_d}) = 0$ if $i > \dim X - d$, there are only finitely many pairs (d, i) for which $C_{d,i,0} \neq 0$, so this claim implies the lemma.

If $d = 0$, there are no H's and (*) is trivial. Suppose $d \geqq 1$ and (*) holds for $d-1$. If $H_1, \ldots, H_d$ is an X-regular sequence of hyperplanes, then for any $j \geqq 0$ the sequence of sheaves

$$0 \to \mathcal{O}_{X \cdot H_1 \cdots H_{d-1}}(-j-1) \xrightarrow{\text{eq of } H_d} \mathcal{O}_{X \cdot H_1 \cdots H_{d-1}}(-j) \to \mathcal{O}_{X \cdot H_1 \cdots H_d}(-j) \to 0$$

is exact. Then we have for all $i \geqq 0$

$$\begin{aligned}&H^i(X \cdot H_1 \cdots H_{d-1}, \mathcal{O}_{X \cdot H_1 \cdots H_{d-1}}(-j)) \\ &\qquad \to H^i(X \cdot H_1 \cdots H_d, \mathcal{O}_{X \cdot H_1 \cdots H_d}(-j)) \\ &\qquad \xrightarrow{\partial} H^{i+1}(X \cdot H_1 \cdots H_{d-1}, \mathcal{O}_{X \cdot H_1 \cdots H_{d-1}}(-j-1))\end{aligned}$$

Hence

$$\dim H^i(X\cdot H_1\cdots H_d, \mathcal{O}_{X\cdot H_1\cdots H_d}(-j)) \leqq C_{d-1,i,j}+C_{d-1,i+1,j+1},$$

so we need only set $C_{d,i,j} = C_{d-1,i,j}+C_{d-1,i+1,j+1}$. QED

LEMMA 7: *Let $X \subset \mathbb{P}_k^N$ be any n-dimensional projective scheme, and let $H_1,\ldots, H_d$ be an X-regular sequence of hypersurfaces. Then the sequence of sheaves*

$$0 \to \mathcal{O}_{X\cdot(H_1\cup\ \ldots\ \cup H_d} \xrightarrow{\alpha_0} \bigoplus_{i_1} \mathcal{O}_{X\cdot H_{i_1}} \xrightarrow{\alpha_1} \bigoplus_{i_1<i_2} \mathcal{O}_{X\cdot H_{i_1}\cdot H_{i_2}} \xrightarrow{\alpha_2} \cdots$$
$$\cdots \xrightarrow{\alpha_{n-1}} \bigoplus_{i_1<\ldots<i_n} \mathcal{O}_{X\cdot H_{i_1}\cdots H_{i_n}} \to 0$$

is exact. Here α_0 is restriction and α_r on $\mathcal{O}_{X\cdot H_{i_1}\cdots H_{i_r}}$ has image in

$$\bigoplus_{s=0}^{r} \bigoplus_{i_s<j<i_{s+1}} \mathcal{O}_{X\cdot H_{i_1}\cdots H_{i_r}\cdot H_j} \quad (\textit{by convention, } i_0 = 0,\ i_{r+1} = d+1),$$

where it is defined on the s-th term as $(-1)^{r-s}$ restriction.

PROOF: The map α is clearly a differential. We must prove acyclicity. Let Spec A be any affine open set in X, let $h_i \in A$ be the equation of H_i in Spec A, $i = 1,\ldots, d$, and let (*) denote the restriction to Spec A of the sheaf sequence in the lemma. We must prove that (*) is exact.

We let $\mathbb{Z}[X] = \mathbb{Z}[X_1,\ldots, X_d]$, and we make A into a $\mathbb{Z}[X]$-algebra by the map $\varphi: \mathbb{Z}[X] \to A$ sending $X_i \mapsto h_i$. Then (*) is the sequence obtained by applying $A \otimes_{\mathbb{Z}[X]}$ to the sequence of $\mathbb{Z}[X]$-modules

$$0 \to \mathbb{Z}[X]/(X_1X_2\cdots X_d) \xrightarrow{\alpha'_0} \bigoplus_{i_1} \mathbb{Z}[X]/(X_{i_1}) \xrightarrow{\alpha'_1} \bigoplus_{i_1<i_2} \mathbb{Z}[X]/(X_{i_1}, X_{i_2}) \xrightarrow{\alpha'_2} \cdots$$
$$(*') \qquad \cdots \xrightarrow{\alpha'_{d-1}} \mathbb{Z}[X]/(X_1,\ldots, X_d) \to 0,$$

where α'_0 is made up of the canonical surjections

$$\mathbb{Z}[X]/(X_1X_2\cdots X_d) \twoheadrightarrow \mathbb{Z}[X]/(X_{i_1})$$

and α'_r takes $\mathbb{Z}[X]/(X_{i_1},\ldots, X_{i_r})$ to

$$\bigoplus_{s=0}^{r} \bigoplus_{i_s<j<i_{s+1}} \mathbb{Z}[X]/(X_{i_1},\ldots, X_{i_r}, X_j)$$

by $(-1)^{r-s}$ restriction. We prove the lemma in three steps.

Step 1. (*′) *is exact.* Because α' is made up of $\pm$ restriction mappings, it follows that (*′) is the direct sum of sequences over $\mathbb{Z}$ corresponding to each monomial $m = \prod X_{i_j}^{\nu_j} \in \mathbb{Z}[X]$:

$$(*'_m) \qquad 0 \to \mathbb{Z}m \xrightarrow{\alpha'_0} \bigoplus_{i_1 \in I} \mathbb{Z}m \xrightarrow{\alpha'_1} \bigoplus_{\substack{i_1 < i_2 \\ i_1, i_2 \in I}} \mathbb{Z}m \xrightarrow{\alpha'_2} \cdots \xrightarrow{\alpha'_{d-1}} \bigoplus_{\substack{i_1 < \dots < i_n \\ i_1, \dots, i_n \in I}} \mathbb{Z}m \to 0.$$

where $I \subset \{1, \dots, d\}$ is the set of indices of X_i's not appearing in m. (If m is divisible by $X_1 X_2 \cdots X_d$, i.e., $I = \emptyset$, then $(*'_m)$ is the zero sequence.) Without loss of generality, it suffices to take $I = \{1, \dots, d\}$, i.e., $m = 1$, and show exactness of $(*'_m)$.

We define the free abelian groups

$$\wedge^r = \bigoplus_{i_1 < \dots < i_r \leq d} \mathbb{Z} dX_{i_1} \wedge dX_{i_2} \wedge \dots \wedge dX_{i_r},$$

give them the usual structure of exterior multiplication, and define the sequence

$$(*'') \qquad 0 \to \mathbb{Z} \xrightarrow{\alpha''_0} \Lambda^1 \xrightarrow{\alpha''_1} \Lambda^2 \xrightarrow{\alpha''_2} \cdots \xrightarrow{\alpha''_{d-1}} \Lambda^d \to 0$$

by letting each α''_i be exterior multiplication by

$$dX_1 + dX_2 + \dots + dX_d \in \Lambda^1.$$

Then, because of the way the α'_i were defined, the complex $(*'_1)$ is isomorphic to (*″). In turn, the integral unimodular transformation of Λ^1 given by

$$dX_1 \mapsto dX_1 - dX_2 - dX_3 - \dots - dX_d$$
$$dX_i \mapsto dX_i, \qquad i = 2, 3, \dots, d$$

induces an isomorphism of (*″) with the sequence

$$(**) \qquad 0 \to \mathbb{Z} \xrightarrow{\beta_0} \Lambda^1 \xrightarrow{\beta_1} \Lambda^2 \xrightarrow{\beta_2} \cdots \xrightarrow{\beta_{d-1}} \Lambda^d \to 0,$$

where now the β_i are defined by exterior multiplication by dX_1. But (**) is clearly exact, since for $r = 1, \dots, d$

$$\ker \beta_r = \bigoplus_{1 < i_2 < \dots < i_r} \mathbb{Z} dX_1 \wedge dX_{i_2} \wedge \dots \wedge dX_{i_r} = \operatorname{im} \beta_{r-1}.$$

This concludes the proof of Step 1.

Step 2. Exactness of (*′) *implies exactness of* (*) *if we have*

$$\mathrm{Tor}_j^{\mathbb{Z}[X]}(\mathbb{Z}[X]/(X_{i_1}, \ldots, X_{i_r}), A) = 0, \quad j > 0, \text{ all } i_1, \ldots, i_r.$$

This is a standard fact about change of rings whose proof is easy and will be omitted.

Step 3. We have:

$$\mathrm{Tor}_j^{\mathbb{Z}[X]}(\mathbb{Z}[X]/(X_{i_1}, \ldots, X_{i_r}), A) = 0, \quad j > 0, \quad \text{all } i_1, \ldots, i_r.$$

We use induction on r. For $r = 0$ we trivially have

$$\mathrm{Tor}_j^{\mathbb{Z}[X]}(\mathbb{Z}[X], A) = 0, \qquad j > 0.$$

Suppose $r \geqq 1$, and $T_{j;i_1,\ldots,i_{r-1}} = 0$ for $j > 0$, all $i_1, \ldots, i_{r-1}$. Given any $i_1, \ldots, i_r$, consider the short exact sequence of $\mathbb{Z}[X]$-modules

$$0 \to \mathbb{Z}[X]/(X_{i_1}, \ldots, X_{i_{r-1}}) \xrightarrow{X_{i_r}} \mathbb{Z}[X]/(X_{i_1}, \ldots, X_{i_{r-1}}) \to \mathbb{Z}[X]/(X_{i_1}, \ldots, X_{i_r}) \to 0,$$

which leads to the long exact sequence of Tors

$$\begin{array}{l} \hookrightarrow T_{j;i_1,\ldots,i_{r-1}} \to T_{j;i_1,\ldots,i_{r-1}} \to T_{j;i_1,\ldots,i_r} \hookleftarrow \\ \qquad\qquad\qquad\qquad \vdots \\ \hookrightarrow A/(h_{i_1}, \ldots, h_{i_{r-1}}) \xrightarrow{h_r} A/(h_{i_1}, \ldots, h_{i_{r-1}}) \to A/(h_{i_1}, \ldots, h_{i_r}) \to 0. \end{array}$$

The first map in the bottom row is injective precisely by the definition of an X-regular sequence. By the induction assumption $T_{j;i_1,\ldots,i_{r-1}} = 0$ for $j > 0$. Hence $T_{j;i_1,\ldots,i_r} = 0$ for $j > 0$. This proves Step 3, and by the same token Lemma 7. QED

5. *Asymptotic invertibility*

Again let $k = \mathbb{F}_q$. If $\bar{X} \subset \mathbb{P}_k^N$ is a reduced equidimensional projective scheme of dimension n and degree D, we let $T_n \subset \mathbb{P}^* \times \overset{n\,\text{times}}{\cdots} \times \mathbb{P}^*$ be the nonempty Zariski open set of n-tuples of hyperplanes $H_1, \ldots, H_n$ for which $\bar{X} \cdot H_1 \cdots H_n$ consists of D reduced points. For $d \geqq n$, we define $T_d \subset \mathbb{P}^* \times \overset{d\,\text{times}}{\cdots} \times \mathbb{P}^*$ as follows:

$$T_d = \bigcap_{i_1 < \ldots < i_n} \Pi_{i_1 \ldots i_n}^{-1}(T_n),$$

where $\Pi_{i_1\ldots i_n}$ is the map from $\mathbb{P}^* \times \overset{d\,\text{times}}{\cdots} \times \mathbb{P}^*$ onto $\mathbb{P}^* \times \overset{n\,\text{times}}{\cdots} \times \mathbb{P}^*$ given by projection onto the i_1-th, i_2-th, ..., i_n-th terms. For $d < n$, we let

$$T_d = \rho_d(T_n),$$

where

$$\rho_d : \mathbb{P}^* \times \overset{n\,\text{times}}{\cdots} \times \mathbb{P}^* \to \mathbb{P}^* \times \overset{d\,\text{times}}{\cdots} \times \mathbb{P}^*$$

is the projection onto the first d terms. Then for $d > 0$ any $(H_1, \ldots, H_d) \in T_d$ is an X-regular sequence.

THEOREM 1: *Let $\bar{X} \subset \bar{\mathbb{P}}^N$ ($\bar{X} = X \times_k \bar{k}$) be a reduced equidimensional projective scheme of dimension n and degree D. Then there exists a hypersurface H in $\bar{\mathbb{P}}^N$ of any degree $d > 0$ such that the defect*

$$e(X, H) \leqq cd^{n-1},$$

where c is a constant depending only on n and D. The stable rank of the Hasse-Witt matrix of $\bar{X} \cdot H$ then has the same leading term as $\dim_{\bar{k}} H^{n-1}(\mathcal{O}_{\bar{X}\cdot H})$, *namely $Dd^n/n!$.*

PROOF: We choose any hyperplanes $(H_1, \ldots, H_d) \in T_d$. Let $H = H_1 \cup \ldots \cup H_d$. We claim that this H satisfies the theorem.

By Lemma 7, we have an exact sequence

$$0 \to \mathcal{O}_{\bar{X}\cdot H} \xrightarrow{\alpha_0} \bigoplus_{i_1} \mathcal{O}_{\bar{X}\cdot H_{i_1}} \xrightarrow{\alpha_1} \bigoplus_{i_1 < i_2} \mathcal{O}_{\bar{X}\cdot H_{i_1}\cdot H_{i_2}} \xrightarrow{\alpha} \cdots \xrightarrow{\alpha_{n-1}} \bigoplus_{i_1 < \cdots < i_n} \mathcal{O}_{\bar{X}\cdot H_{i_1}\cdots H_{i_n}} \to 0.$$

We break this up into short exact sequences, by defining

$$K_i = \operatorname{Ker} \alpha_{n-i}, \quad i = 1, 2, \ldots, n-1 \quad (K_{n-1} = \mathcal{O}_{\bar{X}\cdot H}).$$

We obtain:

$$0 \to K_1 \to \bigoplus_{i_1 < \ldots < i_{n-1}} \mathcal{O}_{\bar{X}\cdot H_{i_1}\cdots H_{i_{n-1}}} \to \bigoplus_{i_1 < \ldots < i_n} \mathcal{O}_{\bar{X}\cdot H_{i_1}\cdots H_{i_n}} \to 0;$$

$$0 \to K_j \to \bigoplus_{i_1 < \ldots < i_{n-j}} \mathcal{O}_{\bar{X}\cdot H_{i_1}\cdots H_{i_{n-j}}} \to K_{j-1} \to 0, \qquad j = 2, 3, \ldots, n-1.$$

(Note: we do not assume that $d \geqq n$; if $d < n$, some terms vanish and the arguments still hold.)

The first sequence gives the exact cohomology sequence

$$0 \to H^0(K_1) \to \bigoplus_{i_1 < \ldots < i_{n-1}} H^0(\mathcal{O}_{\bar{X}\cdot H_{i_1}\cdots H_{i_{n-1}}}) \to \bigoplus_{i_1<\ldots<i_n} H^0(\mathcal{O}_{\bar{X}\cdot H_{i_1}\cdots H_{i_n}})$$

$$\xrightarrow{\partial} H^1(K_1) \to \bigoplus_{i_1<\ldots<i_{n-1}} H^1(\mathcal{O}_{\bar{X}\cdot H_{i_1}\cdots H_{i_{n-1}}}) \to 0.$$

The Frobenius acts bijectively on the second and third terms in the first row, because those intersection schemes are all reduced. Hence F also acts bijectively on the first term. Since passing to the nilpotent part is an exact functor, we have

$$\dim H^1(K_1)_{\mathrm{nilp}} = \sum_{i_1<\ldots<i_{n-1}} \dim H^1(\mathcal{O}_{\bar{X}\cdot H_{i_1}\cdots H_{i_{n-1}}})_{\mathrm{nilp}} \leqq \binom{d}{n-1}\cdot\binom{D-1}{2}$$

by Lemma 5 applied to each scheme $\bar{X}\cdot H_{i_1}\cdots H_{i_{n-1}}$. This same exact sequence also gives us

$$\begin{aligned}\Big|\dim H^1(K_1) - \sum_{i_1<\ldots<i_n} \dim H^0(\mathcal{O}_{\bar{X}\cdot H_{i_1}\cdots H_{i_n}})\Big| &= \Big|\dim H^1(K_1) - D\cdot\binom{d}{n}\Big| \\ &\leqq \sum_{i_1<\ldots<i_{n-1}} [\dim H^1(\mathcal{O}_{\bar{X}\cdot H_{i_1}\cdots H_{i_{n-1}}}) + \dim H^0(\mathcal{O}_{\bar{X}\cdot H_{i_1}\cdots H_{i_{n-1}}})] \\ &\leqq \binom{d}{n-1}\Big[\binom{D-1}{2}+D\Big]\end{aligned}$$

(Note that $\bar{X}\cdot H_{i_1}\cdots H_{i_{n-1}}$ is not necessarily connected, but it has at most D connected components.)

Similarly, the j-th short exact sequence above ($j = 2, 3, \ldots, n-1$) gives the cohomology sequence

$$\bigoplus_{i_1<\ldots<i_{n-j}} H^{j-1}(\mathcal{O}_{\bar{X}\cdot H_{i_1}\cdots H_{i_{n-j}}}) \to H^{j-1}(K_{j-1})$$

$$\xrightarrow{\partial} H^j(K_j) \to \bigoplus_{i_1<\ldots<i_{n-j}} H^j(\mathcal{O}_{\bar{X}\cdot H_{i_1}\cdots H_{i_{n-j}}}) \to 0,$$

since it is clear (for example, arguing inductively) that $H^q(K_j) = 0$ for $q > j$. We have

$$\begin{aligned}\dim H^j(K_j)_{\mathrm{nilp}} - \dim H^{j-1}(K_{j-1})_{\mathrm{nilp}} &\leqq \sum_{i_1<\ldots<i_{n-j}} \dim H^j(\mathcal{O}_{\bar{X}\cdot H_{i_1}\cdots H_{i_{n-j}}}) \\ &\leqq \binom{d}{n-j}\cdot\binom{D-1}{j+1}.\end{aligned}$$

Since $K_{n-1} = \mathcal{O}_{\bar{X}\cdot H}$, we have

$$\begin{aligned}\dim H^{n-1}(\mathcal{O}_{\bar{X}\cdot H})_{\mathrm{nilp}} &= \dim H^1(K_1)_{\mathrm{nilp}} \\ &\quad + \sum_{i=2}^{n-1} [\dim H^i(K_i)_{\mathrm{nilp}} - \dim H^{i-1}(K_{i-1})_{\mathrm{nilp}}] \\ &\leqq \sum_{i=1}^{n-1} \binom{d}{n-i}\binom{D-1}{i+1} \\ &\leqq cd^{n-1},\end{aligned}$$

where c depends only on n and D. But then

$$\begin{aligned}e(X, H) &= \dim (H^{n-1}(\mathcal{O}_{\bar{X}\cdot H})/j^*H^{n-1}(\mathcal{O}_{\bar{X}}))_{\mathrm{nilp}} \\ &\leqq \dim H^{n-1}(\mathcal{O}_{\bar{X}\cdot H})_{\mathrm{nilp}} \leqq cd^{n-1}.\end{aligned}$$

The final assertion of the theorem is proved as follows:

$$\begin{aligned}&|\dim H^{n-1}(\mathcal{O}_{\bar{X}\cdot H}) - D\tbinom{d}{n}| \leqq |\dim H^1(K_1) - D\tbinom{d}{n}| \\ &\quad + \sum_{j=2}^{n-1} |\dim H^j(K_j) - \dim H^{j-1}(K_{j-1})| \leqq \binom{d}{n-1}\left(D + \binom{D-1}{2}\right) \\ &\quad + \sum_{j=2}^{n-1} \sum_{i_1 < \ldots < i_{n-j}} [\dim H^j(\mathcal{O}_{\bar{X}\cdot H_{i_1}\cdots H_{i_{n-j}}}) + \dim H^{j-1}(\mathcal{O}_{\bar{X}\cdot H_{i_1}\cdots H_{i_{n-j}}})] \\ &\leqq \binom{d}{n-1}\left(D + \binom{D-1}{2}\right) + \sum_{j=2}^{n-1} 2C\binom{d}{n-j},\end{aligned}$$

where C is the constant from Lemma 6 (which, we recall, may depend on X, not only on $\deg X$). Hence for some constants C_1 and C_2

$$|\dim H^{n-1}(\mathcal{O}_{\bar{X}\cdot H}) - Dd^n/n!| \leqq C_1 d^{n-1} + C_2 d^{n-2},$$

where C_1 depends only on $\deg X$ and C_2 depends only on X. QED

Combining Theorem 1 and Lemma 4, we have

THEOREM 2: *Let $\bar{X} \subset \bar{\mathbb{P}}^N$ ($\bar{X} = X \times_k \bar{k}$) be an equidimensional projective variety of dimension n and degree D which is Cohen-Macaulay (resp. is a complete intersection). Then there exists an integer d_0 such that for $d \geqq d_0$ (resp. for $d > 0$) the general hypersurface H of degree d in $\bar{\mathbb{P}}^N$ has defect*

$$e(X, d) \leqq cd^{n-1},$$

where c is a constant depending only on n and D (but d_0 may depend on X).

6. *Invertibility for complete intersections*

One of L. Miller's results in [40] is a proof of the invertibility of the Hasse-Witt matrix for general hypersurfaces of any degree. That is,

$$e(\mathbb{P}^n_k, d) = 0 \qquad \text{for } d > 0.$$

In particular, the invertibility conjecture (that $e(X, d) = 0$ for $d \gg 0$) holds for $X = \mathbb{P}^n_k$. Using the technique in the proof of Theorem 1, we have a simple proof of a slight generalization of this.

Namely, let $(d_1, d_2, \ldots, d_r) \in \mathbb{Z}^r_+$, $r \geqq 0$, be any fixed multidegree. Recall that

$$S_{d_1, d_2, \ldots, d_r} \subset S_{d_1} \times S_{d_2} \times \ldots \times S_{d_r}$$

is the nonempty Zariski open set of r-tuples of hypersurfaces $H_i \subset \bar{\mathbb{P}}^N$ of degree d_i which intersect properly, i.e., such that $H_1 \cdot H_2 \cdots H_r$ is a complete intersection. By 'the general complete intersection of multidegree $(d_1, d_2, \ldots, d_r)$' we mean 'any complete intersection in some nonempty Zariski open subset of $S_{d_1, d_2, \ldots, d_r}$.'

THEOREM 3: *The general complete intersection of multidegree* $(d_1, d_2, \ldots, d_r)$ *in* $\bar{\mathbb{P}}^N$ *has invertible Hasse-Witt matrix.*

PROOF: By the second part of Lemma 1, we are dealing with a flat and proper family of varieties. Then the same argument that was used to prove Lemma 4 shows that it is sufficient to find a single example of a complete intersection of given multidegree with invertible Hasse-Witt. We show:

CLAIM: If $H_{11}, H_{12}, \ldots, H_{1d_1}, H_{21}, \ldots, H_{2d_2}, \ldots, H_{rd_r}$ is a sequence of $d_1 + d_2 + \ldots + d_r$ hyperplanes in general position (i.e., a $\mathbb{P}^N$-regular sequence; all possible intersections must have the 'right' dimension) and if

$$H_i = \bigcup_{j=1}^{d_i} H_{ij},$$

then the complete intersection

$$H_1 \cdot H_2 \cdots H_r$$

has invertible Hasse-Witt.

We prove the claim by induction on r. The claim is trivial if $r = 0$. Suppose $r > 0$ and the claim holds for $r-1$ (for all dimensions $N \geqq r-1$ of the ambient projective space). Let $\{H_{ij}\}$ be an $\bar{\mathbb{P}}^N$-regular sequence of hyperplanes with $H_i = \bigcup_{j=1}^{d_i} H_{ij}$, as in the claim. Let

$$X = H_1 \cdot H_2 \cdots H_{r-1}.$$

(Let $X = \bar{\mathbb{P}}^N$ if $r = 1$.) Let $n = \dim X$.

We apply Lemma 7 to the variety X and the hyperplanes $H_{r1}, H_{r2}, \ldots, H_{rd_r}$. As in the proof of Theorem 1, we break up the resulting exact sequence into short exact sequences ($K_{n-1} = \mathcal{O}_{X \cdot H_r} = \mathcal{O}_{H_1 \cdot H_2 \cdots H_r}$):

$$0 \to K_1 \to \bigoplus_{i_1 < \ldots < i_{n-1}} \mathcal{O}_{X \cdot H_{ri_1} \cdots H_{ri_{n-1}}} \to \bigoplus_{i_1 < \ldots < i_n} \mathcal{O}_{X \cdot H_{ri_1} \cdots H_{ri_n}} \to 0;$$

$$0 \to K_j \to \bigoplus_{i_1 < \ldots < i_{n-j}} \mathcal{O}_{X \cdot H_{ri_1} \cdots H_{ri_{n-j}}} \to K_{j-1} \to 0, \quad j = 2, 3, \ldots, n-1.$$

The first sequence gives the exact cohomology sequence

$$\begin{aligned} 0 \to H^0(K_1) \to \bigoplus_{i_1 < \ldots < i_{n-1}} H^0(\mathcal{O}_{X \cdot H_{ri_1} \cdots H_{ri_{n-1}}}) &\to \bigoplus_{i_1 < \ldots < i_n} H^0(\mathcal{O}_{X \cdot H_{ri_1} \cdots H_{ri_n}}) \\ \xrightarrow{\partial} H^1(K_1) \to \bigoplus_{i_1 < \ldots < i_{n-1}} H^1(\mathcal{O}_{X \cdot H_{ri_1} \cdots H_{ri_{n-1}}}) &\to 0. \end{aligned}$$

The Frobenius acts bijectively on the second and third terms in the first row. Moreover, by the induction assumption applied to the complete intersection

$$X \cdot H_{ri_1} \cdots H_{ri_{n-1}}$$

in the projective space

$$H_{ri_1} \cdots H_{ri_{n-1}} \approx \bar{\mathbb{P}}^r,$$

the Frobenius acts bijectively on

$$\bigoplus_{i_1 < \ldots < i_{n-1}} H^1(\mathcal{O}_{X \cdot H_{ri_1} \cdots H_{ri_{n-1}}}).$$

Hence F acts bijectively on $H^1(K_1)$.

Similarly, the j-th short exact sheaf sequence above ($j = 2, 3, \ldots, n-1$) gives the exact cohomology sequence

$$0 \to H^{j-1}(K_{j-1}) \xrightarrow{\partial} H^j(K_j) \to \bigoplus_{i_1 < \ldots < i_{n-j}} H^j(\mathcal{O}_{X \cdot H_{ri_1} \cdots H_{ri_{n-j}}}) \to 0.$$

(Here we use the fact that a j-dimensional complete intersection has vanishing $(j-1)$-st cohomology, $j \geqq 2$.) By the induction assumption applied to the complete intersection

$$X \cdot H_{ri_1} \cdots H_{ri_{n-j}}$$

in the projective space $H_{ri_1} \cdots H_{ri_{n-j}}$, the Frobenius acts bijectively on the third term. Suppose F acts bijectively on $H^{j-1}(K_{j-1})$. Then it acts bijectively on $H^j(K_j)$. Hence, it follows by induction that F acts bijectively on $H^j(K_j)$, $j = 1, 2, \ldots, n-1$. In particular, it acts bijectively on $H^{n-1}(K_{n-1}) = H^{n-1}(\mathcal{O}_{H_1 \cdot H_2 \cdots H_r})$, and we are done. QED

COROLLARY: *Let*

$$\bar{\mathbb{P}}^r \subset \bar{\mathbb{P}}^{r+1} \subset \ldots \subset \bar{\mathbb{P}}^N$$

($0 \leqq r \leqq N$) *be fixed imbeddings as successive hyperplanes. Let*

$$S^*_{d_1, d_2, \ldots, d_r} \subset S_{d_1, d_2, \ldots, d_r}$$

denote the Zariski open set of complete intersections $X \subset \bar{\mathbb{P}}^N$ *of multidegree* $(d_1, d_2, \ldots, d_r)$ *for which*:

(a) *X intersects properly with each* $\bar{\mathbb{P}}^i$, $i = r, r+1, \ldots, N-1$;

(b) *the* $X \cdot \bar{\mathbb{P}}^i$ *all have invertible Hasse-Witt matrices,*

$$i = r, r+1, \ldots, N-1.$$

Then $S^*_{d_1, d_2, \ldots, d_r}$ *is nonempty.*

THEOREM 4: *The general complete intersection X of multidegree* $(d_1, d_2, \ldots, d_r)$ *in* $\bar{\mathbb{P}}^N$ *has the property that* $e(X, d) = 0$ *for* $d > 0$. *In particular, the invertibility conjecture holds for such general X.*

PROOF: We prove that $X \in S^*_{d_1, d_2, \ldots, d_r}$ implies $e(X, d) = 0$ for $d > 0$. The proof is by induction on N. The implication is trivial if $N = r$.

Suppose that $N > r$ and that $e(X', d) = 0$ for $d > 0$ for any X' in the $S^*_{d_1, d_2, \ldots, d_r; N-1}$ corresponding to $\bar{\mathbb{P}}^{N-1}$. By Lemma 4, for our $X \in S^*_{d_1, d_2, \ldots, d_r; N}$ we need only exhibit one $H \in S_d$ which intersects properly with X and for which $e(X, H) = 0$.

We now use induction on d. First, $e(X, 1) = 0$ because $X \cdot \bar{\mathbb{P}}^{N-1}$ has invertible Hasse-Witt. Suppose $e(X, d-1) = 0$. Let $H' \subset \bar{\mathbb{P}}^N$ be a hypersurface of degree $d-1$ intersecting properly with X such that:

(a) $e(X, H') = 0$;

(b) H' intersects properly with $X \cdot \bar{\mathbb{P}}^{N-1}$;

(c) $e(X \cdot \bar{\mathbb{P}}^{N-1}, H' \cdot \bar{\mathbb{P}}^{N-1}) = 0$.

Such H' need only be in the intersection of three nonempty Zariski open sets in S_{d-1}. (Property (c)) is fulfilled for a nonempty Zariski open set in S_{d-1} because of the induction assumption on N and the fact that

$$X \cdot \bar{\mathbb{P}}^{N-1} \in S^*_{d_1, d_2, \ldots, d_r; N-1}.)$$

Let $H = H' \cup \bar{\mathbb{P}}^{N-1}$. Since H', $\bar{\mathbb{P}}^{N-1}$ form an X-regular sequence of hypersurfaces, the following sequence is exact by Lemma 7:

$$0 \to \mathcal{O}_{X \cdot H} \to \mathcal{O}_{X \cdot H'} \oplus \mathcal{O}_{X \cdot \bar{\mathbb{P}}^{N-1}} \to \mathcal{O}_{X \cdot \bar{\mathbb{P}}^{N-1} \cdot H'} \to 0.$$

The resulting exact cohomology sequence is

$$0 \to H^{N-r-2}(\mathcal{O}_{X \cdot \bar{\mathbb{P}}^{N-1} \cdot H'}) \xrightarrow{\partial} H^{N-r-1}(\mathcal{O}_{X \cdot H})$$
$$\to H^{N-r-1}(\mathcal{O}_{X \cdot H'}) \oplus H^{N-r-1}(\mathcal{O}_{X \cdot \bar{\mathbb{P}}^{N-1}}) \to 0.$$

By construction, the Frobenius acts bijectively on the first and third terms. Hence F acts bijectively on $H^{N-r-1}(\mathcal{O}_{X \cdot H})$. QED

7. *Invertibility for curves of given genus*

In [39] Miller proves by explicitly computing an example that the generic curve of genus g (in the sense of Deligne-Mumford [6]) has invertible Hasse-Witt matrix. Here is a simpler, more geometrical construction of an example:

THEOREM 5: *The generic curve of genus g has invertible Hasse-Witt matrix.*

PROOF: Let $E_1, E_2, \ldots, E_g$ be *any* elliptic plane curves with nonzero Hasse invariant. Imbed them in various planes in $\bar{\mathbb{P}}^3$ so that for $1 \leqq i < j \leqq g$:

$$E_i \cdot E_j = \begin{cases} \text{one reduced point if } j = i+1 \\ \emptyset \text{ otherwise.} \end{cases}$$

Let

$$C = E_1 \cup \ldots \cup E_g.$$

Then C is a 'stable curve' in the sense of [6]. The theorem is proved if we show that

(1) genus $C = g$;

(2) C has invertible Hasse-Witt.

We prove this by induction on g. The claim is trivial for $g = 1$. Suppose it holds for $g-1$. Let

$$C' = E_1 \cup \ldots \cup E_{g-1}.$$

We have the short exact sheaf sequence

$$0 \to \mathcal{O}_C \to \mathcal{O}_{C'} \oplus \mathcal{O}_{E_g} \to \mathcal{O}_{C' \cdot E_g} \to 0,$$

coming locally from the short exact sequence of ideals

$$0 \to I_C \to I_{C'} \oplus I_{E_g} \to I_{C'} + I_{E_g} \to 0.$$

The sheaf sequence gives the following exact cohomology sequence:

$$0 \to H^0(\mathcal{O}_C) \to H^0(\mathcal{O}_{C'}) \oplus H^0(\mathcal{O}_{E_g}) \to H^0(\mathcal{O}_{C' \cdot E_g})$$
$$\xrightarrow{\partial} H^1(\mathcal{O}_C) \to H^1(\mathcal{O}_{C'}) \oplus H^1(\mathcal{O}_{E_g}) \to 0.$$

The top row is isomorphic to

$$0 \to k \to k \oplus k \to k,$$

so that the last map here is surjective, i.e., $\partial = 0$. Hence the second row gives

$$H^1(\mathcal{O}_C) \cong H^1(\mathcal{O}_{C'}) \oplus H^1(\mathcal{O}_{E_g}).$$

Therefore:

(1) genus $C =$ genus $C' +$ genus $E_g = (g-1)+1 = g$;

(2) the Frobenius is bijective on $H^1(\mathcal{O}_{C'})$ (by the induction assumption) and on $H^1(\mathcal{O}_{E_g}) \Rightarrow$ it is bijective on $H^1(\mathcal{O}_C)$. QED

COROLLARY OF PROOF: Given integers g and r, $0 \leqq r \leqq g$, there exist stable curves of genus g with diagonal Hasse-Witt matrix of rank r. Namely, let $E_{r+1}, E_{r+2}, \ldots, E_g$ be supersingular in the above construction.

REMARK: To show generic invertibility in the case of triangular genera $g = (d-1)(d-2)/2$, we see by the proof of Theorem 3 that it suffices to take a stable *plane* curve, namely the union of d lines in $\mathbb{P}^2$ in general position.

II. Invertibility conjecture for hypersurface sections

1. *Algorithm for computing the Hasse-Witt matrix of a hypersurface* (see Dwork, [11], § 7.10 and Katz, [21], Corollary 6.1.13).

Let $H \subset \bar{\mathbb{P}}^{n+1}$ be a hypersurface of degree d defined by an equation

$$h \in \bar{k}[X_0, X_1, \ldots, X_{n+1}].$$

We have

$$\begin{array}{ccccccccc}
0 & \longrightarrow & \mathcal{O}_{\bar{\mathbb{P}}^{n+1}}(-d) & \xrightarrow{h} & \mathcal{O}_{\bar{\mathbb{P}}^{n+1}} & \longrightarrow & \mathcal{O}_H & \longrightarrow & 0 \\
 & & \downarrow{\scriptstyle h^{p-1}F} & & \downarrow{\scriptstyle F} & & \downarrow{\scriptstyle F} & & \\
0 & \longrightarrow & \mathcal{O}_{\bar{\mathbb{P}}^{n+1}}(-d) & \xrightarrow{h} & \mathcal{O}_{\bar{\mathbb{P}}^{n+1}} & \longrightarrow & \mathcal{O}_H & \longrightarrow & 0.
\end{array}$$

In the resulting long exact cohomology sequence the coboundary gives

$$H^n(H, \mathcal{O}_H) \xrightarrow{\sim} H^{n+1}(\bar{\mathbb{P}}^{n+1}, \mathcal{O}_{\bar{\mathbb{P}}^{n+1}}(-d)),$$

so that the Frobenius F on $H^n(\mathcal{O}_H)$ corresponds to the map on $H^{n+1}(\bar{\mathbb{P}}^{n+1}, \mathcal{O}_{\bar{\mathbb{P}}^{n+1}}(-d))$ induced by

$$\mathcal{O}_{\bar{\mathbb{P}}^{n+1}}(-d) \xrightarrow{\text{pth power}} \mathcal{O}_{\bar{\mathbb{P}}^{n+1}}(-pd) \xrightarrow{h^{p-1}} \mathcal{O}_{\bar{\mathbb{P}}^{n+1}}(-d).$$

We write

$$h^{p-1} = \sum A_\lambda X^\lambda$$

explicitly in terms of monomials $X^\lambda = \prod X_i^{\lambda_i}$ in $\bar{k}[X_0, \ldots, X_{n+1}]$. Now $H^{n+1}(\bar{\mathbb{P}}^{n+1}, \mathcal{O}_{\bar{\mathbb{P}}^{n+1}}(-d))$ has basis elements $1/X^w$, where $w = (w_0, \ldots, w_{n+1})$ runs through $(n+2)$-tuples of strictly positive integers for which $w_0 + \ldots + w_{n+1} = d$. We index these basis elements by w. Then the (w, v)-entry in the Hasse-Witt matrix of H is given by:

$$A_{pw-v}.$$

The following lemma allows us to use this algorithm to compute $e(X, d)$ if X is a hypersurface.

LEMMA 8: *If $X \subset \mathbb{P}_k^{n+1}$ is a hypersurface, then for any hypersurface $H \subset \bar{\mathbb{P}}^{n+1}$ intersecting properly with $\bar{X}$ we have*:

$$e(X, H) = e(\mathbb{P}^{n+1}, \bar{X} \cup H) - e(\mathbb{P}^{n+1}, \bar{X}).$$

For example, if X has invertible Hasse-Witt, then $\bar{X} \cdot H$ has invertible Hasse-Witt if and only if $\bar{X} \cup H$ has invertible Hasse-Witt.

PROOF: From Lemma 7 we have the exact sheaf sequence

$$0 \to \mathcal{O}_{\bar{X} \cup H} \to \mathcal{O}_{\bar{X}} \oplus \mathcal{O}_H \to \mathcal{O}_{\bar{X} \cdot H} \to 0.$$

This gives

$$0 \to H^{n-1}(\mathcal{O}_{\bar{X} \cdot H}) \xrightarrow{\partial} H^n(\mathcal{O}_{\bar{X} \cup H}) \to H^n(\mathcal{O}_{\bar{X}}) \oplus H^n(\mathcal{O}_H) \to 0,$$

from which the lemma follows immediately.

2. *Counterexample to the invertibility conjecture*

Recall that the invertibility conjecture of Grothendieck-Miller [40] asserts that $e(X, d) = 0$ for $d \gg 0$. We show that this is false in general, even for hypersurfaces X.

Let $X \subset \mathbb{P}_{\mathbb{F}_p}^{n+1}$ be the hypersurface with equation

$$X_0^D + X_1^D + \ldots + X_{n-s}^D,$$

i.e., X is the 'cone' over the Fermat hypersurface in $\mathbb{P}^{n-s}$ with 'vertex' consisting of the $\mathbb{P}^s$ at infinity (having homogeneous coordinates $X_{n-s+1}, X_{n-s+2}, \ldots, X_{n+1}$). Suppose that $p < D$, $p \nmid D$. Then:

CLAIM: $e(X, d) > 0$ for all $d > n+1-D$; and, in fact,

$$e(X, d) \sim d^s/s! \qquad \text{for } d \gg 0.$$

PROOF: Let H be any hypersurface of degree $d > n+1-D$ which intersects properly with $\bar{X}$. In the Hasse-Witt matrix of $\bar{X} \cup H$ there are

$$\binom{d+D-n-2+s}{s}$$

rows corresponding to $w \in \mathbb{Z}_+^{n+2}$ for which $w_0 = w_1 = \ldots = w_{n-s} = 1$. For such a w, the first $n-s+1$ components of the vector $pw-v$ are all $\leqq p-1 < D$ for all v. Let $\sum A_\lambda X^\lambda$ be the equation of $\bar{X} \cup H$ raised to the $(p-1)$-st power:

$$\sum A_\lambda X^\lambda = [h(X_0^D + X_1^D + \ldots + X_{n-s}^D)]^{p-1}.$$

Since $(X_0^D + X_1^D + \ldots + X_{n-s}^D)$ divides $\sum A_\lambda X^\lambda$, it follows that $A_{pw-v} = 0$ if the first $n-s+1$ components of $pw-v$ are all $< D$. Thus, the Hasse-Witt matrix of $\bar{X} \cup H$ has at least

$$\binom{d+D-n-2+s}{s}$$

zero rows. By Lemma 8,

$$\begin{aligned} e(X, H) &= e(\mathbb{P}^{n+1}, \bar{X} \cup H) - e(\mathbb{P}^{n+1}, \bar{X}) \\ &\geqq \binom{d+D-n-2+s}{s} - \text{const} \sim d^s/s! \qquad \text{for } d \gg o. \qquad \text{QED} \end{aligned}$$

3. *Revised conjecture*

It seems that the amount of singularity of the fixed variety X has a bearing on the asymptotic order of growth of the defect of hypersurface sections.

REVISED INVERTIBILITY CONJECTURE: Let X be an equidimensional projective Cohen-Macaulay scheme of dimension n and degree D whose singular locus has dimension s, where $n > 1$, $-1 \leqq s \leqq n$. Then there exists an integer d_0 such that

$$e(X, d) \leqq cd^s \qquad \text{for } d \geqq d_0,$$

where c is a constant depending only on n, s and D (but d_0 may depend on X). In particular, if X is smooth (i.e., $s = -1$), then X satisfies the Grothendieck-Miller invertibility conjecture:

$$e(X, d) = 0 \qquad \text{for } d \gg 0.$$

REMARKS: (a) If $s = n$, i.e., if X has a non-reduced component, then the conjecture only has meaning if we extend the definition of 'degree' to such X, and then it is trivial, since

$$\dim H^{n-1}(\mathcal{O}_{\bar{X}\cdot H}) \sim Dd^n/n!.$$

(b) The revised conjecture is true for $s = n-1$ by Theorem 2.

(c) If $s \geqq 0$, we may equally well define $e(X, H)$ as

$$\dim H^{n-1}(\mathcal{O}_{\bar{X}\cdot H})_{\text{nilp}}$$

instead of

$$\dim (H^{n-1}(\mathcal{O}_{\bar{X}\cdot H})/j^*H^{n-1}(\mathcal{O}_{\bar{X}}))_{\text{nilp}}.$$

The revised conjecture is unaffected by the constant difference between these two nilpotent ranks if $s \geqq 0$. However, if $s = 0$ the new constant c may now depend on X as well as n, s, and D.

(d) The counterexample in § 2 above shows that this revised conjecture is the best possible general result we can hope for.

THEOREM 6: *If the revised conjecture holds for some $s-1 \geqq 0$ (for all $n \geqq s$), then it holds for s. However, if $s-1 = 0$, then the constant c in the conjecture may depend on X as well as n, s, and D.*

PROOF: Let X be as in the revised conjecture. Choose a hyperplane P such that $\bar{X}\cdot P$ is an equidimensional projective Cohen-Macaulay scheme of degree D and dimension $n-1$ whose singular locus has dimension $s-1$. By hypothesis, the revised conjecture applies to $\bar{X}\cdot P$. We choose d_0 large enough so that Lemma 4 applies to X for $d \geqq d_0$ and so that the revised conjecture applies to $\bar{X}\cdot P$ for $d \geqq d_0$.

Now for $d \geqq d_0+1$ let H' be a hypersurface of degree $d-1$ intersecting properly with $\bar{X}$ and with $\bar{X}\cdot P$ such that:

(a) $e(X, H') = e(X, d-1)$;

(b) $e(\bar{X}\cdot P, H') \leqq c(d-1)^{s-1}$.

Let $H = H' \cup P$. By Lemma 7 we have the exact sequence

$$0 \to \mathcal{O}_{\bar{X}\cdot H} \to \mathcal{O}_{\bar{X}\cdot P} \oplus \mathcal{O}_{\bar{X}\cdot H'} \to \mathcal{O}_{\bar{X}\cdot P\cdot H'} \to 0,$$

which gives

$$H^{n-2}(\mathcal{O}_{\bar{X}\cdot P\cdot H'}) \xrightarrow{\partial} H^{n-1}(\mathcal{O}_{\bar{X}\cdot H}) \to H^{n-1}(\mathcal{O}_{\bar{X}\cdot P}) \oplus H^{n-1}(\mathcal{O}_{\bar{X}\cdot H'}) \to 0.$$

Then we obtain

$$\begin{aligned} e(X, d) &\leqq e(X, H) \leqq \dim H^{n-1}(\mathcal{O}_{\bar{X}\cdot H})_{\mathrm{nilp}} \\ &\leqq \dim H^{n-2}(\mathcal{O}_{\bar{X}\cdot P\cdot H'})_{\mathrm{nilp}} + \dim H^{n-1}(\mathcal{O}_{\bar{X}\cdot P}) + \dim H^{n-1}(\mathcal{O}_{\bar{X}\cdot H'})_{\mathrm{nilp}} \\ &\leqq e(\bar{X}\cdot P, H') + c_1 + c_2 + e(X, H') + c_3, \end{aligned}$$

where c_1, c_2, c_3 are constants, of which c_1 and c_3 may depend on X as well as on n and D. Let $c_4 = c_1 + c_2 + c_3$. Then

$$\begin{aligned} e(X, d) &\leqq e(\bar{X}\cdot P, H') + c_4 + e(X, H') \\ &\leqq c(d-1)^{s-1} + c_4 + e(X, d-1) \\ &\leqq cd^{s-1} + c_4 + e(X, d-1). \end{aligned}$$

Using the same inequality with $d-1$ in place of d and iterating this process until we reach d_0, we find

$$\begin{aligned} e(X, d) &\leqq cd^{s-1} + c(d-1)^{s-1} + 2\cdot c_4 + e(X, d-2) \\ &\leqq \cdots \\ &\leqq c\sum_{i=1}^{d} i^{s-1} + c_4 d + e(X, d_0) \\ &\leqq \begin{cases} cd^s & \text{if } s-1 > 0 \\ (c+c_4)d & \text{if } s-1 = 0. \end{cases} \end{aligned}$$

This inequality holds for $d \geqq d_0'$, where d_0' is taken large enough (depending on X) to take care of the constant $e(X, d_0)$ and, if $s-1 > 0$, the linear term. Note that if $s-1 = 0$, then we have a new constant coefficient of d^s, namely $c+c_4$, which may depend on X as well as n, s, and D. QED

We are left with the following

Open questions. (a) If X is a projective Cohen-Macaulay variety with point singularities, is the defect $e(X, d)$ bounded as $d \to \infty$?

(b) If X is a smooth projective variety, does $e(X, d) = 0$ for $d \gg 0$?

4. *Example showing that the revised conjecture is false without the condition $d \gg 0$*

Let X be the Fermat hypersurface of degree $n+1$ and dimension n defined over $\mathbb{F}_p$:

$$X = \{x \in \mathbb{P}^{n+1}_{\mathbb{F}_p} | x_0^{n+1} + \ldots + x_{n+1}^{n+1} = 0\}.$$

Note that X is smooth if $p \nmid n+1$.

Claim: If $p < \frac{1}{2}n+1$ (resp. if $p = 2$), then $e(X, d) > 0$ for $d \leqq n+3$ (resp. for $d \leqq \frac{1}{2}n^2 - 1$).

Proof: Since $H^n(\mathcal{O}_X) = 0$, X trivially has invertible Hasse-Witt. Hence, by Lemma 8, for any properly intersecting hypersurface H

$$e(X, H) = e(\mathbb{P}^{n+1}, \bar{X} \cup H).$$

We use the algorithm to show that, if $d \leqq n+3$ (resp. $d \leqq \frac{1}{2}n^2 - 1$) and $p < \frac{1}{2}n+1$ (resp. $p = 2$), then the Hasse-Witt of $\bar{X} \cup H$ has a zero row corresponding to any $w \in \mathbb{Z}_+^{n+2}$ whose components w_i, $i = 0, \ldots, n+1$, are most nearly equal to each other (i.e., all equal to either

$$\left[\frac{d}{n+2}\right] \quad \text{or} \quad \left[\frac{d}{n+2}\right] + 1,$$

where [ ] is the 'greatest integer' function). In fact, for such w all the components of the vector $pw - v$ are bounded by

$$\text{case } p < \tfrac{1}{2}n+1 : p\left(\left[\frac{d}{n+2}\right] + 1\right) - 1 < (\tfrac{1}{2}n+1)\left[\frac{n+3}{n+2}\right] + \tfrac{1}{2}n = n+1$$

$$\text{case } p = 2 : p\left(\left[\frac{d}{n+2}\right] + 1\right) - 1 \leqq 2\left[\frac{\frac{1}{2}n^2 - 1}{n+2}\right] + 1 < n.$$

But the polynomial $\sum A_\lambda X^\lambda$ in the algorithm is divisible by

$$(X_0^{n+1} + \ldots + X_{n+1}^{n+1}).$$

In particular, $A_{pw-v} \neq 0$ is only possible if some component of $pw - v$ is at least $n+1$. Thus, the Hasse-Witt of $\bar{X} \cup H$ has at least one zero row. The claim is proved.

Note that this example does not preclude good *a priori* estimates for

d_0 in the revised conjecture for low dimensions n. The next chapter offers a conjecture along these lines in the case $n = 2$.

III. A conjecture on hyperplane sections of Lefschetz-imbedded surfaces

Let I_{n,d_0} be the set of smooth n-dimensional projective varieties imbedded in $\mathbb{P}_k^m$ ($k = \mathbb{F}_q$) for some m for which the generic hypersurface section of any degree $\geqq d_0$ has invertible Hasse-Witt matrix:

$$X \in I_{n,d_0} \Leftrightarrow e(X, d) = 0 \qquad \text{for } d \geqq d_0.$$

The revised invertibility conjecture asserts that all smooth varieties belong to some I_{n,d_0}. If $n = 2$, let $I_{d_0} = I_{2,d_0}$. In this case there is some evidence for the following more precise conjecture.

An imbedding

$$i : X \hookrightarrow \mathbb{P}^m$$

of a smooth, proper, irreducible variety is said to be Lefschetz if there exists a Lefschetz pencil of hyperplanes in the dual projective space $\mathbb{P}^*$. Except in the special case when $\dim X$ is odd and X is defined over a field of characteristic 2, this is equivalent to: the map

$$\varphi : \mathbb{P}(N) \to \mathbb{P}^*$$

is either not everywhere ramified or else has image of codimension $\geqq 2$ (see Katz, [25]). Here $\mathbb{P}(N)$ is the subvariety of $X \times \mathbb{P}^*$ consisting of pairs (x, H) such that H is tangent to X at x, and φ is induced by the projection

$$X \times \mathbb{P}^* \to \mathbb{P}^*.$$

For example, if X is a hypersurface with homogeneous equation $F(X_0, \ldots, X_m)$, then $\mathbb{P}(N) \cong X$ and $\varphi : X \to \mathbb{P}^*$ is given in homogeneous coordinates by the 'Gauss map'

$$\varphi = \left(\frac{\partial F}{\partial X_0}, \ldots, \frac{\partial F}{\partial X_m}\right).$$

CONJECTURE: Let

$$i : X \hookrightarrow \mathbb{P}^m$$

be a smooth, proper, irreducible surface. Then

$$X \in I_1 \Leftrightarrow i \text{ is Lefschetz.}$$

In particular, X always belongs to I_2 (since its second and higher Segre imbeddings are always Lefschetz, cf. Katz, [25]).

EVIDENCE: 1°. If X is a Lefschetz-imbedded *cubic* surface in $\mathbb{P}^3$, then $X \in I_1$.

2°. If X is the Fermat cubic surface

$$X_0^3 + X_1^3 + X_2^3 + X_3^3 = 0$$

defined over $\mathbb{F}_2$ – here X is *not Lefschetz* – then $X \notin I_1$ but $X \in I_2$.

3°. Suppose X is the Fermat surface

$$X_0^d + X_1^d + X_2^d + X_3^d = 0$$

defined over $\mathbb{F}_p$, $p \nmid d$. Since the Gauss map in this case is

$$(X_0, \ldots, X_m) \mapsto (dX_0^{d-1}, \ldots, dX_m^{d-1}),$$

it follows that X is Lefschetz if and only if $p \nmid d-1$. Then first of all:

$$p|(d-1) \Rightarrow X \notin I_1.$$

4°. In the situation of 3°,

$$p \nmid (d-1) \Rightarrow X \in I_1 \qquad \text{for } d \leqq 6.$$

Note that in 1° and 4° we have $X \in I_1$ if X has a plane section with invertible Hasse-Witt; this is a special case of

LEMMA 9: *If X is a 2-dimensional complete intersection and H_1 and H_2 are hypersurfaces of degrees d_1 and d_2 which intersect properly with X and for which*

$$e(X, H_1) = e(X, H_2) = 0,$$

then for any positive integers i and j

$$e(X, id_1 + jd_2) = 0.$$

PROOF: Since generic degree d_1 and degree d_2 sections have zero defect by Lemma 4, page 132, we may choose hypersurfaces

$$H_{11}, H_{12}, \ldots, H_{1i}, H_{21}, H_{22}, \ldots, H_{2j}$$

which have degrees

$$\deg H_{rs} = d_r, \qquad r = 1, 2,$$

which form an M-regular sequence with respect to X, and for which

$$e(X, H_{rs}) = 0.$$

Let $H = \bigcup H_{rs}$. Then $\deg H = id_1 + jd_2$. By Lemma 7, page 136, we have the exact sheaf sequence

$$0 \to \mathcal{O}_{\bar{X} \cdot H} \to \bigoplus_{r,s} \mathcal{O}_{\bar{X} \cdot H_{rs}} \to \bigoplus_{(r,s) \neq (r',s')} \mathcal{O}_{\bar{X} \cdot H_{rs} \cdot H_{r's'}} \to 0,$$

which implies the exact cohomology sequence

$$\begin{aligned} 0 \to H^0(\mathcal{O}_{\bar{X} \cdot H}) \to \oplus H^0(\mathcal{O}_{\bar{X} \cdot H_{rs}}) \to \oplus H^0(\mathcal{O}_{\bar{X} \cdot H_{rs} \cdot H_{r's'}}) & \\ \xrightarrow{\partial} H^1(\mathcal{O}_{\bar{X} \cdot H}) \to \oplus H^1(\mathcal{O}_{\bar{X} \cdot H_{rs}}) \to 0. & \end{aligned}$$

Since we know that the Frobenius F acts bijectively on all terms except perhaps for $H^1(\mathcal{O}_{\bar{X} \cdot H})$, it follows that F must act bijectively there too. Hence

$$e(X, H) = 0,$$

and the lemma follows by Lemma 4. QED

PROOF OF 1°: Let $P \subset \mathbb{P}^*$ be any Lefschetz pencil (here $\mathbb{P}^*$ is the set of planes in $\mathbb{P}^3$). Then the hyperplane section $X \cdot H$ is a genus one stable curve if $H \in P$. In fact, the moduli space M_1 of genus one curves consists of the j-line of elliptic curves completed at infinity by a point corresponding to a rational cubic with an ordinary double point. Thus, we have a morphism

$$\psi : P \to M_1,$$

which is not constant, since the image includes both singular and nonsingular cubics. Hence ψ is surjective, and so $\psi(P)$ is not contained in the set of supersingular cubics. QED

ALTERNATE PROOF OF 1°: Since $i : X \hookrightarrow \mathbb{P}^3$ is Lefschetz, there exists a hyperplane H tangent to X such that the only singularity of $X \cdot H$ is one ordinary double point. That is, $X \cdot H$ is the nodal cubic, which is non-supersingular. QED

PROOF OF 2°: Here X is the Fermat cubic surface in characteristic 2. The assertion $X \notin I_1$ is a special case of the example on page 152 above (where $n = 2$, $p = 2$, $d = 1 \leqq \frac{1}{2}n^2 - 1$).

By Lemma 9, $X \in I_2$ follows if we find quadric and cubic sections H_2 and H_3 of X for which $\bar{X} \cdot H_2$ and $\bar{X} \cdot H_3$ have invertible Hasse-Witt. Since X has zero H^2 and so trivially $e(\mathbb{P}^3, \bar{X}) = 0$, it follows by Lemma 8, page 148, that $\bar{X} \cdot H_2$ and $\bar{X} \cdot H_3$ have invertible Hasse-Witt if and only if $\bar{X} \cup H_2$ and $\bar{X} \cup H_3$ have invertible Hasse-Witt.

First, let H_2 have equation

$$X_0 X_1 + X_2 X_3.$$

By the algorithm for computing the Hasse-Witt of a hypersurface, we must find the coefficient of X^{2w-v} in

$$(X_0^3 + X_1^3 + X_2^3 + X_3^3) \cdot (X_0 X_1 + X_2 X_3).$$

The following table gives these (w, v)-entries in the Hasse-Witt matrix of $\bar{X} \cup H_2$:

$w \diagdown v$	(1, 1, 1, 2)	(1, 1, 2, 1)	(1, 2, 1, 1)	(2, 1, 1, 1)
(1, 1, 1, 2)	0	1	0	0
(1, 1, 2, 1)	1	0	0	0
(1, 2, 1, 1)	0	0	0	1
(2, 1, 1, 1)	0	0	1	0

This is obviously an invertible matrix.

Next, let H_3 have equation

$$X_1^3 + \alpha X_2^3 + \beta X_3^3 + X_0 X_1 X_2 + X_0 X_1 X_3 + X_0 X_2 X_3 + X_1 X_2 X_3,$$

where α and β are variable coefficients. Then $\bar{X} \cup H_3$ has a Hasse-Witt matrix (see next page) whose determinant has the following leading term in (α, β): $(\alpha+\beta)\alpha^2\beta^2$. Hence, this Hasse-Witt matrix is invertible for some α, β in some algebraic extension of $\mathbb{F}_2$. This establishes 2°.

Hasse-Witt Matrix of $\bar{X} \cup H_3$

$w \diagdown v$	1113	1131	1311	3111	1122	1212	2112	1221	2121	2211
1113	1	0	0	0	1	1	1	0	0	0
1131	0	1	0	0	1	0	0	1	1	0
1311	0	0	1	0	0	1	0	1	0	1
3111	0	0	0	1	0	0	1	0	1	1
1122	1	1	0	0	0	0	0	0	0	$\alpha+\beta$
1212	1	0	1	0	0	0	0	0	$1+\beta$	0
2112	1	0	0	1	0	0	0	β	0	0
1221	0	1	1	0	0	0	$1+\alpha$	0	0	0
2121	0	1	0	1	0	α	0	0	0	0
2211	0	0	1	1	1	1	0	0	0	0

Proof of 3°: Let $d = tp+1$. Suppose $X \cdot H$ is a hyperplane section with invertible Hasse-Witt. Without loss of generality we may assume that the plane H has equation of the form

$$X_0 = aX_1+bX_2+cX_3.$$

Then the equation f of $X \cdot H$ is

$$X_1^d+X_2^d+X_3^d+(aX_1+bX_2+cX_3)^d,$$

and we are interested in the X^{pw-v} coefficient ($w, v \in \mathbb{Z}_+^3, \sum w_i = \sum v_i = d$) of

$$f^{p-1} = [X_1^{tp+1}+X_2^{tp+1}+X_3^{tp+1} \\ +(aX_1+bX_2+cX_3)(a^pX_1^p+b^pX_2^p+c^pX_3^p)^t]^{p-1}.$$

Let

$$T_i = X_i^{tp+1}, \qquad i = 1, 2, 3$$
$$T_4 = aX_1+bX_2+cX_3$$
$$T_5 = (a^pX_1^p+b^pX_2^p+c^pX_3^p)^t,$$

so that

$$\begin{aligned} f^{p-1} &= (T_1+T_2+T_3+T_4\cdot T_5)^{p-1} \\ &= \sum_{r_1+r_2+r_3+r_4=p-1} \frac{(p-1)!}{r_1!r_2!r_3!r_4!} T_1^{r_1}T_2^{r_2}T_3^{r_3}T_4^{r_4}T_5^{r_4} \\ &= \sum_{\substack{r_1+r_2+r_3+r_4=p-1 \\ s_1+s_2+s_3=r_4}} (\text{term with no } X_i)\; T_1^{r_1}T_2^{r_2}T_3^{r_3}T_5^{r_4}X_1^{s_1}X_2^{s_2}X_3^{s_3}. \end{aligned}$$

In the Hasse-Witt matrix choose any v-column for which the sum of the least positive residues mod p of $-v_i$ (which we denote $\{-v_i\}$) is at least p. This is clearly possible (e.g., $v = (1, 1, d-2)$). Let v_0 be such a v. If a term in the above summation with indices $r_1, r_2, r_3, r_4, s_1, s_2, s_3$ contributes to the coefficient of X^{pw-v_0} for any w, then we must have the mod p relations

$$-v_i \equiv r_i+s_i, \qquad i = 1, 2, 3.$$

But then

$$\sum_{i=1}^{3}\{-v_i\} = \sum_{i=1}^{3}(r_i+s_i) = \sum_{i=1}^{4} r_i = p-1,$$

a contradiction. Hence the v_0-column is identically zero. This proves 3°.

PROOF OF 4°: 4° is trivial for $d = 1, 2$ and is a special case of 1° for $d = 3$.

Suppose $d = 4$. If $p \equiv 1 \pmod 4$, then the Fermat curve

$$X_1^4+X_2^4+X_3^4 = 0$$

has invertible Hasse-Witt, so we need only take the plane section $X_0 = 0$ to show $X \in I_1$. Suppose $p = 4t+3$, $t \in \mathbb{Z}_+$ (by assumption $p \neq 2, 3$).

Consider the section given by $X_0 = aX_1+bX_2+cX_3$. This section has Hasse-Witt matrix with (w, v)-entry ($w, v \in \mathbb{Z}_+^3$, $\sum w_i = \sum v_i = 4$) equal to the coefficient of X^{pw-v} in

$$f^{p-1} = (X_1^4+X_2^4+X_3^4+(aX_1+bX_2+cX_3)^4)^{p-1}.$$

We first make a table of the vectors $pw-v$ as w, v run over the triples $(1, 1, 2)$, $(1, 2, 1)$, $(2, 1, 1)$:

$w \backslash v$	(1, 1, 2)	(1, 2, 1)	(2, 1, 1)
(1, 1, 2)	$(4t+2, 4t+2, 8t+4)$	$(4t+2, 4t+1, 8t+5)$	$(4t+1, 4t+2, 8t+5)$
(1, 2, 1)	$(4t+2, 8t+5, 4t+1)$	$(4t+2, 8t+4, 4t+2)$	$(4t+1, 8t+5, 4t+2)$
(2, 1, 1)	$(8t+5, 4t+2, 4t+1)$	$(8t+5, 4t+1, 4t+2)$	$(8t+4, 4t+2, 4t+2)$

Considering the coefficient of X^{pw-v} as a polynomial in a, b, c, we take only the monomial in each entry with the *least* total degree in a, b, c:

$w \backslash v$	(1, 1, 2)	(1, 2, 1)	(2, 1, 1)
(1, 1, 2)	$\dfrac{(p-1)!}{t!t!(t+1)!}\cdot 6a^2b^2$	$\dfrac{(p-1)!}{t!t!(t+1)!}\cdot 12a^2bc$	$\dfrac{(p-1)!}{t!t!(t+1)!}\cdot 12ab^2c$
(1, 2, 1)	$\dfrac{(p-1)!}{t!(t+1)!t!}\cdot 12a^2bc$	$\dfrac{(p-1)!}{t!(t+1)!t!}\cdot 6a^2c^2$	$\dfrac{(p-1)!}{t!(t+1)!t!}\cdot 12abc^2$
(2, 1, 1)	$\dfrac{(p-1)!}{(t+1)!t!t!}\cdot 12ab^2c$	$\dfrac{(p-1)!}{(t+1)!t!t!}\cdot 12abc^2$	$\dfrac{(p-1)!}{(t+1)!t!t!}\cdot 6b^2c^2$

The determinant of the Hasse-Witt matrix, as a polynomial in a, b, c, then has lowest degree term equal to

$$a^4b^4c^4\left(\frac{(p-1)!}{t!t!(t+1)!}\right)^3 6^3 \det \begin{bmatrix} 1 & 2 & 2 \\ 2 & 1 & 2 \\ 2 & 2 & 1 \end{bmatrix} = 5\cdot 6^3 \frac{(p-1)!^3}{t!^6(t+1)!^3} a^4b^4c^4,$$

which is nonzero because $p \geqq 7$. Hence the determinant is generically nonzero.

Suppose $d = 5$. If $p \equiv 1 \pmod 5$, we may take the coordinate plane section $X_0 = 0$ as before. Suppose $p = 5t+2$, $t \in \mathbb{Z}_+$ (by assumption $p \neq 2, 5$). As before, we consider the $pw-v$ coefficient in

$$f^{p-1} = (X_1^5+X_2^5+X_3^5+(aX_1+bX_2+cX_3)^5)^{p-1}$$

as polynomials in a, b, c and we isolate the lowest degree term.

We index the w, v as follows:

$$w^{(1)} = v^{(1)} = (1, 1, 3); \qquad w^{(4)} = v^{(4)} = (1, 2, 2);$$

$$w^{(2)} = v^{(2)} = (1, 3, 1); \qquad w^{(5)} = v^{(5)} = (2, 1, 2);$$

$$w^{(3)} = v^{(3)} = (3, 1, 1); \qquad w^{(6)} = v^{(6)} = (2, 2, 1).$$

We first find the (w, v)-entries which have a constant term (i.e., with no a, b, c). It is evident from the equation of f^{p-1} that the (w, v)-entry has a constant term if and only if

$$pw - v \equiv 0 \pmod 5 \Leftrightarrow v \equiv 2w \pmod 5 \Leftrightarrow (w, v) = \begin{matrix} (w^{(1)}, v^{(6)}); \\ (w^{(2)}, v^{(5)}); \\ (w^{(3)}, v^{(4)}). \end{matrix}$$

That is, these constant terms – which turn out to equal

$$\frac{(p-1)!}{t!t!(3t+1)!} \neq 0$$

– are located on the upper half of the antidiagonal of the 6×6 Hasse-Witt matrix. Hence, to show the non-vanishing of the first coefficient in the determinant it suffices to consider the first coefficient in the determinant of the lower-left hand 3×3 sub-matrix. The lowest degree term in a, b, c in the determinant of this 3×3 matrix is easily computed. It equals

$$20^3 \frac{(p-1)!^3}{t!^3(2t)!^6} a^5 b^5 c^5 \det \begin{bmatrix} 1 & 1 & 0 \\ 1 & 0 & 1 \\ 0 & 1 & 1 \end{bmatrix} = -2 \cdot 20^3 \frac{(p-1)!^3}{t!^3(2t)!^6} a^5 b^5 c^5$$

which is nonzero because $p \geqq 7$.

The computations are analogous if $d = 5$ and $p \equiv 3$ or $4 \pmod 5$. In the case $p \equiv 4 \pmod 5$ there are no (w, v)-entries with constant term, so the whole 6×6 matrix must be considered. We omit the details.

Finally, let $d = 6$. The case $p \equiv 1 \pmod 6$ can be handled, as always, by taking a coordinate plane section $X_0 = 0$. Since $p \neq 2, 3, 5$ by assumption, this leaves the case $p = 6t + 5$, $t \in \mathbb{Z}_+$. Since there are no (w, v)-entries with constant term, we must consider an entire 10×10 matrix of terms of total degree 6 in a, b, c. (10 = genus = $\frac{1}{2}(6-1)(6-2)$.) We find that this determinant can be immediately factored into the product of a term which is nonzero when $p \nmid d$, $p \nmid (d-1)$ (this term is

$$\frac{p-1!^{10}}{t!^{12}(2t+1)!^9(3t+2)!^6(4t+3)!^3} 5^{10} a^{20} b^{20} c^{20})$$

and the following determinant:

$$\det \begin{bmatrix} 0 & 6 & 6 & 0 & 3 & 0 & 12 & 3 & 12 & 4 \\ 6 & 0 & 6 & 3 & 0 & 12 & 0 & 12 & 3 & 4 \\ 6 & 6 & 0 & 12 & 12 & 3 & 3 & 0 & 0 & 4 \\ 0 & 3 & 12 & 3 & 6 & 4 & 12 & 12 & 18 & 12 \\ 3 & 0 & 12 & 6 & 3 & 12 & 4 & 18 & 12 & 12 \\ 0 & 12 & 3 & 4 & 12 & 3 & 18 & 6 & 12 & 12 \\ 12 & 0 & 3 & 12 & 4 & 18 & 3 & 12 & 6 & 12 \\ 3 & 12 & 0 & 12 & 18 & 6 & 12 & 3 & 4 & 12 \\ 12 & 3 & 0 & 18 & 12 & 12 & 6 & 4 & 3 & 12 \\ 4 & 4 & 4 & 12 & 12 & 12 & 12 & 12 & 12 & 18 \end{bmatrix} = 2^4 \cdot 3^3 \cdot 7^6.$$

This determinant is also nonzero for $p = 6t+5, t \in \mathbb{Z}_+$. Hence the Hasse-Witt matrix is generically invertible in this case as well, and 4° is proved.

IV. p-rRank stratification of principally polarized abelian varieties

1. *Basic set-up*

Let (A, λ) be a g-dimensional principally polarized abelian variety defined over an algebraically closed field k of characteristic $p > 0$, where

$$\lambda : A \xrightarrow{\sim} \hat{A}$$

is the polarization, which identifies A with its dual $\hat{A}$. Following Oort [50], we define the *p-rank* r_s of A to be the stable rank of the Hasse-Witt matrix of A:

$$r_s(A) = \dim H^1(\mathcal{O}_A)_{ss} = \dim \operatorname{im} F^n|H^1(\mathcal{O}_A), \qquad n \gg 0,$$

where F is the Frobenius. We define the *rank* r of A to be the rank of the Hasse-Witt matrix:

$$r(A) = \dim \operatorname{im} F|H^1(\mathcal{O}_A).$$

We are interested in the stratification of the $\frac{1}{2}g(g+1)$-dimensional moduli space M_g of g-dimensional principally polarized abelian varieties over k according to the p-rank r_s. More precisely, for $N \geqq 3$ prime to p, we consider principally polarized abelian varieties A together with a 'level N' structure, i.e., an isomorphism

$$\pi : (\mathbb{Z}/N\mathbb{Z})^{2g} \xrightarrow{\sim} {}_NA,$$

where ${}_NA$ is the group of points of order N on A, such that

$$\det(\langle \pi(\delta_i), \lambda \circ \pi(\delta_j)\rangle) = 1,$$

where the $\delta_i = (0, \ldots, 0, 1, 0, \ldots, 0)$ are canonical generators of $(\mathbb{Z}/N\mathbb{Z})^{2g}$, and $\langle , \rangle$ is the e_N-pairing on ${}_NA \times {}_N\hat{A}$. By Mumford, [43], Theorem 7.9, the functor of principally polarized abelian schemes over k-schemes with a level N structure is representable by a fine moduli scheme $M_g^{(N)}$ over k. (In [43], the proof is for $N > 6^g\sqrt{g!}$, and it is remarked that the fine moduli scheme exists for $N \geqq 3$.) We further claim that $M_g^{(N)}$ is smooth over k. In fact, since this is a local question and $M_g^{(N)}$ $(p \nmid N)$ is étale over the moduli stack M_g of principally polarized abelian varieties over k-schemes (without level), it is sufficient to show that M_g is smooth. But M_g is smooth because the functor of principally polarized abelian schemes is formally smooth (cf. Oort, [49], p. 244–246).

Thus, let $f : A_g^{(N)} \to M_g^{(N)}$ be the universal family of g-dimensional principally polarized abelian varieties over k with level N structure. Since f is flat and proper, and $\dim_k H^1(A_{g,y}^{(N)}, \mathcal{O}_{A_{g,y}^{(N)}})$ is constant at all closed points $y \in M_g^{(N)}$, it follows by the base-changing theorems (cf. [42], p. 51) that $R^1(f_* \mathcal{O}_{A_g^{(N)}})$ is a locally free sheaf $\mathscr{E}$ on $M_g^{(N)}$ and that for all $y \in M_g^{(N)}$

$$\mathscr{E} \otimes \mathcal{O}_{M_g^{(N)}} k(y) \xrightarrow{\sim} H^1(A_{g,y}^{(N)}, \mathcal{O}_{A_{g,y}^{(N)}}).$$

Let m and n be any positive integers, and let F be the p-linear Frobenius endomorphism on $\mathscr{E} = R^1(f_* \mathcal{O}_{A_g^{(N)}})$. Let $F_{n,m}$ be the (p^n-linear) endomorphism induced by F^n on $\bigwedge^m \mathscr{E}$ ('matrix of minors'). If we choose an affine open set $\operatorname{Spec} B \subset M_g^{(N)}$ over which

$$\mathscr{E} \approx \tilde{B}^g$$

is free, then $F_{n,m}$ can be given by a matrix with entries in B. In particular, the condition $F_{n,m} \equiv 0$ (identically) defines a closed subscheme of $\operatorname{Spec} B$. Thus, let $S_{n,m}^{(N)}$ be the closed subscheme of $M_g^{(N)}$ defined by the condition $F_{n,m} \equiv 0$.

We first describe in terms of the $S_{n,m}^{(N)}$ the set of abelian varieties (i.e., closed points $A \in M_g^{(N)}$) for which $r_s(A) \leqq r_s$. Suppose $r_s < g$. Let $V = H^1(\mathcal{O}_A)$. Notice that dim im $F^i|_V$ is strictly decreasing as $i = 1, 2, \ldots$ until this dimension reaches $r_s(A)$ (cf. proof of Lemma 3, p. 131). Since dim im $F|_V \leqq g-1$, this means that

$$\begin{aligned} r_s(A) \leqq r_s &\Leftrightarrow \dim \operatorname{im} F^{g-r_s}|_V \leqq r_s \\ &\Leftrightarrow F^{g-r_s}|_{\wedge^{r_s+1}V} \equiv 0 \\ &\Leftrightarrow A \in S_{g-r_s, r_s+1} \end{aligned}$$

Thus, the abelian varieties $A \in M_g^{(N)}$ for which $r_s(A) \leqq r_s$ are the closed points of

$$M_{g;r_s}^{(N)} \underset{\text{def}}{=} (S_{g-r_s,r_s+1}^{(N)})_{\text{red}}.$$

We similarly describe the set of abelian varieties $A \in M_g^{(N)}$ for which $r_s(A) \leqq r_s$ and $r(A) \leqq r$. The condition $r(A) \leqq r$ is clearly equivalent to

$$A \in S_{1,r+1}^{(N)}.$$

If $r(A) \leqq r$, then $r_s(A) \leqq r_s$ if and only if $\dim \operatorname{im} F^{r-r_s+1}|_V \leqq r_s$, i.e., if and only if

$$A \in S_{r-r_s+1,r_s+1}^{(N)}.$$

Thus, the abelian varieties $A \in M_g^{(N)}$ for which $r(A) \leqq r$ and $r_s(A) \leqq r_s$ are the closed points of

$$M_{g;r_s;r}^{(N)} \underset{\text{def}}{=} (S_{1,r+1}^{(N)})_{\text{red}} \cap (S_{r-r_s+1,r_s+1}^{(N)})_{\text{red}}.$$

For later use, we further classify $A \in M_{g;r_s;r}^{(N)}$ according to the least $i = 0, 1, \ldots, r-r_s$ such that $\dim \operatorname{im} F^{i+1}|_V \leqq r_s$. That is, we write $M_{g;r_s;r}^{(N)}$ in terms of a disjoint union:

$$M_{g;r_s;r}^{(N)} = (S_{1,r+1}^{(N)})_{\text{red}} \cap \Big[(S_{1,r_s+1}^{(N)})_{\text{red}} \underset{\text{disj}}{\bigcup} \underset{\text{disj}}{\bigcup}{}_{i=1}^{r-r_s} (S_{i+1,r_s+1}^{(N)} - S_{i,r_s+1}^{(N)})_{\text{red}}\Big].$$

The goal of this chapter is to prove:

THEOREM 7: *Let $M_g^{(N)}$ ($N \geqq 3, p \nmid N$) be the fine moduli scheme of g-dimensional principally polarized abelian varieties with level N structure over an algebraically closed field of characteristic $p > 0$. For $0 \leqq r_s \leqq g$, let $M_{g;r_s}^{(N)}$ be the closed subset of $M_g^{(N)}$ of abelian varieties of p-rank $\leqq r_s$. Then:*

(1) *Each component of $M_{g;r_s}^{(N)}$ has codimension $g-r_s$ in $M_g^{(N)}$.*

(2) *If $r_s < g$, then the locally closed set of abelian varieties in $M_{g;r_s}^{(N)}$ whose Hasse-Witt matrix has rank $g-1$ is Zariski dense in $M_{g;r_s}^{(N)}$.*

(3) $M^{(N)}_{g;r_s}$ *is smooth at those abelian varieties whose Hasse-Witt matrix has stable rank* $\leqq r_s$ *and rank equal to* $g-1$.

REMARK: It seems reasonable to conjecture that part (3) of Theorem 7 is precise in the sense that $M^{(N)}_{g;r_s}$ is singular at abelian varieties whose Hasse-Witt matrix has rank $\leqq g-2$.

2. *Outline of proof of Theorem* 7

A key element in the proof is the upper bound for the codimension of the set $M^{(N)}_{g;r_s}$ that is provided by the following result of Oort (cf. [50], Lemma 1.6): Let S be an irreducible algebraic k-scheme, and let $X \to S$ be an abelian scheme over S; let f be the p-rank of the generic fibre; and let W be the closed subset of S over which the fibre has p-rank at most $f-1$. Then either W is empty or each component of W has codimension one in S.

We first note that the product of g supersingular elliptic curves has p-rank zero, so that all the sets $M^{(N)}_{g;r_s}$ are nonempty. Fix $r_s < g$. Let C_{r_s} be any irreducible component of $M^{(N)}_{g;r_s}$. Let $C_{r_s+1} \supseteq C_{r_s}$ be the unique irreducible component of $M^{(N)}_{g;r_s+1}$ which contains C_{r_s}. Note that *a priori* C_{r_s+1} could equal C_{r_s}. In this manner we obtain $C_{r_s} \subseteq C_{r_s+1} \subseteq \ldots \subseteq C_g$. For $r' = r_s, r_s+1, \ldots, g-1$, Oort's result tells us that, if the p-rank of the generic fibre of $C_{r'+1}$ is *strictly* greater than the p-rank of the generic fibre of $C_{r'}$, i.e., if $C_{r'} \neq C_{r'+1}$, then it follows that $C_{r'}$ has codimension one in $C_{r'+1}$. This implies that the codimension of C_{r_s} in $M^{(N)}_g$ is $\leqq g-r_s$.

To obtain the opposite inequality we prove two lemmas:

LEMMA 10: *If* $A \in M^{(N)}_g$, $r_s(A) < g$, $r(A) = g-1$, *and* $r_s(A) \leqq r' \leqq g$, *then the Zariski tangent space to* $M^{(N)}_{g;r'}$ *at* A *has codimension* $\geqq g-r'$ *in the tangent space to* $M^{(N)}_g$ *at* A.

LEMMA 11: *Let* $A \in M^{(N)}_g$, $r(A) = g-h$, $h > 1$, *and* $r_s = r_s(A)$. *Suppose that* A *is in the set* $S = S^{(N)}_{1,g-h+1} \cap (S^{(N)}_{i+1,r_s+1} - S^{(N)}_{i,r_s+1})$ *in the expression for* $M^{(N)}_{g;r_s;g-h}$ *on* p. 163 (*where if* $i = 0$ *we take* $S^{(N)}_{0,r_s+1} = \emptyset$). *Then the Zariski tangent space to* S *at* A *has codimension* $> g-r_s$ *in the tangent space to* $M^{(N)}_g$ *at* A.

Theorem 7 is easily proved using Lemmas 10 and 11 and Oort's upper bound on the codimensions. In fact, by Lemma 11 and the smoothness of $M^{(N)}_g$, it follows that $M^{(N)}_{g;r';g-2}$ is a union of sets all having codimension $> g-r'$. Hence, if we define

$$C_{r',g-1} = C_{r'} - (C_{r'} \cap M^{(N)}_{g;r';g-2}),$$

then $C_{r',g-1}$ is Zariski dense in $C_{r'}$. Let $A \in C_{r',g-1}$. By Lemma 10, locally at A the set $C_{r'}$ has codimension $\geqq g-r'$. But then Oort's result implies that $C_{r'}$ has codimension $= g-r'$. This proves parts (1) and (2) of Theorem 7. Part (3) now follows because at $A \in C_{r',g-1}$ the codimension of the Zariski tangent space to $C_{r'}$ in the tangent space to the smooth scheme $M_g^{(N)}$ is the same as the codimension of $C_{r'}$ in $M_g^{(N)}$.

Since we shall henceforth be dealing exclusively with local questions, we shall suppress the level N structure, writing M_g, $M_{g;r_s}$, $M_{g;r_s;r}$, $S_{n,m}$ in place of $M_g^{(N)}$, $M_{g;r_s}^{(N)}$, $M_{g;r_s;r}^{(N)}$, $S_{n,m}^{(N)}$. This is permissible because the functor of *infinitesimal* deformations of $A \in M_g^{(N)}$ as principally polarized abelian variety with level N structure is canonically isomorphic to the functor of deformations of A as principally polarized abelian variety without level.

Moreover, we know by a theorem of Grothendieck and Mumford (cf. Oort, [49], p. 244–246) that this deformation functor is *effectively* pro-representable by

$$k[[m_{t,\mathrm{Symm}}]] \underset{\mathrm{def}}{=} k[[\{t_{ij}\}_{i,j=1}^{g}]]/(\{t_{ij}-t_{ji}\}).$$

That is, there exists an abelian scheme over $k[[m_{t,\mathrm{Symm}}]]$ such that for any artinian local k-algebra R with an isomorphism $k \approx R/m_R$, an element

$$f \in \mathrm{Hom}\,(k[[m_{t,\mathrm{Symm}}]], R)$$

corresponds to the deformation $A_f = A_t \otimes_{k[[m_{t,\mathrm{Symm}}]]} \underset{f}{\rightarrow} R$ of A over R.

$$\begin{array}{ccc} A_f & \longrightarrow & A_t \\ \big\downarrow & & \big\downarrow \\ \mathrm{Spec}\, R & \longrightarrow & \mathrm{Spec}\, k[[m_{t,\mathrm{Symm}}]] \end{array}$$

In particular, the expression we shall derive for the Hasse-Witt matrix of a deformation of A over the dual numbers $k[\varepsilon]/\varepsilon^2$ will also give us the Hasse-Witt matrix of A_t modulo the square of the maximal ideal $m_{t,\mathrm{Symm}}$ of $k[[m_{t,\mathrm{Symm}}]]$.

The basic tool needed to prove Lemmas 10 and 11 is

LEMMA 12: (1) *The functor of deformations of A as principally polarized abelian variety over artinian local rings is formally smooth and effectively pro-representable by*

$$k[[\text{Symm Hom}\,(H^0(\Omega_A^1), H^1(\mathcal{O}_A))]].$$

Here 'Symm Hom' *means that if we choose dual bases* ω_i, η_j *of* $H^0(\Omega_A^1)$, $H^1(\mathcal{O}_A)$, *respectively, with respect to the polarization form given by*

$$H^1(\mathcal{O}_A) \approx tg_{\hat{A}} \overset{\lambda^{-1}}{\approx} tg_A = \text{Hom}\,(H^0(\Omega_A^1), k)$$

('tg' *means tangent space at the origin*), *then* 'Symm Hom' *corresponds to symmetric matrices in these bases. Thus, the* t_{ij} *in* $k[[\{t_{ij}\}]]/(\{t_{ij}-t_{ji}\})$ *may be identified with the map from* $H^0(\Omega_A^1)$ *to* $H^1(\mathcal{O}_A)$ *taking* $\omega_i \mapsto \eta_j$, $\omega_{i'} \mapsto 0$ *if* $i' \neq i$.

(2) *The deformation over* $k[\varepsilon]/\varepsilon^2$ *corresponding to the homomorphism* $t_{ij} \mapsto u_{ij}\varepsilon$ *has Hasse-Witt matrix*

$$H_u = H - \varepsilon U B,$$

where H *and* B *are* $g \times g$ *matrices,* H *is the Hasse-Witt matrix of* A *and* $U = \{u_{ij}\}$.

(3) *The* $2g \times g$ *matrix* $\binom{B}{H}$ *has rank* g.

Sections 3–7 below are devoted to proving Lemma 12. In sections 8–9 we prove Lemmas 10 and 11. Sections 10–11 discuss two further applications of Lemma 12.

The idea of using a deformation theoretic approach to prove Theorem 7 is due to P. Deligne.

3. *Deformations*

Let (A, λ), $\lambda : A \xrightarrow{\sim} \hat{A}$, be a fixed principally polarized abelian variety. We want to know how A deforms (1) as abelian variety, and (2) as principally polarized abelian variety.

Let $\tilde{\mathscr{C}}_k$ be the category of artinian local k-algebras R together with an isomorphism $k \approx R/m_R$. Define a functor $\tilde{D}_{AV}$ from $\tilde{\mathscr{C}}_k$ to Sets by

$$\tilde{D}_{AV}(R) = \left\{\begin{array}{c}\text{isomorphism classes of pairs } (A', \varphi_0)\text{, where } A' \\ \text{is an abelian scheme over } R\text{, and } \varphi_0 : A' \otimes_R k \xrightarrow{\sim} A\end{array}\right\}$$

Let $\mathscr{C}_k$ be the full subcategory of $\tilde{\mathscr{C}}_k$ whose objects R have $m_R^2 = 0$. We note that

$$R \rightsquigarrow m_R$$

gives an equivalence of categories between $\mathscr{C}_k$ and the category of finite dimensional k-vector spaces (with linear homomorphisms). Let $D_{AV}: \mathscr{C}_k \rightsquigarrow$ Sets be the restriction of the functor $\tilde{D}_{AV}$ to $\mathscr{C}_k$.

A theorem of Grothendieck (cf. Oort, [49], p. 231) tells us that the functor $\tilde{D}_{AV}$ is pro-representable by $k[[\{t_{ij}\}_{i,j=1}^g]]$. It then follows that, if m_t is the ideal generated by the t_{ij}, and

$$k[m_t] \underset{\text{def}}{=} k[\{t_{ij}\}_{i,j=1}^g],$$

then D_{AV} is representable by $k[m_t]/m_t^2$.

We recall the explicit construction of the isomorphism

$$D_{AV}(R) \to \operatorname{Hom}(k[m_t]/m_t^2, R)$$

for R in $\mathscr{C}_k$. Let m_ε denote the dual vector space of m_t. Then canonically

$$\operatorname{Hom}(k[m_t]/m_t^2, R) \approx \operatorname{Hom}_{\text{vec sp}}(m_t, m_R) \approx m_\varepsilon \otimes m_R.$$

Let $(A', \varphi_0) \in D_{AV}(R)$.

$$\begin{array}{ccc} A' & \longrightarrow & A \\ \downarrow & & \downarrow \\ \operatorname{Spec} R & \longrightarrow & \operatorname{Spec} k \end{array}$$

Consider an open affine covering $\{U_i\}$ of A, $U_i = \operatorname{Spec} B_i$. Let

$$B_{ij} = B_i|_{U_{ij}} = B_j|_{U_{ij}}, \qquad U_{ij} = U_i \cap U_j.$$

Then A' has an affine open covering by $U_i' \approx \operatorname{Spec} B_i[m_R]/m_R^2$. Then on $U_{ij}' = U_i' \cap U_j'$ we have patching isomorphisms

$$\varphi_{ij}: B_{ij}[m_R]/m_R^2 \xrightarrow{\sim} B_{ij}[m_R]/m_R^2$$

such that $\varphi_{ij} \otimes_R \mathrm{k} = 1_{B_{ij}}$. Hence φ_{ij} induces a map $\gamma_{ij} = (\varphi_{ij} - 1)|B_{ij}$ of B_{ij}:

$$(\varphi_{ij} - 1): B_{ij} \to m_R,$$

where $\gamma_{ij} \in \operatorname{Der}_k(B_{ij}, B_{ij}) \otimes m_R$, i.e., φ_{ij} determines a section of $\theta_A \otimes m_R$ over U_{ij}. It is easy to see that the φ_{ij} determine a 1-cocycle, which is uniquely determined by the deformation modulo 1-coboundaries. Hence, the deformations in $D_{AV}(R)$ are given by elements in

$$H^1(A, \theta_A \otimes m_R) \approx H^1(A, \theta_A) \otimes m_R.$$

Now the Kodaira-Spencer map from $H^1(A, \theta_A) \times H^0(\Omega_A^1)$ to $H^1(\mathcal{O}_A)$ is defined by taking a 1-cocycle $\{\gamma_{ij}\}$ representing a class in $H^1(A, \theta_A)$ and an element $\omega \in H^0(\Omega_A^1)$ to the class in $H^1(\mathcal{O}_A)$ of the 1-cocycle $\{f_{ij}\}$, where $f_{ij} = \langle \gamma_{ij}, \omega \rangle$ is obtained by evaluating the differential ω (restricted to U_{ij}) at the derivation γ_{ij}. This Kodaira-Spencer map then gives a canonical isomorphism

$$H^1(A, \theta_A) \xrightarrow{\sim} \operatorname{Hom}(H^0(\Omega_A^1), H^1(\mathcal{O}_A)).$$

Then the map

$$D_{AV}(R) \to \operatorname{Hom}(k[m_t]/m_t^2, R) \approx m_\varepsilon \otimes m_R$$

is given by assigning to any deformation the corresponding class in

$$\begin{aligned} H^1(A, \theta_A) \otimes m_R &\xrightarrow{\sim} \operatorname{Hom}(H^0(\Omega_A^1), H^1(\mathcal{O}_A)) \otimes m_R \\ &\approx \operatorname{Hom}(ctg_A, tg_{\hat{A}}) \otimes m_R \\ &\approx (tg_A \otimes tg_{\hat{A}}) \otimes m_R, \end{aligned}$$

where '*tg*' (resp. '*ctg*') denotes tangent space (resp. cotangent space) at the origin. That is, the vector space m_t in the above assertion is identified as the dual of the g^2-dimensional vector space $tg_A \otimes tg_{\hat{A}}$:

$$m_t \approx (tg_A \otimes tg_{\hat{A}})\hat{} \approx ctg_A \otimes ctg_{\hat{A}}.$$

Since the polarization λ induces $d\lambda\colon tg_A \xrightarrow{\sim} tg_{\hat{A}}$, we may take

$$\begin{aligned} m_\varepsilon &= tg_A \otimes tg_A; \\ m_t &= ctg_A \otimes ctg_A. \end{aligned}$$

We define the functor $\tilde{D}_{PPAV} : \tilde{\mathscr{C}}_k \rightsquigarrow \text{Sets}$ by

$$\tilde{D}_{PPAV}(R) = \left\{ \begin{array}{c} \text{isomorphism classes of } (A', \lambda', \varphi_0), \text{ where } (A', \lambda') \\ \text{is a principally polarized abelian scheme over } R, \\ \text{and where } \varphi_0 : (A', \lambda') \otimes_R k \xrightarrow{\sim} (A, \lambda) \end{array} \right\}.$$

Let $D_{PPAV} : \mathscr{C}_k \rightsquigarrow$ Sets be the restriction of $\tilde{D}_{PPAV}$ to $\mathscr{C}_k$.

4. *'Rigidity' of H^1_{DR}.*

Let R be an object of $\tilde{\mathscr{C}}_k$, and let $A' \in \tilde{D}_{AV}(R)$. The i-th De Rham cohomology along the fibres of the family

$$\begin{array}{ccc} A' & \longrightarrow & A \\ \downarrow & & \downarrow \\ \operatorname{Spec} R & \longrightarrow & \operatorname{Spec} k \end{array}$$

has a canonical integrable connection $\nabla_{A'}$, the Gauss-Manin connection:

$$\nabla_{A'} : H^i_{DR}(A') \to \Omega^1_{R/k} \otimes H^i_{DR}(A').$$

Thus, $\nabla_{A'}$ gives an action of any $d \in Der_k(R, R)$ on $H^i_{DR}(A')$. Following Katz (unpublished notes), we use this structure to give an elementary proof of freeness, base-changing, and degeneration of the Hodge $\Rightarrow$ De Rham spectral sequence for $H^i_{DR}(A')$ over a 'small enough' artinian local ring (cf. Sublemma 7), and to construct a projection operator $P \in \operatorname{End}_k H^i_{DR}(A')$ which will explicitly give us a convenient basis of $H^1_{DR}(A')$ for computing the infinitesimal behavior of the Frobenius F on $H^1_{DR}(A')$.

SUBLEMMA 1: *Let R_0 be any ring of characteristic p, let*

$$R_n = R_0[T_1, \ldots, T_n]/(T_1^p, \ldots, T_n^p),$$

and let M be an R_n-module with a (not necessarily integrable) connection

$$\nabla : Der_{R_0}(R_n, R_n) \to \operatorname{End}_{R_0} M.$$

If $M/(T_1, \ldots, T_n)M$ is flat over R_0, then M is flat over R_n.

PROOF: We first prove the sublemma for $n = 1$, i.e., $T = T_1$, $R = R_1 = R_0[T]/T^p$. By [13], Exp. IV, Corollary 5.5, M is flat over R if and only if M/TM is flat over R_0 and $\operatorname{Tor}_1^R(M, R_0) = 0$. Now R_0 has a free resolution as R-module

$$\ldots \overset{xT}{\to} R \xrightarrow{xT^{p-1}} R \overset{xT}{\to} R \to R_0 \to 0.$$

Hence:

$$\operatorname{Tor}_1^R(M, R_0) = \operatorname{Ker}(M \overset{xT}{\to} M)/T^{p-1}M.$$

Let $Tm = 0$, $m \in M$. We must show that $m \in T^{p-1}M$. Since

$$\frac{\partial}{\partial T} \in \mathrm{Der}_{R_0}(R, R),$$

we have

$$\nabla\left(\frac{\partial}{\partial T}\right) \in \mathrm{End}_{R_0} M.$$

Let $m_0 = m$, and let

$$m_r \underset{\mathrm{def}}{=} -\nabla\left(\frac{\partial}{\partial T}\right)(m_{r-1}), \qquad r = 1, 2, \ldots, p-1.$$

We prove by induction that $m = (1/r!)T^r m_r$. This is trivial for $r = 0$. Suppose

$$m = \frac{1}{(r-1)!} T^{r-1} m_{r-1}.$$

Then $T^r m_{r-1} = (r-1)!Tm = 0$, so that

$$\begin{aligned} 0 &= \frac{1}{r!}\nabla\left(\frac{\partial}{\lambda T}\right)(T^r m_{r-1}) \\ &= \frac{1}{r!} T^r \nabla\left(\frac{\partial}{\partial T}\right)(m_{r-1}) + \frac{1}{(r-1)!} T^{r-1} m_{r-1} \\ &= -\frac{1}{r!} T^r m_r + m, \end{aligned}$$

as claimed. Letting $r = p-1$ concludes the proof of the sublemma for $n = 1$.

We now use induction on n. Suppose the sublemma holds for $1, 2, \ldots, n-1$. Note that $\mathrm{Der}_{R_0}(R_n, R_n)$ is the free R_n-module

$$\sum_{i=1}^{n} R_n \frac{\partial}{\partial T_i},$$

and thus that we have a natural inclusion

$$\mathrm{Der}_{R_0}(R_{n-1}, R_{n-1}) \hookrightarrow \mathrm{Der}_{R_0}(R_n, R_n).$$

Thus, ∇ induces a connection on M as R_{n-1}-module. Moreover, for any $i = 1, 2, \ldots, n-1$ and for any $m \in M$ we have

$$\left(\nabla\left(\frac{\partial}{\partial T_i}\right)\right)(T_n m) = T_n \nabla\left(\frac{\partial}{\partial T_i}\right)(m),$$

since $\partial T_n/\partial T_i = 0$. Hence, for all $d \in \mathrm{Der}_{R_0}(R_{n-1}, R_{n-1})$ the endomorphism $\nabla(d)$ respects the ideal $T_n M$, and so factors through $\mathrm{End}_{R_0}(M/T_n M)$. Thus, $M/T_n M$ has a connection, and the induction assumption applies. It follows that $M/T_n M$ is flat over R_{n-1}. Since $R_n = R_{n-1}[T_n]/T_n^p$, and since ∇ restricted to $R_n(\partial/\partial T_n)$ gives an R_{n-1}-connection on M, we are now in the situation of the sublemma for $n = 1$, with R_{n-1} in place of R_0. We conclude that M is flat over R_n. QED

In our application, $R_0 = k$,

$$R_n = k[T_1, \ldots, T_n]/(T_1^p, \ldots, T_n^p),$$

$A' \in \tilde{D}_{AV}(R_n)$, $M = H^i_{DR}(A')$, $\nabla = \nabla_{A'}$. First note that, since k is a field, the assumptions of Sublemma 1 all hold, and M is flat over R_n. For any change of base $R_n \to S$ we have

$$H^i_{DR}(A' \underset{R_n}{\otimes} S) \approx H^i_{DR}(A') \underset{R_n}{\otimes} S;$$

This follows because of the flatness of the De Rham complex and the flatness of its cohomology groups $H^i_{DR}(A')$. Thus:

SUBLEMMA 2: *If $A' \in \tilde{D}_{AV}(R_n)$, where $R_n = k[T_1, \ldots, T_n]/(T_1^p, \ldots, T_n^p)$, then for arbitrary change of base $R_n \to S$*

$$H^i_{DR}(A' \underset{R_n}{\otimes} S) \approx H^i_{DR}(A') \underset{R_n}{\otimes} S.$$

In particular, letting $S = k$, we have

$$H^i_{DR}(A) \approx H^i_{DR}(A')/(T_1, \ldots, T_n)H^i_{DR}(A').$$

SUBLEMMA 3: *Let R_0, R_n, M be as in Sublemma 1, with $M/(T_1, \ldots, T_n)M$ flat over R_0. Suppose that in the following diagram $\bar{P}$ is an R_0-linear map such that $\pi \circ \bar{P} =$ identity.*

$$\begin{array}{ccc} M/(T_1,\ldots,T_n)M & \xrightarrow{\bar{P}} & M \\ & & \downarrow{\scriptstyle\pi} \\ & & M/(T_1,\ldots,T_n)M \end{array}$$

Then the map

$$\bar{P} \otimes id : M/(T_1,\ldots,T_n)M \underset{R_0}{\otimes} R_n \to M$$

is an isomorphism. If $M/(T_1,\ldots,T_n)M$ is free over R_0, then M is free over R_n.

PROOF: Let $N = M/(T_1,\ldots,T_n)M \otimes_{R_0} R_n$, and let I be the nilpotent ideal $(T_1,\ldots,T_n)$ in R_n. Then

$$\bar{P} \otimes id\,(\mathrm{mod}\, I) : N/IN \simeq M/IM.$$

In

$$C \to \mathrm{Ker} \to N \to M,$$

the last arrow is surjective because, if $m \in M$, then $\exists n \in N$ such that

$$\bar{P} \otimes id\,(n) = m + t_1 m_1, \qquad t_1 \in I$$

by the surjectivity of $\bar{P} \otimes id\,(\mathrm{mod}\, I)$; repeating this step for $m_1,\ldots,$ we find a sequence $n, n_1, n_2,\ldots, n_r$ such that

$$\bar{P} \otimes id(n - t_1 n_1 - \ldots - t_r n_r) = m + t_{r+1} m_{r+1}, t_{r+1} \in I^{r+1}.$$

Since I is nilpotent, it follows that $\bar{P} \otimes id$ is surjective. Now, since M is flat over R_n, applying $\otimes_{R_n} R_0$ to

$$0 \to \mathrm{Ker} \to N \to M \to 0$$

gives

$$0 = \mathrm{Tor}_1^{R_n}(M, R_0) \to \mathrm{Ker}/I \cdot \mathrm{Ker} \to N/IN \to M/IM \to 0.$$

Hence $\mathrm{Ker} = I \cdot \mathrm{Ker} = I^2\,\mathrm{Ker} = \ldots = 0$ because I is nilpotent. QED

In our case, when $M = H^i_{DR}(A')$, we want to find a map

$$\bar{P} : H^i_{DR}(A) \to H^i_{DR}(A')$$

which allows us explicitly to 'trivialize' $H^i_{DR}(A')$. We actually find a map $P \in \mathrm{End}_k(H^i_{DR}(A'))$ such that $\mathrm{Ker}\, P = (T_1, \ldots, T_n)H^i_{DR}(A')$ which induces $\bar{P}$ on $H^i_{DR}(A')/(T_1, \ldots, T_n)H^i_{DR}(A') \approx H^i_{DR}(A)$. This map is constructed by 'exponentiating' the Gauss-Manin connection $\nabla_{A'}$, using a 'divided power structure' γ on the ring R_n and the ideal $(T_1, \ldots, T_n)$.

Namely, back in the general case with M as in Sublemma 1, there exists a divided power structure on the ring R_n and the ideal $(T_1, \ldots, T_n)$ (for the definition, see for example [38], p. 77) such that for $t = T_1, T_2, \ldots, T_n$ we have

$$\gamma_i(t) = \begin{cases} t^i/i! & \text{for } i = 1, 2, \ldots, p-1 \\ 0 & \text{for } i \geqq p. \end{cases}$$

We then define $P \in \mathrm{End}_{R_0} M$ by

$$P = \sum_w (-1)^{|w|} \prod_{i=1}^n \gamma_{w_i}(T_i) \prod_{i=1}^n \left(\nabla\left(\frac{\partial}{\partial T_i}\right)\right)^{w_i},$$

where the $w = (w_1, \ldots, w_n)$ run through $\mathbb{Z}^n_{\geqq 0}$, $|w| \underset{\text{def}}{=} \sum w_i$, and

$$\left(\nabla\left(\frac{\partial}{\partial T_i}\right)\right)^{w_i} \underset{\text{def}}{=} \nabla\left(\frac{\partial}{\partial T_i}\right) \circ \nabla\left(\frac{\partial}{\partial T_i}\right) \circ \overset{w_i \text{ times}}{\cdots} \circ \nabla\left(\frac{\partial}{\partial T_i}\right).$$

Note that this is a finite sum. We also define an R_0-linear endomorphism of R_n, which will also be denoted P, by

$$P(f) = \sum_w (-1)^{|w|} \prod_{i=1}^n \gamma_{w_i}(T_i) \prod_{i=1}^n \left(\frac{\partial}{\partial T_i}\right)^{w_i} f$$

for $f \in R_n$.

Sublemma 4: *If $f \in R_n$, $m \in M$, then $P(fm) = P(f)P(m)$.*

Proof: We first claim that for $u, v \in \mathbb{Z}_{\geqq 0}$ and for $t \in (T_1, \ldots, T_n)$ we have

$$(*) \qquad \binom{u+v}{v} \gamma_{u+v}(t) = \gamma_u(t)\gamma_v(t).$$

In fact, if $u+v < p$, then this becomes

$$\binom{u+v}{v} \frac{t^{u+v}}{(u+v)!} = \frac{t^u}{u!} \frac{t^v}{v!}.$$

If either u or $v \geqq p$, then both sides of (*) are zero. If $u+v \geqq p$ but $u, v < p$, then the left side is zero, and the right side is $(t^u/u!)(t^v/v!) = 0$ because $t^p = 0$.

Now

$$P(fm) = \sum_w (-1)^{|w|}\Big[\prod_{i=1}^n \gamma_{w_i}(T_i)\Big] \sum_{0 \leqq v_i \leqq w_i} \left\{\left[\prod_{i=1}^n \binom{w_i}{v_i}\left(\frac{\partial}{\partial T_i}\right)^{v_i}\right](f) \cdot \left[\prod_{i=1}^n \left(\nabla\left(\frac{\partial}{\partial T_i}\right)\right)^{w_i - v_i}\right](m)\right\}$$

by repeated application of Liebnitz's rule. By the change of indices $u = w-v$ we obtain

$$\begin{aligned} P(fm) &= \sum_{u,v} (-1)^{|u|+|v|}\left\{\left[\prod_{i=1}^n \binom{u_i+v_i}{v_i}\gamma_{u_i+v_i}(T_i)\right] \cdot \left[\prod_{i=1}^n \left(\frac{\partial}{\partial T_i}\right)^{v_i}\right](f) \cdot \left[\prod_{i=1}^n \left(\nabla\left(\frac{\partial}{\partial T_i}\right)\right)^{u_i}\right](m)\right\} \\ &= \sum_{u,v} (-1)^{|u|+|v|}\left\{\Big[\prod_{i=1}^n \gamma_{u_i}(T_i)\gamma_{v_i}(T_i)\Big] \cdot \left[\prod_{i=1}^n \left(\frac{\partial}{\partial T_i}\right)^{v_i}\right](f) \cdot \left[\prod_{i=1}^n \left(\nabla\left(\frac{\partial}{\partial T_i}\right)\right)^{u_i}\right](m)\right\} \\ &= P(f)P(m). \end{aligned}$$

QED

Corollary: *If $f, g \in R_n$, then $P(fg) = P(f)P(g)$.*

(Apply Sublemma 4 to $M = R_n$ with the 'obvious' connection $\nabla(\partial/\partial T_i) = \partial/\partial T_i$.)

Sublemma 5: *$P|_{R_n}$ is a projection onto R_0 with kernel $(T_1, \ldots, T_n)R_n$.*

Proof: If $r \in R_0$, then, since all $(\partial/\partial T_i)r = 0$, obviously $P(r) = r$. For $t = \sum r_i T_i$ in the ideal $(T_1, \ldots, T_n)$, to show $P(t) = 0$ it suffices by the corollary to show that $P(T_i) = 0$, $i = 1, \ldots, n$. But, since $(\partial/\partial T_j)T_i = \delta_{ij}$, we have

$$P(T_i) = \left(1 - \gamma_1(T_i)\frac{\partial}{\partial T_i}\right)T_i = T_i - T_i = 0. \qquad \text{QED}$$

Corollary: Ker $P|_M = (T_1, \ldots, T_n)M$;

$$P(\operatorname{mod}(T_1, \ldots, T_n)M) : M/(T_1, \ldots, T_n)M \to M/(T_1, \ldots, T_n)M$$

is the identity, and $P^2 = P$ *on* M.

In fact, the formula for P shows that

$$P(m) \in m + (T_1, \ldots, T_n)M,$$

which, together with Sublemma 5, immediately gives the corollary.

SUBLEMMA 6: $P(m_{R_n}^2 M) \subset m_{R_n}^2 M$.

PROOF: We show that each term $\prod \gamma_{w_i}(T_i) \prod (\nabla(\partial/\partial T_i))^{w_i}$ in P takes $m_{R_n}^2 M$ to itself. It suffices to show that for all r and s (say $r \neq s$; the verification is analogous if $r = s$)

$$(*) \qquad \prod \gamma_{w_i}(T_i) \prod \left(\frac{\partial}{\partial T_i}\right)^{w_i} (T_r T_s) \in m_{R_n}^2.$$

If $w_r > 1$, then $(\partial/\partial T_r)^{w_r}(T_r T_s) = 0$. If $w_s > 1$, then $(\partial/\partial T_s)^{w_s}(T_r T_s) = 0$. If $w_i > 0$ for $i \neq r, s$, then $(\partial/\partial T_i)^{w_i}(T_r T_s) = 0$. This reduces (*) to the following assertions:

$$1 \cdot T_r T_s \in m_{R_n}^2$$

$$\left(T_r \frac{\partial}{\partial T_r}\right)(T_r T_s) \in m_{R_n}^2$$

$$\left(T_s \frac{\partial}{\partial T_s}\right)(T_r T_s) \in m_{R_n}^2$$

$$\left(T_r T_s \frac{\partial}{\partial T_r} \frac{\partial}{\partial T_s}\right)(T_r T_s) \in m_{R_n}^2.$$

These are all obvious. QED

SUBLEMMA 7: *Let* $R_n = k[T_1, \ldots, T_n]/(T_1^p, \ldots, T_n^p)$, *let* $A' \in \tilde{D}_{AV}(R_n)$, *let* $R_n \to S$ *be a morphism in* $\tilde{\mathscr{C}}_k$, *and let* $A_S = A' \otimes_{R_n} S$. *Then the Hodge* $\Rightarrow$ *De Rham spectral sequence*

$$E_1^{p,q} = H^q(A_S, \Omega_{A_S}^p) \Rightarrow H_{DR}^{p+q}(A_S)$$

degenerates at E_1, *and so we have an exact sequence*

$$(*) \qquad 0 \to H^0(\Omega_{A_S}^1) \to H_{DR}^1(A_S) \to H^1(\mathcal{O}_{A_S}) \to 0$$

of modules which are f r e e *over* S *and whose formation commutes with arbitrary change of base* $S \to S'$.

PROOF: The degeneration of the Hodge $\Rightarrow$ De Rham spectral sequence in the case $S = k$ is proved, for example, in Oda, [47], Proposition 5.1.

In general, since all the $E_r^{p,q}$ are S-modules of finite length, and hence finite dimensional k-vector spaces, we have

$$(**)\qquad E \text{ degenerates at } E_1 \Leftrightarrow \sum_{p,q} \dim_k E_1^{p,q} = \sum_{p+q} \dim_k H_{DR}^{p+q}(A_S).$$

We always have $\geqq$ in (**). We must show $\leqq$.

By Sublemma 3, $H_{DR}^{p+q}(A') \approx H_{DR}^{p+q}(A) \otimes_k R_n$, so that, by Sublemma 2, $H_{DR}^{p+q}(A_S) \approx H_{DR}^{p+q}(A) \otimes_k S$. Hence, the right hand side of (**) equals

$$\dim_k S \sum_{p+q} \dim_k H_{DR}^{p+q}(A).$$

Now by 'semi-continuity' (cf. Deligne, [5], Theorem 3.3)

$$(***)\qquad \dim_k H^q(A_S, \Omega_{A_S}^p) \leqq \dim_k S \cdot \dim_k H^q(A, \Omega_A^p).$$

Hence,

$$\begin{aligned}\sum_{p,q} \dim_k E_1^{p,q} &\leqq \dim_k S \sum_{p,q} \dim_k H^q(A, \Omega_A^p)\\ &= \dim_k S \sum_{p+q} \dim_k H_{DR}^{P+Q}(A),\end{aligned}$$

because we know (**) for $S = k$. But this is equal to the right hand side of (**).

Furthermore, we now know that equality holds in (***). Hence, by the same Theorem 3.3 of [5], it follows that the $H^q(A_S, \Omega_{A_S}^p)$ are all free over S and thus their formation commutes with change of base. In addition, the $H_{DR}^i(A_S)$ are free, and their formation commutes with change of base. QED

5. *Alternating inner product on* H_{DR}^1

We note that Sublemma 7 holds for a principally polarized abelian scheme over any base scheme S, not just over an R_n-algebra. In fact, it suffices to show this for the universal family $f: A_g^{(N)} \to M_g^{(N)}$. In that case, since $\dim_k H_{DR}^i(A_{g,y}^{(N)})$ and $\dim_k H^q(A_{g,y}^{(N)}, \Omega_{A_{g,y}^{(N)}}^p)$ are constant at all closed points $y \in M_g^{(N)}$, which is reduced, we may apply the base-changing theorems for coherent cohomology to conclude that the De Rham cohomology and the Hodge cohomology are locally free sheaves on $M_g^{(N)}$ whose formation commutes with arbitrary change of base. It then follows by standard arguments that the Hodge $\Rightarrow$ De Rham spectral sequence degenerates at E_1 if it degenerates at E_1 at all closed points $y \in M_g^{(N)}$. But the case of an abelian variety over a field is proved, e.g., in [47], Proposition 5.1.

REMARK: Actually, this result is true for an abelian scheme over any base, without requiring principal polarization. Messing proves this in the 'Addendum' to [37], to appear.

Thus, for any base scheme S and any principally polarized abelian scheme $A_S \to S$ we have

$$0 \to H^0(\Omega^1_{A_S}) \to H^1_{DR}(A_s) \to H^1(\mathcal{O}_{A_S}) \to 0.$$

Using the principal polarization $\lambda_S : A_S \xrightarrow{\sim} \hat{A}_S$, we may identify

$$H^1(\mathcal{O}_{A_S}) \approx tg_{\hat{A}_S} \overset{\lambda^{-1}}{\approx} tg_{A_S} \approx \operatorname{Hom}(H^0(\Omega^1_{A_S}), \mathcal{O}_S),$$

and thereby obtain a bilinear polarization form

$$\langle, \rangle : H^0(\Omega^1_{A_S}) \times H^1(\mathcal{O}_{A_S}) \to \mathcal{O}_S.$$

We claim that $\langle, \rangle$ can be induced from a certain canonical alternating inner product on $H^1_{DR}(A_S)$ by passing to the associated graded

$$H^0(\Omega^1_{A_S}) \otimes H^1(\mathcal{O}_{A_S}).$$

The following construction, and the proof of its compatibility with the polarization form, are due to P. Berthelot and W. Messing (unpublished notes).

Consider the product $A_S \times \hat{A}_S$ with the two projections

$$\begin{array}{ccc} & A_S \times \hat{A}_S & \\ \swarrow^{\pi_1} & & \searrow^{\pi_2} \\ A_S & & \hat{A}_S. \end{array}$$

Now $A_S \times \hat{A}_S$ has a canonical 'Poincaré line bundle' $\mathcal{L}$ such that the restriction $\mathcal{L}_x$ to the fibre of a closed point $x \in \hat{A}_S$ is the line bundle on A_S corresponding to x. (Recall that, by definition, $\hat{A}_S$ parametrizes the line bundles on A_S algebraically equivalent to zero.) Then the class $c(\mathcal{L}) \in H^1(A_S \times \hat{A}_S, \mathcal{O}^x_{A_S \times \hat{A}_S})$ of the line bundle $\mathcal{L}$ gives rise to the Chern class $c_{DR} \in H^2_{DR}(A_S \times \hat{A}_S)$. We consider the map

$$\pi_{2*} \circ (\text{cup product with } c_{DR}) \circ \pi_1^*$$

on $H^{2g-1}_{DR}(A_S)$. We have

$$\pi_1^* : H^{2g-1}_{DR}(A_S) \to H^{2g-1}_{DR}(A_S \times \hat{A}_S),$$

$$\cup\, c_{DR} : H^{2g-1}_{DR}(A_S \times \hat{A}_S) \to H^{2g-1}_{DR}(A_S \times \hat{A}_S) \approx H_{2g-1}(A_S \times \hat{A}_S)$$

by Poincaré duality;

$$\pi_{2*} : H_{2g-1}(A_S \times \hat{A}_S) \to H_{2g-1}(\hat{A}_S) \approx H^1_{DR}(\hat{A}_S)$$

again by Poincaré duality. Hence we have a canonical map

$$`\cup\, c_{DR}' : H^{2g-1}_{DR}(A_S) \to H^1_{DR}(\hat{A}_S),$$

which can be shown to be an isomorphism. But $H^{2g-1}_{DR}(A_S)$ is dual to $H^1_{DR}(A_S)$. Hence we have a perfect pairing

$$H^1_{DR}(A_S) \times H^1_{DR}(\hat{A}_S) \to \mathcal{O}_S.$$

Since A_S has a principal polarization λ_S, we have $H^1_{DR}(\hat{A}_S) \approx H^1_{DR}(A_S)$, and so a pairing

$$H^1_{DR}(A_S) \times H^1_{DR}(A_S) \to \mathcal{O}_S.$$

It can be shown that this inner product is alternating; that the induced bilinear form on the associated graded

$$H^0(\Omega^1_{A_S}) \oplus H^1(\mathcal{O}_{A_S})$$

has the properties: $H^0(\Omega^1_{A_S})^\perp = H^0(\Omega^1_{A_S})$, $H^1(\mathcal{O}_{A_S})^\perp = H^1(\mathcal{O}_{A_S})$; and that the induced map

$$H^0(\Omega^1_{A_S}) \times H^1(\mathcal{O}_{A_S}) \to \mathcal{O}_S$$

is the same as our earlier $\langle , \rangle$.

6. *The Gauss-Manin map and principally polarized deformations*

Let R be in $\mathscr{C}_k$, i.e., $R = k[m_R]/m_R^2$, $m_R = (T_1, \ldots, T_N)$, and let

$A' \in D_{PPAV}(R)$. We have an inclusion

$$i : \mathrm{End}_k(m_R) \hookrightarrow \mathrm{Der}_k(R, R)$$

given by $f \mapsto$ the derivation $d : R \to R$ such that $d|k = 0$, $d|_{m_R} = f$. (If $p > 2$, this inclusion is a bijection.) Hence $\nabla_{A'}$ induces a canonical map

$$\nabla_{A'} \circ i : \mathrm{End}_k(m_R) \to \mathrm{End}_k(H^1_{DR}(A')).$$

Because the functor $\tilde{D}_{PPAV}$ is formally smooth and effectively pro-representable, it follows that A' can be realized by change of base from some $A_{R_n} \in \tilde{D}_{PPAV}(R_n)$. Hence, applying Sublemma 7 to A_{R_n} and the change of base $R_n \twoheadrightarrow R$ gives

$$0 \to H^0(\Omega^1_{A'}) \to H^1_{DR}(A') \to H^1(\mathcal{O}_{A'}) \to 0.$$

Thus, $\nabla_{A'} \circ i$ gives a canonical map

$$\bar{\nabla}_{A'} : \mathrm{End}_k(m_R) \to \mathrm{Hom}_k(H^0(\Omega^1_{A'}), H^1(\mathcal{O}_{A'})).$$

Let $d \in \mathrm{End}_k(m_R)$. For any $m \in m_R$, $\omega \in H^0(\Omega^1_{A'})$, we have

$$\begin{aligned} \bar{\nabla}_{A'}(d)(m\omega) &= m\bar{\nabla}_{A'}(d)(\omega) + d(m)\omega \\ &= \bar{\nabla}_{A'}(md)(\omega), \qquad \text{since} \quad \omega \mapsto 0 \text{ in } H^1(\mathcal{O}_{A'}) \\ &= 0, \qquad \text{since} \quad md = 0. \end{aligned}$$

Hence $\bar{\nabla}_{A'}(d)$ kills $m_R H^0(\Omega^1_{A'})$. We easily see that, in addition, the image of $\bar{\nabla}_{A'}(d)$ is in $m_R H^1(\mathcal{O}_{A'})$.

But, by the last assertion of Sublemma 7 applied to the change of base $S = R \to k$,

$$\begin{aligned} H^0(\Omega^1_{A'})/m_R H^0(\Omega^1_{A'}) &\approx H^0(\Omega^1_A); \\ H^1(\mathcal{O}_{A'})/m_R H^1(\mathcal{O}_{A'}) &\approx H^1(\mathcal{O}_A). \end{aligned}$$

In addition, if we tensor

$$0 \to m_R \to R \to k \to 0$$

with $H^1(\mathcal{O}_{A'})$, which is flat over R, we obtain

$$m_R H^1(\mathcal{O}_{A'}) \approx m_R \underset{R}{\otimes} H^1(\mathcal{O}_{A'}).$$

Hence

$$m_R H^1(\mathcal{O}_{A'}) \approx m_R \underset{R}{\otimes} H^1(\mathcal{O}_{A'}) \approx m_R \underset{k}{\otimes} (H^1(\mathcal{O}_{A'})/m_R H^1(\mathcal{O}_{A'})) \approx m_R \underset{k}{\otimes} H^1(\mathcal{O}_A).$$

Thus, $\nabla_{A'}$ induces a map

$$\operatorname{End}_k(m_R) \to \operatorname{Hom}(H^0(\Omega_A^1), H^1(\mathcal{O}_A)) \otimes m_R.$$

By the 'Gauss-Manin map', which will be denoted $\rho_{A'}$, we mean the image of the identity of $\operatorname{End}_k(m_R)$ in $\operatorname{Hom}(H^0(\Omega_A^1), H^1(\mathcal{O}_A)) \otimes m_R$.

SUBLEMMA 8 (cf. Katz, [20], Proposition 1.4.1.7): *$\rho_{A'}$ is the element in*

$$(tg_A \otimes tg_A) \otimes m_R \approx \operatorname{Hom}(H^0(\Omega_A^1), H^1(\mathcal{O}_A)) \otimes m_R$$

corresponding to the deformation $A' \in D_{PPAV}(R)$.

SUBLEMMA 9: $\rho_{A'} \in \operatorname{Symm}\operatorname{Hom}(H^0(\Omega_A^1), H^1(\mathcal{O}_A)) \otimes m_R$.

PROOF: Let ω_i', η_j' be a basis of $H^1_{DR}(A')$ such that $\omega_i' \in H^0(\Omega_{A'}^1)$ and ω_i', η_j' are dual with respect to the alternating inner product in section 5:

$$\langle \omega_i', \eta_j^i \rangle = \delta_{ij}$$
$$\langle \omega_i', \omega_j' \rangle = 0$$
$$\langle \eta_i', \eta_j' \rangle = 0.$$

Let

$$d \underset{\text{def}}{=} \bar{\nabla}_{A'}(1) \in \operatorname{Hom}_k(H^0(\Omega_{A'}^1), H^1(\mathcal{O}_{A'})).$$

Let $t_{ij} \in \operatorname{Hom}(H^0(\Omega_A^1), H^1(\mathcal{O}_A))$ be the basis element $\omega_i \mapsto \bar{\eta}_j$, $\omega_{i'} \mapsto 0$ if $i' \neq i$ (where $\omega_i = \omega_i' \otimes_R k$ and $\bar{\eta}_j$ is the image of $\eta_j' \otimes_R k$ in $H^1(\mathcal{O}_A)$). If we write

$$\rho_{A'} = \sum_{i,j} m_{ij} t_{ij}, \qquad m_{ij} \in m_R,$$

then the m_{ij} are given by:

$$d\omega'_i \equiv \sum_j m_{ij}\eta'_j (\text{mod } H^0(\Omega^1_{A'})).$$

Because the cup-product construction of $\langle , \rangle$ is horizontal with respect to the Gauss-Manin connection, we always have

$$d\langle a, b\rangle = \langle da, b\rangle + \langle a, db\rangle \qquad \text{for } a, b \in H^1_{DR}(A').$$

Hence, since $\langle \omega'_i, \omega'_j\rangle = 0$, we have

$$\begin{aligned} 0 = d\langle \omega'_i, \omega'_j\rangle &= \langle d\omega'_i, \omega'_j\rangle + \langle \omega'_i, d\omega'_j\rangle \\ &= \langle \sum_k m_{ik}\eta'_k, \omega'_j\rangle + \langle \omega'_i, \sum_k m_{jk}\eta'_k\rangle \\ &= -\langle \omega'_j, \sum_k m_{ik}\eta'_k\rangle + \langle \omega'_i, \sum_k m_{jk}\eta'_k\rangle = -m_{ij} + m_{ji}, \end{aligned}$$

so that $\rho_{A'}$ gives a symmetric element. QED

PROOF OF LEMMA 12 (1): According to a theorem of Grothendieck and Mumford (cf. Oort, [49], p. 242–246), the functor $\tilde{D}_{PPAV}$ is a formally smooth subfunctor of $\tilde{D}_{AV}$, and the t_{ij} in Grothendieck's theorem on the pro-representability of $\tilde{D}_{AV}$ can be chosen in such a way that $\tilde{D}_{PPAV}$ is effectively pro-representable by

$$k[[\{t_{ij}\}^g_{i,j=1}]]/(\{t_{ij} - t_{ji}\}^g_{i,j=1}).$$

It then follows that the functor D_{PPAV} is representable by

$$k[m_{t,\text{Symm}}]/m^2_{t,\text{Symm}},$$

where $m_{t,\text{Symm}}$ is defined as the quotient of the vector space generated by the t_{ij} by the vector space generated by the $t_{ij} - t_{ji}$.

But by Sublemma 9 the functor D_{PPAV} is a subfunctor of the subfunctor of D_{AV} represented by the vector space of symmetric elements. Since D_{PPAV} is represented by a vector space of the same dimension as this vector space of symmetric elements, we may conclude that the symmetric basis elements may be taken as the t_{ij} in the Grothendieck-Mumford theorem. This proves part (1) of Lemma 12.

7. *Action of Frobenius*

Let $R_n = k[T_1, \ldots, T_n]/(T_1^p, \ldots, T_n^p)$, $A' \in \tilde{D}_{PPAV}(R_n)$, $M = H^1_{DR}(A')$, and let $P \in \operatorname{End}_k M$ be as in section 4.

SUBLEMMA 10: $PF(m) = F(m)$.

PROOF: We show that, for any $m \in M$, $F(m)$ is horizontal with respect to $\nabla = \nabla_{A'}$, so that all terms of P with $w \neq (0, 0, \ldots, 0)$ vanish on $F(m)$.

In general, any change of base

$$\begin{tikzcd} S \arrow[r, phantom, "\supset"] & S_0 \\ R_n \arrow[u, "\alpha"] \arrow[r, phantom, "\supset"] & R_0 \arrow[u] \end{tikzcd}$$

induces a map $\alpha : \Omega^1_{R_n/R_0} \to \Omega^1_{S/S_0}$ and then a connection $\nabla^{(\alpha)}$ on $M^{(\alpha)} = M \otimes_{R_n} S$ as follows:

$$\begin{tikzcd} M \arrow[r, "\nabla"] \arrow[d, "id\otimes S"] \arrow[drr, "\nabla^{(\alpha)}"] & M \underset{R_n}{\otimes} \Omega^1_{R_n/R_0} \arrow[r, "1\otimes\alpha"] & M \underset{R_n}{\otimes} \Omega^1_{S/S_0} \arrow[d, phantom, "\wr"] \\ M^{(\alpha)} = M \underset{R_n}{\otimes} S \arrow[rr, dashed, "\nabla^{(\alpha)}"] & & (M \underset{R_n}{\otimes} S) \underset{S}{\otimes} \Omega^1_{S/S_0} \end{tikzcd}$$

Now for $m \in M$, $s \in S$ we define $\nabla^{(\alpha)}(m \otimes s)$ as

$$\bar{\nabla}^{(\alpha)}(m)s + mds.$$

It is easy to see that $\nabla^{(\alpha)}$ is well-defined, and that ∇ composed with the map on M induced by the base change is $\nabla^{(\alpha)}$.

In our case, $S = R_n$, $S_0 = R_0 = k$, and the map

$$\begin{tikzcd} R_n \arrow[r, phantom, "\supset"] & k \\ R_n \arrow[u, "F"] \arrow[r, phantom, "\supset"] & k \arrow[u, "F"] \end{tikzcd}$$

is the Frobenius F. Since F kills differentials, the map α is zero. Hence, for any $m \in M$, $\nabla^{(\alpha)}(m \otimes 1) = 0$. Because F as *linear* map $M^{(F)} \to M$ is a horizontal map from $(M^{(F)}, \nabla^{(F)})$ to (M, ∇), it follows that $F : M \to M$ as *p-linear* map satisfies

$$\nabla(F(m)) = 0$$

for all $m \in M$. QED

Now let $\{\bar{\eta}_j\}$ be an arbitrary basis of $H^1(\mathcal{O}_A)$, and let $\{\omega_i\}$ be the dual basis of $H^0(\Omega^1_A)$ with respect to the polarization form. Consider the ω_i as elements of $H^1_{DR}(A)$ and choose any $\eta_j \in H^1_{DR}(A)$ lifting $\bar{\eta}_j$.

Sublemma 11: *There exists a basis ω'_i, η'_j of $H^1_{DR}(A')$ lifting ω_i, η_j and such that $\omega'_i \in H^0(\Omega^1_{A'})$ and $P(\eta'_j) = \eta'_j$.*

Proof: Because

$$H^1_{DR}(A') \approx H^1_{DR}(A) \otimes_k R_n \quad \text{and} \quad H^0(\Omega^1_{A'}) \approx H^0(\Omega^1_A) \otimes_k R_n,$$

the basis ω_i, η_j can be lifted to a basis ω'_i, $\tilde{\eta}'_j$ of $H^1_{DR}(A')$ such that $\omega'_i \in H^0(\Omega^1_{A'})$. In fact, any elements in a free module M which reduce to a basis in M/IM, I a nilpotent ideal, must themselves be a basis of M (see proof of Sublemma 3). Let $\eta'_j = P(\tilde{\eta}'_j)$. Since P is the identity modulo $(T_1, \ldots, T_n)H^1_{DR}(A')$, it follows that ω'_i, η'_j still lift ω_i, η_j and so are a basis of $H^1_{DR}(A')$ adopted to the Hodge filtration. Moreover, since $P^2 = P$, we have $P(\eta'_j) = \eta'_j$. QED

Since F kills differentials, the matrix of F on $H^1_{DR}(A)$ with respect to the basis ω_i, η_j is of the form

$$\begin{pmatrix} 0 & B \\ 0 & H \end{pmatrix},$$

and the matrix of F on $H^1_{DR}(A')$ with respect to the basis ω'_i, η'_j is of the form $\left(\begin{smallmatrix} 0 & B' \\ 0 & H' \end{smallmatrix}\right)$. In addition, F on $H^1_{DR}(A)$ has the property (cf. Oda, [47], Proposition 5.4):

$$\operatorname{Ker} F | H^1_{DR}(A) = H^0(\Omega^1_A).$$

Hence the $2g \times g$ matrix $\left(\begin{smallmatrix} B \\ H \end{smallmatrix}\right)$ has rank g.

Now the Hasse-Witt matrix $H' = \{h'_{ij}\}$ of A' is given by

$$F(\eta'_j) \equiv \sum_i h'_{ij}\eta'_i \ (\operatorname{mod} H^0(\Omega^1_{A'})),$$

i.e.,

$$(*) \qquad F(\eta'_j) = \sum_i (b'_{ij}\omega'_i + h'_{ij}\eta'_i).$$

Applying P to (*) gives

$$(**)\qquad F(\eta'_j) = PF(\eta'_j) = \sum_i (P(b'_{ij})P(\omega'_i) + P(h'_{ij})\eta'_i)$$
$$= \sum_i (b_{ij}P(\omega'_i) + h_{ij}\eta'_i),$$

since b'_{ij}, h'_{ij} reduce in $R_n/(T_1, \ldots, T_n) = k$ to the matrix of the action of F on $H^1_{DR}(A')/(T_1, \ldots, T_n)H^1_{DR}(A') \approx H^1_{DR}(A)$, namely b_{ij}, h_{ij}.

Now let m_{R_n} denote the ideal $(T_1, \ldots, T_n)$, let $S = R_n/m^2_{R_n} = k[m_{R_n}]/m^2_{R_n}$, and let $A_S = A' \otimes_{R_n} S \in D_{PPAV}(S)$. Then $\nabla_{A'}$ induces ∇_{A_S} on $H^1_{DR}(A_S)$. Let $\omega^S_i = \omega'_i \otimes_{R_n} S$; $\eta^S_j = \eta'_j \otimes_{R_n} S$.

By Sublemma 6, P induces an endomorphism P_S on

$$H^1_{DR}(A_S) \approx H^1_{DR}(A') \underset{R_n}{\otimes} S \approx H^1_{DR}(A')/m^2_{R_n} H^1_{DR}(A').$$

SUBLEMMA 12: $P_S = 1 - \sum_i \nabla_{A_S}(T_i(\partial/\partial T_i))$.

PROOF: First note that all terms in P with $|w| \geqq 2$ map all of $H^1_{DR}(A')$ to $m^2_{R_n}H^1_{DR}(A')$. Next, since $T_i(\partial/\partial T_i)$ is a derivation of S, it follows by the functoriality of the Gauss-Manin connection that

$$T_i \nabla_{A'}\left(\frac{\partial}{\partial T_i}\right) = \nabla_{A'}\left(T_i \frac{\partial}{\partial T_i}\right)$$

induces

$$\nabla_{A_S}\left(T_i \frac{\partial}{\partial T_i}\right) \in \mathrm{End}_k\, H^1_{DR}(A_S).$$

Hence

$$P_S = 1 - \sum_i \nabla_{A_S}\left(T_i \frac{\partial}{\partial T_i}\right). \qquad \text{QED}$$

PROOF OF LEMMA 12 (2): The Hasse-Witt matrix $H^S = \{h^S_{ij}\}$ of A_S is given by

$$F(\eta^S_j) = \sum_i (b^S_{ij}\omega^S_i + h^S_{ij}\eta^S_i).$$

Reducing the equation (**) above modulo $m_{R_n}^2 H_{DR}^1(A')$ gives

$$F(\eta_j^S) = \sum_i (b_{ij} P_S(\omega_i^S) + h_{ij}\eta_i^S)$$
$$\equiv \sum_i \left[b_{ij}\left(- \sum_r \nabla_{A_S}\left(T_R \frac{\partial}{\partial T_r}\right)\omega_i^S \right) + h_{ij}\eta_i^S \right] (\mathrm{mod}\; H^0(\Omega_{A_S}^1)).$$

Notice that $\sum_r \nabla_{A_S}(T_r(\partial/\partial T_r))$ is the image of the identity endomorphism of $(T_1, \ldots, T_n)$ under the map $\bar{\nabla}_{A_S}$ defined in section 6.

We now specify a choice for S, A_S, R_n, A'. Let m_S be the quotient of the vector space with basis $\{T_{ij}\}_{i,j=1}^g$ by the vector space generated by the $T_{ij} - T_{ji}$. Let $S = k[m_S]/m_S^2$. Let $R_n = k[m_S]/(\{m^p\}_{m \in m_S})$, i.e., here

$$n = \dim m_S = \tfrac{1}{2}g(g+1).$$

Let $A_S \in D_{PPAV}(S)$ be the 'generic square zero deformation', i.e., the deformation corresponding to the element in

$$\mathrm{Hom}\,((ctg_A \otimes ctg_A)_{\mathrm{Symm}}, m_S)$$

given by $\bar{\eta}_i \otimes \bar{\eta}_j \mapsto T_{ij}$. Since A_S can be realized by change of base from some $A' \in \tilde{D}_{PPAV}(R_n)$, it follows that the construction in the last paragraph applies. As remarked there, $\sum_r \nabla_{A_S}(T_r\,(\partial/\partial T_r))$ is the image of $1 \in \mathrm{End}_k\, m_S$ under $\bar{\nabla}_{A_S}$. But, by Sublemma 8, $\bar{\nabla}_{A_S}(1)$ induces the element in

$$\mathrm{Symm}\ \mathrm{Hom}\,(ctg_A, tg_A) \otimes\ m_S,$$

namely ρ_{A_S}, which corresponds to A_S. That is,

$$\sum_r \nabla_{A_S}\left(T_r \frac{\partial}{\partial T_r}\right)\omega_i^S \equiv \sum_j T_{ij}\eta_j^S\ (\mathrm{mod}\; H^0(\Omega_{A_S}^1)).$$

(Recall that ω_i, $\bar{\eta}_j$ were chosen to be dual bases.) Thus,

$$F(\eta_j^S) \equiv \sum_i (h_{ij} - \sum_k T_{ik} b_{kj})\eta_i^S\ (\mathrm{mod}\; H^0(\Omega_{A_S}^1)),$$

i.e.,

$$H^S = H - TB,$$

where T is the generic symmetric matrix $\{T_{ij}\}$. Thus, the deformation over $k[\varepsilon]/\varepsilon^2$ corresponding to the homomorphism $T_{ij} \mapsto u_{ij}\varepsilon$ has Hasse-Witt matrix $H_u = H - \varepsilon UB$, and Lemma 12 is proved.

8. *Isomorphism types of p-linear endomorphisms*

We now discuss how to normalize $H(A)$ in a convenient way by a suitable choice of basis for $H^1(\mathcal{O}_A)$.

Let H be the matrix of a p-linear endomorphism F with respect to a basis $v_1, \ldots, v_g$ of a g-dimensional k-vector space V on which F acts. First, $v_1, \ldots, v_{r_s}$ (r_s = stable rank of H) may be chosen to be fixed by F (cf. Katz, [21], Proposition 1.1). Then, just as in the linear case, we easily see that, for suitable choice of $v_{r_s+1}, \ldots, v_g$, the p-linear action of F on V_{nilp} has matrix

$$N = \begin{pmatrix} N_{g_1} & 0 & \ldots & 0 \\ 0 & N_{g_2} & \ldots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & & N_{g_h} \end{pmatrix},$$

where N_{g_i} is the $g_i \times g_i$ nilpotent rank $g_i - 1$ matrix of the form

$$N_{g_i} = \begin{pmatrix} 0 & 1 & 0 & & & & \\ 0 & 0 & 1 & 0 & & & \\ & 0 & 0 & 1 & 0 & & \\ & & & & \cdot & & \\ & & & & & \ddots & \\ & & & & & 0 & 1 \\ & & & & & 0 & 0 \end{pmatrix}$$

Hence, there is a one-to-one correspondence between isomorphism types of p-linear endomorphisms of V and partitions $P = (r', g_1, g_2, \ldots, g_h)$ of g such that

$$r' \geqq 0, \qquad g_1 \geqq g_2 \geqq \ldots \geqq g_h \geqq 1, \qquad r' + \sum g_i = g$$

given by

$$(r', g_1, \ldots, g_h) \leftrightarrow H = \begin{pmatrix} I_{r'} & 0 & & \\ 0 & N_{g_1} & & \\ & & \ddots & \\ & & & N_{g_h} \end{pmatrix},$$

where $I_{r'}$ is the $r' \times r'$ identity matrix.

If $A \in M_g$ and the Hasse-Witt matrix $H(A)$ is of type P,

$$P = (r', g_1, \ldots, g_h),$$

then clearly

$$r_s(A) = r';$$
$$r(A) = g - h.$$

9. *Tangent space computations*

By [44], p. 331–332, the Zariski tangent space to the scheme $S_{n,m}$ at A is given by the set of morphisms

$$\operatorname{Spec} k[\varepsilon]/\varepsilon^2 \to S_{n,m} \subset M_g$$

whose restrictions to Spec k have image point A. Since M_g represents the deformation functor, this tangent space is given in $\operatorname{Spec} k[m_t]/m_t^2$ by the condition that the morphism $k[m_t]/m_t^2 \to k[\varepsilon]/\varepsilon_2$

$$t_{ij} \mapsto u_{ij}\varepsilon \qquad (u_{ij} \in k,\ u_{ij} = u_{ji})$$

corresponds to a deformation A_u whose Hasse-Witt matrix H_u satisfies the equations of $S_{n,m}$:

$$\text{all } m \times m \text{ minors of } H_u H_u^{(p)} \ldots H_u^{(p^{n-1})} \text{ vanish,}$$

where the superscript (p^i) denotes raising all entries to the p^i-th power.

We saw that

$$H_u = H - \varepsilon UB,$$

where U is the matrix $\{u_{ij}\}$ and where $\left(\begin{smallmatrix} 0 & B \\ 0 & H \end{smallmatrix}\right)$ is the matrix of $F|H^1_{DR}(A)$. We may assume that a basis of $H^1_{DR}(A)$ is chosen so that H is normalized as in section 8 above. Then, since $\varepsilon^2 = 0$ and H has all entries 0 or 1, we have

$$\begin{aligned} H_u H_u^{(p)} \ldots H_u^{(p^{n-1})} &= (H - \varepsilon UB)(H^{(p)} - \varepsilon^p U^{(p)} B^{(p)}) \ldots \\ &= (H - \varepsilon UB) H^{n-1} \\ &= H^n - \varepsilon UBH^{n-1}. \end{aligned}$$

Proof of Lemma 10: Here $A \in M_g$, $r_s(A) < g$, $r(A) = g-1$, and $r_s(A) \leqq r' \leqq g$. The Zariski tangent space to $S_{g-r',r'+1}$ at A, which contains the tangent space to $M_{g,r'} = (S_{g-r',r'+1})_{\text{red}}$, is given by the condition:

$$\text{all } (r'+1)\times(r'+1) \text{ minors in } H^{g-r'} - \varepsilon UBH^{g-r'-1} \text{ vanish.}$$

If we again take $H(A)$ in the normalized form of section 8, which in this case is $\left(\begin{smallmatrix} I_{r_s} & 0 \\ 0 & N_{g-r_s}\end{smallmatrix}\right)$, then clearly

$$H^{g-r'-1} = \begin{pmatrix} \overbrace{\begin{matrix}1 & 0 & & & \\ 0 & 1 & & & \\ & & 1 & & \\ & & & \ddots & \\ & & & & 1\end{matrix}}^{r_s} & & \\ & \overbrace{0 \ \dots\ 0}^{g-r'-1} & \overbrace{\begin{matrix}1 & & & \\ 0 & 1 & & \\ & & \ddots & \\ & & & 1\end{matrix}}^{r'-r_s+1} \\ & 0 \qquad 0 & 0 \\ & \cdots & \\ & 0 \qquad 0 & 0\end{pmatrix}$$

and $H^{g-r'}$ is the same type of matrix with '$g-r'-1$' replaced by '$g-r'$' (i.e., one more zero column) and with '$r'-r_s+1$' replaced by '$r'-r_s$' (i.e., one fewer column on the right with a one). It follows that the possibly nonzero $(r'+1)\times(r'+1)$ minors in $H^{g-r'}-\varepsilon UBH^{g-r'-1}$ are obtained by multiplying the r' ones in $H^{g-r'}$ and then taking a term in the $(r'+1)$-th, $(r'+2)$-th, ..., or g-th row and in the (r_s+1)-th, (r_s+2)-th, ..., or $(g-r'+r_s)$-th column of $\varepsilon UBH^{g-r'-1}$. But all of these columns of $\varepsilon UBH^{g-r'-1}$ except for the $(g-r'+r_s)$-th vanish, while the i-th term a_i in the $(g-r'+r_s)$-th column is equal to

$$\varepsilon \sum_j u_{ij} b_{j,r_s+1}.$$

Since the (r_s+1)-th column of B is nonzero (or else we would have $\eta_{r_s+1} \in \operatorname{Ker} F|H^1_{DR}(A)$), it follows that the a_i give nonzero linearly independent forms in the u_{ij}. Hence the vanishing of all possible $(r'+1)\times(r'+1)$

minors is equivalent to the $g-r'$ independent conditions:

$$a_{r'+1} = a_{r'+2} = \dots = a_g = 0. \qquad \text{QED}$$

PROOF OF LEMMA 11: Here $A \in M_g$, $r(A) = g-h$, $h > 1$, and $r_s = r_s(A)$. Suppose $H = H(A)$ is of isomorphism type $P = (r_s, g_1, \dots, g_h)$. Since Lemma 11 suppose $A \in S_{i+1,r_s+1} - S_{i,r_s+1}$, this means $g_1 = i+1$. Since S_{g_1-1,r_s+1} is a closed subscheme of S_{g_1,r_s+1} not containing A, the claim of Lemma 11 becomes: the Zariski tangent space to $S_{1,g-h+1} \cap S_{g_1,r_s+1}$ at A has codimension $> g-r_s$. Let T_1 denote the tangent space to $S_{1,g-h+1}$ at A, and let T_2 denote the tangent space to S_{g_1,r_s+1} at A. We must show that

$$\operatorname{codim}(T_1 \cap T_2) > g-r_s.$$

Now T_1 is given by the condition:

all $(g-h+1)\times(g-h+1)$ minors in $H-\varepsilon UB$ vanish.

This condition implies that an entry in UB vanishes if it is in the

(r_s+g_1)-th, $(r_s+g_1+g_2)$-th, ..., or g-th

row of UB and in the

(r_s+1)-th, (r_s+g_1+1)-th, ..., or $(r_s+g_1+\dots+g_{h-1}+1)$-th

column. Since by assumption $h > 1$, we have at least the following two relations:

$$(*_1) \qquad \begin{aligned} &(BU_{01}) \qquad \sum_{j=1}^{g} b_{j,r_s+g_1+1}\, u_{r_s+g_1,j} = 0 \\ &(BU_{02}) \qquad \sum_{j=1}^{g} b_{j,r_s+g_1+1}\, u_{r_s+g_1+g_2,j} = 0 \end{aligned}$$

Next, T_2 is given by the condition:

all $(r_s+1)\times(r_s+1)$ minors in $H^{g_1} - \varepsilon UBH^{g_1-1}$ vanish.

But the possibly nonzero minors are precisely equal to the entries in the lower-right $(g-r_s)\times(g-r_s)$ block of εUBH^{g_1-1}. Note that H^{g_1-1}

has at least one entry 1 in its lower-right $(g-r_s)\times(g-r_s)$ block (it has more if $g_2 = g_1$):

$$H^{g_1-1} = \begin{pmatrix} I_{r_s} & & \\ & g_1\left\{\begin{array}{l} \overbrace{0\ 1\ 0\ \dots\ 0}^{g_1} \\ 0\ 0\ 0 \\ \dots \end{array}\right. & 0 \\ & 0 & ? \end{pmatrix}$$

Let $UBH^{g_1-1} = \{c_{ij}\}$. We set the following entries equal to zero:

$$c_{r_s+1,r_s+2}, \qquad c_{r_s+2,r_s+2}, \dots, c_{g,r_s+2}.$$

We obtain:

$$(*_2) \qquad (BU_i) \qquad \sum_{j=1}^{g} b_{j,r_s+1} u_{r_s+i,j} = 0, \qquad i = 1, 2, \dots, g-r_s.$$

It suffices to show that, among the $g-r_s+2$ linear forms BU_{01}, $BU_{02}, BU_1, BU_2, \dots, BU_{g-r_s}$ in $(*_1)$ and $(*_2)$, there are at least $g-r_s+1$ independent forms. We must keep in mind that $u_{ij} = u_{ji}$, but that otherwise the u_{ij} are linearly independent.

Suppose that the $g-r_s+1$ forms BU_{01}, BU_1, $BU_2, \dots, BU_{g-r_s}$ are linearly dependent:

$$(*_3) \qquad a_0 BU_{01} + \sum_{i=1}^{g-r_s} a_i BU_i = 0, \qquad a_i \in k$$

First note that for some $i_0 \neq 0, g_1$ we must have $a_{i_0} \neq 0$; otherwise the two forms

$$\sum b_{j,r_s+g_1+1} u_{r_s+g_1,j},$$
$$\sum b_{j,r_s+1} u_{r_s+g_1,j}$$

would be linearly dependent, which is impossible because the (r_s+1)-th and (r_s+g_1+1)-th columns of B are linearly independent.

Since $a_{i_0} \neq 0$, looking at the coefficient of $u_{r_s+i_0,j}$ in $(*_3)$ for any $j = 1, \dots, r_s$ gives

$$(*_4) \qquad b_{j,r_s+1} = 0 \qquad \text{for } j = 1, \ldots, r_s$$

(because for such j no other BU_i contains $u_{r_s+i_0,j} = u_{j,r_s+i_0}$).

Looking at the coefficient of $u_{r_s+i_0,r_s+i_0}$ in $(*_3)$ (this variable only occurs in BU_{i_0}), we see that

$$b_{r_s+i_0,r_s+1} = 0.$$

Now for any $i_1 \neq 0, g_1$ the coefficient of $u_{r_s+i_1,r_s+i_0}$ in $(*_3)$ is

$$a_{i_0} b_{r_s+i_1,r_s+1} + a_{i_1} b_{r_s+i_0,r_s+1} = a_{i_0} b_{r_s+i_1,r_s+1}.$$

Since this coefficient is zero, while $a_{i_0} \neq 0$, we have

$$(*_5) \qquad b_{r_s+i_1,r_s+1} = 0, \qquad \text{for all } i_1 = 1, 2, \ldots, \hat{g}_1, \ldots, g-r_s$$

Now suppose that the $g-r_s+1$ forms $BU_{02}, BU_1, BU_2, \ldots, BU_{g-r_s}$ are linearly dependent. In exactly the same way this would imply that

$$b_{r_s+i_1,r_s+1} = 0, \qquad \text{for all } i_1 = 1, 2, \ldots, \widehat{g_1+g_2}, \ldots, g-r_s.$$

By $(*_4)$ and $(*_5)$, this means

$$b_{i,r_s+1} = 0 \qquad \text{for all } i = 1, 2, \ldots, g.$$

But the (r_s+1)-th column of B can not vanish.

Hence, we must have $g-r_s+1$ linearly independent forms, so that the codimension of $T_1 \cap T_2$ is strictly greater than $g-r_s$. This proves Lemma 11, and completes the proof of Theorem 7. QED

10. *Relation to Igusa's theorem*

Suppose that the Hasse-Witt matrix $H(A)$ is identically zero. Then, by Lemma 12, rank $B = g$. B can be regarded as the matrix of a bijective p-linear homomorphism from $H^1(\mathcal{O}_A)$ to $H^0(\Omega_A^1) \approx \operatorname{Hom}(H^1(\mathcal{O}_A), k)$.

LEMMA 13: *Let V be a g-dimensional vector space over a separably closed field k of characteristic p. Let $\hat{V}$ be the dual vector space. Let $\varphi : V \to \hat{V}$ be a bijective q-linear homomorphism, $q = p^a$. Then there exists a basis $\underline{e}$ of V whose image under φ is the dual basis $\underline{\hat{e}}$ of $\hat{V}$, i.e.,*

$$\langle e_i, \varphi(e_j) \rangle = \delta_{ij}.$$

PROOF: Let $\underline{e}$ be any basis of V, and write

$$\varphi(\underline{e}) = B\underline{\hat{e}}, \qquad B \in GL(g, k).$$

Let $F : GL(g, k) \to GL(g, k)$ be the map 'raising all entries to the q-th power.' First, for $C \in GL(g, k)$, note that $\widehat{(C\underline{e})} = C^{t^{-1}}\underline{\hat{e}}$ ('t' denotes transpose). In fact,

$$\langle Ce_i, C^{t^{-1}}\hat{e}_j\rangle = \langle e_i, C^t C^{t^{-1}}\hat{e}_j\rangle = \langle e_i, \hat{e}_j\rangle = \delta_{ij}.$$

Hence, the basis $C\underline{e}$ satisfies the lemma if and only if

$$C^{t^{-1}}\underline{\hat{e}} = \widehat{(C\underline{e})} = \varphi(C\underline{e}) = F(C)B\underline{\hat{e}},$$

i.e., if and only if

$$F(C)BC^t = 1.$$

The rest of the proof is identical to the proof of Proposition 1.1 in [21], p. 4–5. QED

COROLLARY OF LEMMAS 12 AND 13: *If* $H(A) = 0$, *and if* H_t *denotes the Hasse-Witt matrix of the universal principally polarized deformation* A_t *(see p. 165), then*

$$H_t \equiv -T \pmod{m_{t,\mathrm{Symm}}^2},$$

where $T = \{t_{ij}\}$ *is the generic symmetric matrix.*

In fact, the corollary follows by lifting the expression for H_u in Lemma 12, namely

$$H_u = H - \varepsilon UB = -\varepsilon UB$$

from the deformation over $k[\varepsilon]/\varepsilon^2$ to the deformation A_t over $k[[m_{t,\mathrm{Symm}}]]$, and noting that, by Lemma 13, we may choose suitable bases ω_i, $\bar{\eta}_j$ of $H^0(\Omega_A^1)$, $H^1(\mathcal{O}_A)$, respectively, which are dual to each other, such that B is the $g \times g$ identity matrix.

This corollary is a higher dimensional analogy of Igusa's theorem that the Hasse invariant of an elliptic curve has simple zeros. In the case $g = 1$, the corollary gives an independent proof of that theorem. In fact, it was Deligne's proof of Igusa's theorem by deformation theoretic methods that made it clear that these methods could be used to study the behavior of the Hasse-Witt matrix near *any* principally polarized abelian variety. (Compare: Deligne and Rapoport, [63], p. 138–139.)

11. *The case* $g = 2$

Here $\dim M_2 = 3$. There are four isomorphism types of Hasse-Witt, represented by:

(1) $H(A) = \left(\begin{smallmatrix}1 & 0\\ 0 & 1\end{smallmatrix}\right)$ $(r(A) = r_s(A) = 2)$;

(2) $H(A) = \left(\begin{smallmatrix}1 & 0\\ 0 & 0\end{smallmatrix}\right)$ $(r(A) = r_s(A) = 1)$;

(3) $H(A) = \left(\begin{smallmatrix}0 & 1\\ 0 & 0\end{smallmatrix}\right)$ $(r(A) = 1, r_s(A) = 0)$;

(4) $H(A) = \left(\begin{smallmatrix}0 & 0\\ 0 & 0\end{smallmatrix}\right)$ $(r(A) = r_s(A) = 0)$.

Theorem 7 gives a picture of the stratification except at those A whose Hasse-Witt matrix is identically zero (type 4).

In that case, we can use the above corollary of Lemmas 12 and 13 to compute the leading term of the determinant of H_t (resp. compute the leading terms of the entries of $H_t H_t^{(p)}$) in order to determine what kind of singularity $M_{2;1}$ (resp. $M_{2;0}$) has at an abelian variety of type 4. The results of these computations are as follows:

(1) $M_{2;1}$ is a (2-dimensional) divisor which is smooth at all points A for which $H(A)$ is of type 2 or 3 and which has isolated singularities at points A for which $H(A)$ is of type 4. These singularities are of the form:

$$t_{11}t_{22} - t_{12}^2 = 0.$$

(2) $M_{2;0}$ is a curve which is smooth at all points A for which $H(A)$ is of type 3 and which is singular at points A for which $H(A)$ is of type 4. These singularities are ordinary $(p+1)$-points of the form:

$$t_{12} = \xi t_{11},$$
$$t_{22} = \xi^2 t_{11},$$

where ξ is any $(p+1)$-th root of -1.

V. Examples and conjectures

1. *Supersingular abelian varieties*

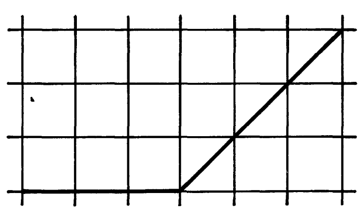
DEFINITIONS (cf. Oort, [50]): *An abelian variety (or curve) is called very special if it has p-rank zero, i.e., if it has nilpotent Hasse-Witt matrix. It is called* supersingular *if the Newton polygon of its zeta-function (as defined on p. 122) has all slopes* $\frac{1}{2}$.

COROLLARY OF THEOREM 7: *The set of very special principally polarized abelian varieties has pure codimension* g *in* M_g. *The set of supersingular principally polarized abelian varieties has codimension* $\geqq g$, *with strict inequality holding if and only if every supersingular principally polarized abelian variety is a specialization of a very special but* not *supersingular principally polarized abelian scheme.*

CONJECTURE[1]: In each irreducible component of the set of supersingular principally polarized abelian varieties, only a proper closed subset of the component is a specialization of a very special but not supersingular principally polarized abelian scheme. Equivalently, the set of supersingular principally polarized abelian varieties has pure codimension g in M_g.

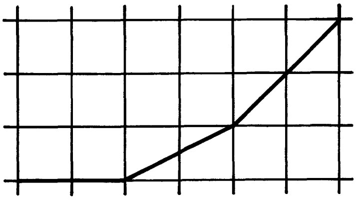
The first case when the conjecture has content – i.e., not all very special abelian varieties are supersingular – occurs when $g = 3$. In this case every 3-dimensional principally polarized abelian variety can be realized as the jacobian of a genus 3 curve. Here $\dim M_3 = \frac{1}{2}g(g+1) = 6$ (also $= 3g-3$, the formula for the number of moduli of curves).

When $g = 3$, there are 5 possible Newton polygons, with the last two types corresponding to the very special case $r_s = 0$:

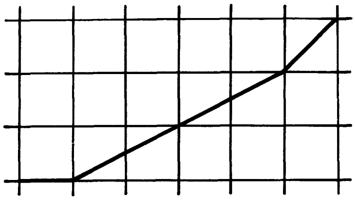


Type 1

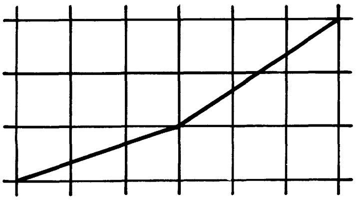
[1] However, Professor Oort has recently *disproved* this conjecture. He has shown that there are no 3-dimensional families of supersingular principally polarized 3-dimensional abelian varieties. (But Oort and Oda have proved that in any characteristic there exist 2-dimensional supersingular families in the moduli space. See their paper 'Supersingular Abelian Varieties', to appear.) In particular, Oort has thereby called into serious question the conjectured transversality of the hyperelliptic locus to the Newton polygon stratification. It now seems likely (though not yet proved) that an entire component of the *two*-dimensional set of supersingular genus 3 curves is hyperelliptic.



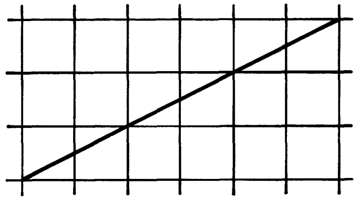
Type 2



Type 3



Type 4



Type 5

Let S_i be the set of genus 3 curves whose zeta-function has Newton polygon of type i, $i = 1, 2, 3, 4, 5$. We have

$$\begin{aligned} \dim S_1 &= 6 \\ \dim S_2 &= 5 \\ \dim S_3 &= 4 \\ \dim S_4 &= 3 \end{aligned}$$

$$\dim S_5 \begin{cases} = 3 \text{ if the conjecture holds} \\ \leqq 2 \text{ otherwise.} \end{cases}$$

(Actually, $\dim S_5 = 3$ does *not strictly imply* the conjecture as stated, because of the possibility that S_5 has some 3-dimensional and also some lower dimensional components, i.e., that it is not of *pure* codimension 3; but evidence that $\dim S_5 = 3$ will *support* the conjecture.) All of these relations follow from Theorem 7, except for the equality $\dim S_4 = 3$ (Theorem 7 only gives $\dim (S_4 \cup S_5) = 3$), which follows from a specialization theorem of Grothendieck and a result of Tate and Honda, which will be discussed later.

We tested the conjecture experimentally on the IBM 360 computer, which examined genus 3 hyperelliptic curves of the following form:

$$y^2 = f(x) = x^7 + a_1 x^6 + a_2 x^5 + a_3 x^4 + a_4 x^3 + a_5 x^2 + a_6 x + a_7,$$

where f has distinct roots, $a_i \in \mathbb{F}_p$, and:

$$\text{if } p \neq 7, \quad \text{then } a_1 = 0, a_2 = 1, 1 \leqq a_3 \leqq \tfrac{1}{2}(p-1);$$
$$\text{if } p = 7, \quad \text{then } a_1 = 1, a_2 = 0, 0 \leqq a_3 \leqq 6.$$

This is a convenient family of curves defined over the prime field which are easily seen to be pairwise non-isomorphic.

The computer first found the Hasse-Witt matrix $\{h_{ij}\}$, using the formula

$$h_{ij} = \text{coefficient of } x^{pi-j} \text{ in } [f(x)]^{\frac{1}{2}(p-1)}$$

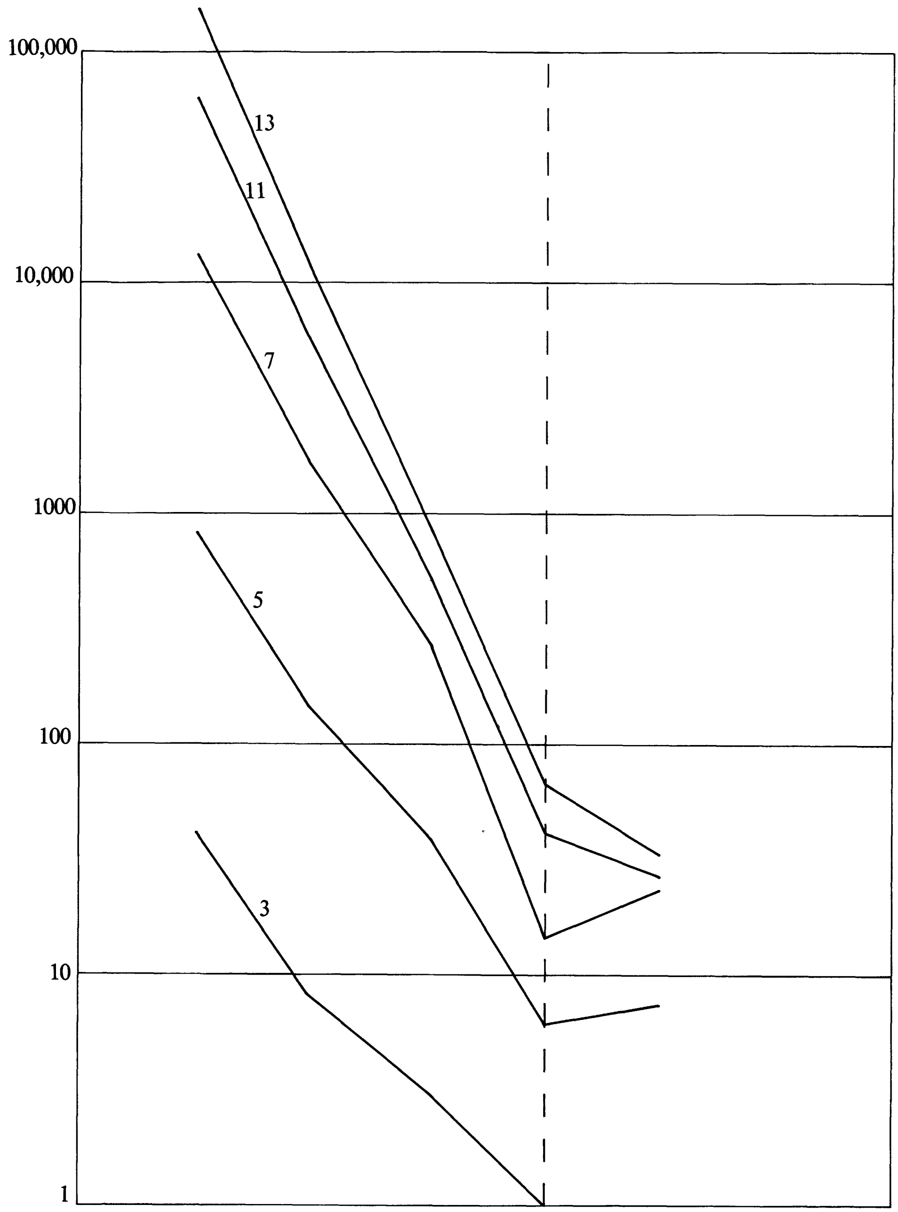
To distinguish between types 4 and 5, the computer then had to count the number of $\mathbb{F}_{p^3}$-rational points on the curve. A very special genus 3 curve is supersingular (of type 5) if and only if the number of $\mathbb{F}_{p^3}$-rational points is $\equiv 1 \pmod{p^3}$.

The number of curves in each type in this family of hyperelliptic curves was determined for $p = 3, 5, 7, 11, 13$:

p	Type 1	Type 2	Type 3	Type 4	Type 5
3	39	8	3	1	1
5	802	148	38	6	7
7	12320	1773	277	14	22
11	60205	5759	526	40	25
13	145548	11703	836	66	31

This table seems to support the conjecture, since the drop from type 4 to type 5 – if any – is never as sharp as in the other cases, when the dimension drop is clearly evident. This point can be made more visually with the help of logarithmic graph paper (see next page), which converts constant-ratio sequences to linear sequences. Note that all five graphs have a fair degree of linearity until the transition from type 4 to type 5, indicated by the vertical dotted line on the graph.

REMARK: An implicit assumption has been that there is no loss of generality in looking only at hyperelliptic genus 3 curves, which form a 5-dimensional subset in the 6-dimensional moduli space of all stable genus 3 curves. In fact, the transversality of the condition of hyperellipticity to the stratification is supported by the graph on p. 197, which shows that the dimension drop in Theorem 7 seems to be preserved under restriction to hyperelliptic curves.


100,000
10,000
1000
100
10
1
13
11
7
5
3

2. *Fermat hypersurfaces*

Let $F_{n,d,p} \subset \mathbb{P}^{n+1}_{\mathbb{F}_p}$ denote the n-dimensional 'Fermat hypersurface'

$$F_{n,d,p} = \{(x_0, \ldots, x_{n+1}) \in \mathbb{P}^{n+1}_{\mathbb{F}_p} | x_0^d + \ldots + x_{n+1}^d = 0\}.$$

If $p \not\mid d$, then $F_{n,d,p}$ is smooth. We suppose in what follows that $n \geqq 1$, $d \geqq 2$, $p \not\mid d$.

Algorithm for computing p-adic ordinals of the reciprocal roots of $Z(F_{n,d,p}/\mathbb{F}_p; t)$ (cf. Weil [61] and Katz [26]). Let $I = \{1, 2, \ldots, d-1\}$, and let

$$W = \{w = (w_0, \ldots, w_{n+1}) \in I^{n+2} | \sum w_i \equiv 0 \pmod{d}\}.$$

Let $|\,| : W \to \mathbb{Z}_+$ be defined by

$$|w| = \sum w_i.$$

Let

$$W_0 = \{w \in W |\, |w| = d\}.$$

Let $\{\,\} : \mathbb{Z} \to \{0, 1, \ldots, d-1\}$ be defined by

$$\{z\} \equiv z \pmod{d}.$$

Then, the group $(\mathbb{Z}/d\mathbb{Z})^x$ acts on W by

$$zw \underset{\text{def}}{=} (\{zw_0\}, \ldots, \{zw_{n+1}\}), \quad \text{any } z \in (\mathbb{Z}/d\mathbb{Z})^x.$$

In particular, $p \not\mid d$ acts on W. Let $o(z)$ denote the order of z in the multiplicative group $(\mathbb{Z}/d\mathbb{Z})^x$. Then:

(1) W_0 is in one-to-one correspondence with a basis of $H^n(\mathcal{O}_{F_{n,d,p}})$ in such a way that the Hasse-Witt matrix $H = \{h_{v,w}\}_{v,w \in W_0}$ is given by

$$h_{v,w} = \begin{cases} \text{a nonzero element of } \mathbb{F}_p \text{ if } w = pv \\ 0 \text{ otherwise.} \end{cases}$$

It follows that H has the form of a permutation matrix, and that

$$r_s(F_{n,d,p}) = \#\left(\bigcap_{i=1}^{o(p)} p^i W_0\right),$$

i.e., the stable rank of H equals the number of $w \in W_0$ whose orbits in W under the action of p remain in W_0. For example, $F_{n,d,p}$ has invertible Hasse-Witt if $p \equiv 1 \pmod{d}$. Conversely, suppose $W_0 \neq \emptyset$, i.e., $d \geqq n+2$, and suppose $p \not\equiv 1 \pmod{d}$. Then, if

$$m = \min\left(\left[\frac{d-1}{n+1}\right], \left[\frac{d-1}{\{p\}}\right]\right)$$

([ ] is the 'greatest integer' function), it is easy to see that

$$p(m, m, \ldots, m, d-(n+1)m) \notin W_0,$$

so that H is not invertible.

(2) W is in one-to-one correspondence with the reciprocal roots α_w of the numerator of $Z(F_{n,d,p}/\mathbb{F}_p; t)$ in such a way that the p-adic ordinals are given by

$$v_p(\alpha_w) = \frac{\sum_{i=1}^{o(p)} |p^i w|}{o(p)d} - 1.$$

In particular,

(a) For fixed n, d and w and variable p, $v_p(\alpha_w)$ only depends on the cyclic subgroup of $(\mathbb{Z}/d\mathbb{Z})^x$ generated by p.

(b) If p is a root of -1 modulo d, i.e., $p^{\frac{1}{2}o(p)} \equiv -1 \pmod{d}$, then

$$v_p(\alpha_w) = \tfrac{1}{2}n \qquad \text{for all } w \in W.$$

DEFINITION: *An n-dimensional complete intersection is supersingular if its Newton polygon* (*see p.* 122) *consists of one line of slope $\frac{1}{2}n$.* (*In the case of a smooth curve, this definition agrees with the earlier definition of supersingularity of its jacobian.*)

CONJECTURE (I): The converse of (b) is true, i.e., if $F_{n,d,p}$ is supersingular, then $p^{\frac{1}{2}o(p)} \equiv -1 \pmod{d}$.

LEMMA 14: *The following two variants of Conjecture* (*I*) *are equivalent to it*:

CONJECTURE (II): For $m \in \{1, 2, \ldots, d-1\}$, let S_m denote the average of the numbers $\{p^i m\}$, $i = 1, 2, \ldots, o(p)$. Then

$$\text{all the } S_m = \tfrac{1}{2}d \Rightarrow p \text{ is a root of } -1 \text{ modulo } d.$$

CONJECTURE (III): Conjecture (I) holds when $n = 1$.

PROOF: Obviously $I \Rightarrow III$.

$III \Rightarrow II$. Suppose all the $S_m = \frac{1}{2}d$. The p-adic ordinals of the reciprocal roots of $Z(F_{1,d,p}/\mathbb{F}_p; t)$ are given by

$$\begin{aligned} v_p(\alpha_w) &= \frac{1}{o(p)d} \sum_{i=1}^{o(p)} (\{p^i w_0\} + \{p^i w_1\} + \{p^i w_2\}) - 1 \\ &= \frac{1}{o(p)d} (S_{w_0} o(p) + S_{w_1} o(p) + S_{w_2} o(p)) - 1 \\ &= \frac{1}{o(p)d} (\tfrac{3}{2} d o(p)) - 1 = \tfrac{1}{2}. \end{aligned}$$

Hence, by Conjecture III, $p^{\frac{1}{2}o(p)} \equiv -1 \pmod{d}$.

II $\Rightarrow$ I. Suppose p is not a root of -1 modulo d. By Conjecture II, there exists an m such that $S_m \neq \frac{1}{2}d$. Let m_1 be any number in $\{1, 2, \ldots, d-1\}$ such that S_{m_1} is minimal among all the S_m. Let $m_2 = d - m_1$. Clearly $S_{m_2} = d - S_{m_1}$ is maximal among all the S_m. Obviously, $S_{m_1} < \frac{1}{2}d$. Consider three cases:

(i) For some such choice of m_1 for which S_{m_1} is minimal, we have:

$$(n+1)m_1 \not\equiv 0 \pmod{d}.$$

Then let $m' = d - \{(n+1)m_1\}$, and let

$$w = (\overbrace{m_1, \ldots, m_1}^{n+1}, m').$$

Now

$$\begin{aligned} v_p(\alpha_w) &= \frac{\sum_{i=1}^{o(p)} |p^i w|}{o(p)d} - 1 \\ &= \frac{1}{d} \sum_{j=0}^{n+1} S_{w_j} - 1 \\ &= \frac{1}{d} [(n+1) S_{m_1} + S_{m'}] - 1 \end{aligned}$$

$$\leqq \frac{1}{d}[(n+1)S_{m_1}+S_{m_2}]-1$$

$$= \frac{1}{d}(nS_{m_1}+d)-1$$

$$= \frac{n}{d}S_{m_1}$$

$$< \tfrac{1}{2}n.$$

(ii) $n \geqq 3$, and for all such choices of m_1

$$(n+1)m_1 \equiv 0 \pmod{d}.$$

Choose any $m', m'' \in \{1, 2, \ldots, d-1\}$ such that

$$nm_1 + m' + m'' \equiv 0 \pmod{d}.$$

Let

$$w = (\overbrace{m_1, \ldots, m_1}^{n}, m', m'').$$

Then

$$v_p(\alpha_w) = \frac{1}{d}\sum_{j=0}^{n+1} S_{w_j} - 1$$

$$= \frac{1}{d}(nS_{m_1}+S_{m'}+S_{m''})-1$$

$$\leqq 1 + \frac{n-2}{d}S_{m_1}$$

$$< \tfrac{1}{2}n,$$

since $n \geqq 3$.

(iii) $n = 1$ or 2, and for all such choices of m_1

$$(n+1)m_1 \equiv 0 \pmod{d}.$$

If $n = 1$, then $m_1 = \frac{1}{2}d$, and $S_{m_1} = \frac{1}{2}d$, a contradiction. Hence $n = 2$. Then $m_1 = \frac{1}{3}d$ or $\frac{2}{3}d$. We have $p \equiv 1 \pmod 3$, since if $p \equiv 2 \pmod 3$ we would have $S_{m_1} = \frac{1}{2}d$. Thus, $m_1 = \frac{1}{3}d$, and $m_2 = \frac{2}{3}d$. Since $p \not\equiv 1 \pmod{d}$, this means $d \geqq 6$, so that $m_1 \geqq 2$. Let

$$w = (m_1, m_1, 1, m_1 - 1).$$

Notice that in case iii with $n = 2$ the only possible choice for the pair (m_1, m_2) is $(\frac{1}{3}d, \frac{2}{3}d)$. That is, for $m \neq \frac{1}{3}d, \frac{2}{3}d$, we have $S_{m_1} < S_m < S_{m_2}$. Hence

$$v_p(\alpha_w) = \frac{1}{d}\sum_{j=0}^{3} S_{w_j} - 1 = \frac{1}{d}(2S_{m_1} + S_1 + S_{m_1 - 1}) - 1$$
$$< \frac{1}{d}(2S_{m_1} + S_{m_2} + S_{m_2}) - 1 = \frac{1}{d}(2d) - 1 = 1 = \tfrac{1}{2}n.$$

In all three cases $F_{n,d,p}$ is not supersingular. QED

PARTIAL CONVERSE OF PROPERTY 2(b), p. 199: (1) If $o(p)$ is odd, then $F_{n,d,p}$ is not supersingular. (2) If $o(p) \equiv 2 \pmod 4$ and $p^{\frac{1}{2}o(p)} \not\equiv -1 \pmod{d}$, then $F_{n,d,p}$ is not supersingular.

PROOF: (1) If d is a power of 2, then $o(p)$ odd $\Rightarrow p \equiv 1 \pmod{d}$ and (1) is trivial. So let b be an odd number such that $d = bc$. If $F_{n,d,p}$ were supersingular, by the proof of Lemma 14 we would have

$$\sum_{i=1}^{o(p)} \{p^i c\} = o(p)S_j = o(p)\frac{d}{2} = \frac{o(p)b}{2}c.$$

Since c divides the sum on the left, it follows that $2|o(p)b$. But $o(p)$ and b are both odd.

(2) Let d be the least degree for which the assertion is false. d can not be an odd prime power or twice an odd prime power, since then $(\mathbb{Z}/d\mathbb{Z})^x$ would be a cyclic group and

$$o(p) \text{ even} \Rightarrow p^{\frac{1}{2}o(p)} \equiv -1 \pmod{d}.$$

If $d = 2^r$ is a power of 2, then $o(p) = 2$, and so $p \equiv 2^{r-1} \pm 1 \pmod{2^r}$, $r > 2$. But then

$$\sum_{i=1}^{o(p)} \{p^i\} = 2^{r-1} \quad \text{or} \quad 2^{r-1} + 2 \neq o(p)\frac{d}{2}.$$

Hence, there exist relatively prime numbers $b_1, b_2 > 2$ such that $d = b_1 b_2$. Let $j = 1$ or 2. Since for all $m \in \{1, 2, \ldots, b_j - 1\}$ we have

$$\sum_{i=1}^{o(p)} \left\{ p^i m \frac{d}{b_j} \right\} = \frac{o(p)}{2} d,$$

it follows that

$$\sum_{i=1}^{o(p)} \frac{\left\{ p^i m \dfrac{d}{b_j} \right\}}{d/b_j} = \frac{o(p)}{2} b_j.$$

But the summand on the left is the least residue of $p^i m$ in $\mathbb{Z}/b_j\mathbb{Z}$. Since the order $o_{b_j}(p)$ of p in $(\mathbb{Z}/b_j\mathbb{Z})^x$ divides $o(p)$, we have

$$\begin{aligned} \sum_{i=1}^{o_{b_j}(p)} \frac{\{p^i md/b_j\}}{d/b_j} &= \frac{o_{b_j}(p)}{o(p)} \sum_{i=1}^{o(p)} \frac{\{p^i md/b_j\}}{d/b_j} \\ &= \frac{o_{b_j}(p)}{2} b_j. \end{aligned}$$

By the proof of Lemma 14, $F_{n, b_j, p}$ is supersingular. But by part (1) and the induction assumption, it follows that $o_{b_j}(p)$ is even and $p^{\frac{1}{2}o_{b_j}(p)} \equiv -1 \pmod{b_j}$. Hence $p^{\frac{1}{2}o(p)} \equiv -1 \pmod{b_j}$, $j = 1, 2$. Since $d = b_1 b_2$ with b_1, b_2 relatively prime, we have $p^{\frac{1}{2}o(p)} \equiv -1 \pmod{d}$, a contradiction.

QED

Remarks: (1) Note that the remaining case $4 | o(p)$ but $p^{\frac{1}{2}o(p)} \not\equiv -1 \pmod{d}$ implies that d must either be divisible by 16 or else a multiple at least three times a prime of the form $4m+1$, e.g., $d = 15, 16, 20, 30, 32, \ldots$. The conjecture was verified by computer for all $d < 500$.

(2) We can prove the conjecture if $o(p) = 4$, but the proof is longer, and will be omitted.

(3) The Fermat hypersurfaces with $p^{\frac{1}{2}o(p)} \equiv -1 \pmod{d}$ occur naturally as an example of supersingularity because they have even more automorphisms than other Fermat hypersurfaces. For example, if $d = p^{\frac{1}{2}o(p)} + 1$, then over the field $\mathbb{F}_{p^{o(p)}}$ the hypersurface $F_{n,d,p}$ is taken to itself by the projective transformations $x_j \mapsto \sum a_{ij} x_i$, where $\{a_{ij}\}$ is a unitary matrix with respect to the conjugation $a \mapsto a^{p^{\frac{1}{2}o(p)}}$ (cf. Tate, [57], p. 101–102, where these hypersurfaces are cited in a slightly different context).

The tables on the next page give the slopes of the Newton polygons

Table of Newton Polygons for $F_{1,d,p}$, $d \leqq 20$, all p

Note:

1. The Newton polygon only depends on cyclic sub gp of p in $(\mathbb{Z}/d\mathbb{Z})^x$.
2. Because of the symmetry, horizontal lengths of the segments are only listed for slopes $m/n \leqq \frac{1}{2}$; the slope $1-m/n$ has same length.
3. The trivial subgp $\{1\}$ is omitted; it has g slopes 0 and g slopes 1.
4. Any subgp containing -1 is omitted; it has all slopes $\frac{1}{2}$.

degree d	cyclic subgp	slope	horizontal length
7	2, 4, 1	0	6
		$\frac{1}{3}$	9
8	3, 1	0	12
		$\frac{1}{2}$	18
8	5, 1	0	9
		$\frac{1}{2}$	24
9	4, 7, 1	0	1
		$\frac{1}{3}$	27
11	3, 9, 5,	$\frac{1}{5}$	15
	4, 1	$\frac{2}{5}$	30
12	5, 1	0	27
		$\frac{1}{2}$	56
12	7, 1	0	28
		$\frac{1}{2}$	54
13	3, 9, 1	0	21
		$\frac{1}{3}$	45
14	9, 11, 1	0	6
		$\frac{1}{3}$	72
15	2, 4, 8, 1	0	36
		$\frac{1}{4}$	36
		$\frac{1}{2}$	38
15	4, 1	0	55
		$\frac{1}{2}$	72
15	7, 4, 13, 1	0	1
		$\frac{1}{4}$	36
		$\frac{1}{2}$	108
15	11, 1	0	36
		$\frac{1}{2}$	110
16	3, 9,	0	24
	11, 1	$\frac{1}{4}$	48
		$\frac{1}{2}$	66
16	5, 9,	0	9
	13, 1	$\frac{1}{4}$	48
		$\frac{1}{2}$	96
16	7, 1	0	48
		$\frac{1}{2}$	114
16	9, 1	0	57
		$\frac{1}{2}$	96
18	7, 13, 1	0	28
		$\frac{1}{3}$	108
19	4, 16, 7,	$\frac{1}{3}$	45
	9, 17, 11,	$\frac{4}{9}$	108
	6, 5, 1		
19	7, 11, 1	0	45
		$\frac{1}{3}$	108
20	3, 9, 7, 1	0	48
		$\frac{1}{4}$	48
		$\frac{1}{2}$	150
20	9, 1	0	75
		$\frac{1}{2}$	192
20	11, 1	0	96
		$\frac{1}{2}$	150
20	13, 19,	0	3
	17, 1	$\frac{1}{4}$	48
		$\frac{1}{2}$	240

of all $F_{1,d,p}$ for $d \leqq 20$ as a function of p – more precisely, as a function of the cyclic subgroups of $(\mathbb{Z}/d\mathbb{Z})^x$.

3. *Artin-Schreier curves*

Let C be the Artin-Schreier curve which is the nonsingular model of

$$y^2 = x^q - x, \qquad q = p^a, \qquad p > 2,$$

defined over $k = \mathbb{F}_q$. Then its zeta-function $Z(C/\mathbb{F}_q; t)$ is given by

$$Z(C/\mathbb{F}_q; t) = \frac{(1-(-1)^{\frac{1}{2}(q-1)}qt^2)^{\frac{1}{2}(q-1)}}{(1-t)(1-qt)}.$$

Proof: The assertion is that the reciprocal roots λ_j, $j = 1, \ldots, 2g$ ($g = \frac{1}{2}(q-1) =$ genus of C), of the numerator of $Z(C/\mathbb{F}_q; t)$ are given by

$$\lambda_j = i^{\frac{1}{2}(q-1)}\sqrt{q}, \qquad j = 1, \ldots, g \ (i = \sqrt{-1})$$
$$\lambda_j = -i^{\frac{1}{2}(q-1)}\sqrt{q}, \qquad j = g+1, \ldots, 2g.$$

If N_s is the number of $\mathbb{F}_{q^s}$-rational points on C, then

$$N_s = 1 + q^s - \sum_{j=1}^{2g} \lambda_j^s \quad \text{and} \quad Z(C/\mathbb{F}_q; t) = \exp\left(\sum_{s=1}^{\infty} N_s t^s/s\right),$$

so that our assertion is equivalent to:

$$\begin{aligned} N_s &= 1 + q^s - \tfrac{1}{2}(q-1)i^{\frac{1}{2}(q-1)s}q^{\frac{1}{2}s} - \tfrac{1}{2}(q-1)(-1)^s i^{\frac{1}{2}(q-1)s}q^{\frac{1}{2}s} \\ &= \begin{cases} 1 + q^s, & \text{if } s \text{ is odd} \\ 1 + q^s - (-1)^{\frac{1}{2}(q-1)s'}q^{s'}(q-1), & \text{if } s = 2s' \text{ is even.} \end{cases} \end{aligned}$$

We first note that for $s = 1, 2, 3, \ldots$ the nonsingular model C has exactly one $\mathbb{F}_{q^s}$-rational point over the point at infinity on the plane curve given by $y^2 = x^q - x$. Hence, we are reduced to computing $N'_s = N_s - 1$ for the nonsingular affine plane curve $y^2 = x^q - x$.

Case (1): *s iss odd.* Then $x = 0$ gives the one point $x = y = 0$. If $x \neq 0$, we let x run through a set of $(q^s-1)/(q-1)$ multiplicative coset representatives of $\mathbb{F}_{q^s}^\times/\mathbb{F}_q^\times$. We claim that there are exactly $q-1$ solutions (y, ax), $y \in \mathbb{F}_{q^s}$, $a \in \mathbb{F}_q^\times$, for each coset representative. For the one coset with $x \in \mathbb{F}_q^\times$, we have the $q-1$ solutions $(0, ax)$, $a \in \mathbb{F}_q^\times$. For the other coset representatives x, we have $x^q - x \neq 0$, and $(ax)^q - ax = a(x^q - x)$ is a square in $\mathbb{F}_{q^s}$ if and only if either both a and $(x^q - x)$ are squares in $\mathbb{F}_{q^s}$ or neither one is. Thus, regardless of whether or not $x^q - x$ is a square, there are precisely $\frac{1}{2}(q-1)$ values of $a \in \mathbb{F}_q^\times$ for which $(ax)^q - ax$ is a square, since

$$a \text{ is a square in } \mathbb{F}_{q^s} \Leftrightarrow a \text{ is a square in } \mathbb{F}_q.$$

(Here is where we use the fact that s is odd.) Each of these $\frac{1}{2}(q-1)$ values of ax gives 2 solutions $(\pm y, ax)$.

We conclude that N'_s equals:

$$1+\left(\frac{q^s-1}{q-1}\right)(q-1) = q^s.$$

Case (2): $s = 2s'$ *is even.* Let $F' = \mathbb{F}_{q^{s'}} \subset \mathbb{F}_{q^s}$, i.e., $\mathbb{F}_{q^s}/F'$ is a quadratic extension. Let $u \in F'$ be a nonsquare in F', so that $\mathbb{F}_{q^s} = F'(\alpha)$ where $\alpha^2 = u$. Next, let β be a square root of -1 in $\mathbb{F}_{q^s}$ (which exists because s is even). Then

$$\beta \notin F' \Leftrightarrow s' \text{ is odd and } \tfrac{1}{2}(q-1) \text{ is odd.}$$

(We recall that -1 is a square in a finite field if and only if the number of elements in the field is $\equiv 1 \pmod 4$.)

If we let $x = x_1+x_2\alpha$, $y = y_1+y_2\alpha$, $x_i, y_i \in F'$, then the equation $y^2 = x^q-x$ becomes

$$(*) \qquad (y_1^2+uy_2^2)+2y_1y_2\alpha = (x_1^q-x_1)+(x_2^q u^{\frac{1}{2}(q-1)}-x_2)\alpha$$

Since t is a nonsquare in F', it follows that $u^{\frac{1}{2}(q^{s'}-1)} = -1$. Hence the additive homomorphism $\varphi : F' \to F'$ given by

$$x_2 \mapsto x_2^q u^{\frac{1}{2}(q-1)} - x_2$$

is bijective, since if $x_2 \neq 0$ were in its kernel we would have

$$u^{\frac{1}{2}(q^{s'}-1)} = (u^{\frac{1}{2}(q-1)})^{(q^{s'}-1)/(q-1)} = (x_2/x_2^q)^{(q^{s'}-1)/(q-1)} = 1/x_2^{q^{s'}-1} = 1.$$

Therefore, each solution $x_1, y_1, y_2 \in F'$ to

$$(**) \qquad y_1^2+uy_2^2 = x_1^q-x_1$$

gives precisely one solution to (*) by setting

$$x_2 = \varphi^{-1}(2y_1y_2).$$

Thus N'_s is the number of solutions to (**) in F'.

We consider two sub-cases.

Case (2*a*): $\beta \in F'$. Replacing y_2 by βy_2 transforms (**) to

$$(***) \qquad x_1^q - x_1 = y_1^2 - uy_2^2 = \mathbb{N}_{\mathbb{F}_{q^s/F}}(y_1 + y_2\alpha),$$

where $\mathbb{N}_{\mathbb{F}_{q^s/F'}}$ designates the norm from $\mathbb{F}_{q^s}$ to F'. Now

$$x_1^q - x_1 = 0 \Leftrightarrow x_1 \in \mathbb{F}_q,$$

so that $x_1^q - x_1 = 0$ corresponds to q solution sets $(x_1, 0, 0)$, $x_1 \in \mathbb{F}_q$.

Suppose $x_1^q - x_1 \neq 0$. Let $\gamma = x_1^q - x_1$. Hence, if $N_s''(\gamma)$ is the number of solutions of

$$\mathbb{N}_{\mathbb{F}_{q^s/F'}}(y) = \gamma, \qquad y \in \mathbb{F}_{q^s}$$

and if $N_s'' = N_s''(\gamma)$ is independent of $\gamma \in F'^{\times}$, it follows that

$$N_s' = q + (q^{s'} - q)N_s''.$$

But $\mathbb{N}_{\mathbb{F}_{q^s/F'}}$ is a multiplicative homomorphism from $\mathbb{F}_{q^s}^{\times}$ to $F'^{\times}$. Moreover, it is surjective, since the set

$$\{y_1^2\} \cup \{-uy_2^2\} = \{y_1^2\} \cup \{uy_2^2\} \qquad (\text{since } \beta \in F')$$

runs through all elements of $F'^{\times}$. Thus, for $\gamma \in F'^{\times}$ we have

$$N_s''(\gamma) = \frac{q^s - 1}{q^{s'} - 1} = q^{s'} + 1,$$

and

$$\begin{aligned} N_s &= 1 + N_s' \\ &= 1 + q + (q^{s'} - q)N_s'' \\ &= 1 + q + (q^{s'} - q)(q^{s'} + 1) \\ &= 1 + q^s - q^{s'}(q - 1). \end{aligned}$$

Case (2*b*): $\beta \notin F'$. We may take $u = -1$, i.e., $\alpha = \beta$. Then (**) becomes

$$(y_1 + y_2)(y_1 - y_2) = x_1^q - x_1.$$

The nonsingular linear transformation

$$\begin{aligned} y_1' &= y_1 + y_2 \\ y_2' &= y_1 - y_2 \end{aligned}$$

allows us to replace this equation with the equation

$$y_1' y_2' = x_1^q - x_1 .$$

For each $x_1 \in F'$ such that $x_1^q - x_1 \neq 0$, this equation has $q^{s'} - 1$ solutions (y_1', y_2'), one for each $y_1' \in F'^{\times}$. If $x_1^q - x_1 = 0$, it has $2q^{s'} - 1$ solutions $(0, y_2')$, $(y_1', 0)$. Hence

$$\begin{aligned} N_s' &= (q^{s'} - 1)q^{s'} + q^{s'}(\#\text{ of } x_1 \in F' \text{ such that } x_1^q - x_1 = 0) \\ &= (q^{s'} - 1)q^{s'} + q^{s'} \cdot q, \end{aligned}$$

and

$$N_s = 1 + N_s' = 1 + q^s + q^{s'}(q-1).$$

In both cases (2a) and (2b) we have

$$N_s = 1 + q^s - (-1)^{\frac{1}{2}(q-1)s'} q^{s'}(q-1). \qquad \text{QED}$$

Corollary: *For any odd prime p and for $g = \frac{1}{2}(p^a - 1)$, there exists a nonsingular supersingular curve of genus g in characteristic p.*

Remark: If the same curve C with equation $y^2 = x^q - x$ is considered as defined over the prime field $\mathbb{F}_p$, then the same technique shows that

$$(1-t)(1-pt)Z(C/\mathbb{F}_p; t) = \left[\frac{\prod_{j|a'} \left(1 - [(-1)^{\frac{1}{2}(q-1)} p^{2^r} t^{2^{r+1}}]^j\right)^{\frac{1}{j}\sum_{k|j} \mu\left(\frac{j}{k}\right) p^{2^r k}}}{1 - (-1)^{\frac{1}{2}(q-1)} p^{2^r} t^{2^{r+1}}} \right]^{1/2^{r+1}}$$

where $q = p^a$; $a = 2^r a'$, $2 \nmid a'$; and μ is the Möbius function:

$$\mu(n) = \begin{cases} 0 \text{ if } n \text{ has a square factor} \\ (-1)^{\#\text{ of prime factors}}, \text{ otherwise.} \end{cases}$$

Example: If C is the genus 4 hyperelliptic curve $y^2 = x^9 - x$ in characteristic 3, then

$$Z(C/\mathbb{F}_9; t) = \frac{(1-9t^2)^4}{(1-t)(1-9t)}$$

$$Z(C/\mathbb{F}_3; t) = \frac{(1-9t^4)^2}{(1-t)(1-3t)}.$$

C is an example of a nonsingular supersingular genus 4 curve in characteristic 3.

4. *Stratification by the full Newton polygon*

In this paper we have systematically studied only the unit root part of the Newton polygon, i.e., the mod p zeta-function. For this reason we have only needed mod p data, namely the Hasse-Witt matrix. A new set of finer (and more difficult) questions arises if we concern ourselves with the entire Newton polygon.

The simplest cases show that the Hasse-Witt matrix is the wrong invariant for answering such questions.

EXAMPLE: Consider the following three nonsingular genus 3 curves define over $\mathbb{F}_3$:

C_1 is the Fermat plane curve $X_0^4 + X_1^4 + X_2^4 = 0$;

C_2 is the nonsingular model of $Y^2 = f_2(X) = X^7 + 1$;

C_3 is the nonsingular model of $Y^2 = f_3(X) = X^7 - X + 1$.

All have nilpotent Hasse-Witt. C_1 and C_2 are supersingular: C_1 by section 2 above, C_2 by direct computation of the zeta-function. C_3 is Manin's example in [34] of a curve with slopes $\frac{1}{3}$, $\frac{2}{3}$. On the one hand, C_1 has Hasse-Witt identically zero by section 2, while C_2 and C_3 both have Hasse-Witt of rank 2 (i.e., isomorphism type $P = (0, 3)$). In fact, the Hasse-Witt $\{h_{i,j;m}\}$ of C_m, $m = 2, 3$, is given by: $h_{i,j;m}$ equals the coefficient of X^{3i-j} in $f_m(X)$. Thus:

$$H(C_2) = \begin{pmatrix} 0 & 0 & 1 \\ 0 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix}; \qquad H(C_3) = \begin{pmatrix} 0 & -1 & 1 \\ 0 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix}.$$

Thus, two curves can have the same Hasse-Witt and different Newton polygons, or the same Newton polygon and different Hasse-Witt matrices (i.e., Hasse-Witt matrices of different isomorphism types).

NOTATION: Let

$$0 \leqq \frac{m_1}{n_1} < \frac{m_2}{n_2} < \ldots < \frac{m_h}{n_h} = \tfrac{1}{2}$$

be a sequence of fractions in lowest terms (if $m_1 = 0$ we take $n_1 = 1$); let $r_i > 0$, $i = 1, \ldots, h-1$, $r_h \geqq 0$; and let

$$g = \sum_{i=1}^{h-1} r_i n_i + r_h.$$

Let $NP(\sum_{i=1}^{h} r_i(m_i, n_i))$ denote the Newton polygon with segments of slope m_i/n_i and $1-(m_i/n_i)$ each having horizontal length $r_i n_i$, $i = 1, \ldots, h$. Thus, any Newton polygon can be uniquely written as a 'sum' $\sum r_i N_i$ of 'simple' Newton polygons N_i. Here if $m_1 = 0$, then r_1 is the length of the unit root part.

Remark: When we talk of a 'Newton polygon', we mean, of course, a convex polygonal line connecting $(0,0)$ with $(2g, g)$ and having the required symmetry. We note that Tate [58] and Honda [17] proved a conjecture of Manin that any Newton polygon actually occurs as the Newton polygon of the zeta-function of an abelian variety. According to Oort and H. W. Lenstra, Jr. [64], any Newton polygon except for the supersingular Newton polygon occurs as the Newton polygon of a *simple* abelian variety; in [50], Oort proves that an abelian variety is supersingular if and only if it is isogenous to a product of supersingular elliptic curves.

Further, let $S(NP) \subset M_g$ denote the set of g-dimensional principally polarized abelian varieties whose zeta-function has Newton polygon NP. Let $\bar{S}(NP)$ denote the Zariski closure of $S(NP)$ in M_g. (Recall that these sets are actually in the fine moduli scheme of principally polarized abelian varieties with level N structure, but we shall omit mention of the level N structure in what follows.) Let $CD(NP)$ denote the codimension of (a highest dimensional irreducible component of) the set $\bar{S}(NP)$. For example, for elliptic curves we have

$$\bar{S}((0,1)) = \text{the whole } j\text{-line}; \;\; CD((0,1)) = 0$$

$$\bar{S}((1,2)) = \text{a finite set of points}; \;\; CD((1,2)) = 1.$$

Conjecture: $CD(\sum_{i=1}^{h} r_i(m_i, n_i)) = \sum_{i=1}^{h} r_i CD((m_i, n_i))$.

Remarks: (1) The conjecture in section 1, p. 194, is the following special case of this conjecture:

$$CD(g(1,2)) = g.$$

(In our notation $NP(g(1,2))$ is the supersingular Newton polygon.)

(2) In the case of the 'Hodge polygon' $NP(g(0,1))$, this conjecture is the well-known generic invertibility of the Hasse-Witt matrix of principally polarized abelian varieties.

(3) Theorem 7 of Chapter IV implies the conjecture if the unit root part is at least $g-2$ (i.e., $m_1 = 0$, $r_1 \geqq g-2$), since then the Newton polygon is determined by the unit root part (p-rank).

In addition to the codimensions of the sets $\bar{S}(NP)$, it would be interesting to know how they intersect – that is, what sequences of Newton polygons can be obtained by successive specializations in the moduli space.

DEFINITION: *A partial ordering on the set of Newton polygons is introduced by*:

$$NP_1 \leqq NP_2 \Leftrightarrow \text{ all points on } NP_1 \text{ are on or below } NP_2.$$

A theorem of Grothendieck (cf. [7], p. 91) says that specialization from NP_1 to NP_2 is only possible if $NP_1 \leqq NP_2$, i.e.,

$$\bar{S}(NP_1) \cap S(NP_2) \neq \emptyset \Rightarrow NP_1 \leqq NP_2.$$

Conversely, it may be asked whether all totally ordered sequences of Newton polygons can be realized by successive specializations of principally polarized abelian varieties.

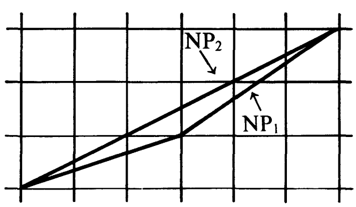
CONJECTURE: If $NP_1 < NP_2 < \ldots < NP_h$, then

$$\overline{\overline{S(NP_1)} \cap S(NP_2)} \cap S(NP_3) \cap \ldots \cap S(NP_h) \neq \emptyset.$$

(The bar denotes Zariski closure.) In particular, the relation 'NP_1 specializes to NP_2' is transitive (which is far from *a priori* obvious).

Note that the intersection in the conjecture can only be nonempty if $\dim S(NP_1) \geqq h-1$.

This conjecture seems to be unknown even in the simplest case when



it does not follow from the p-rank (unit root part) stratification, namely: $g = 3$, $NP_1 = NP((1,3))$, $NP_2 = NP(3(1,2))$. In this case, whereas the conjecture on p. 194 claimed that *not all* points of $S(NP_2)$ are specializations from $S(NP_1)$, this latest conjecture claims that *some* points of $S(NP_2)$ are such specializations.

REMARK: This 'first nontrivial case' of the conjecture follows in characteristic $p = 3$ by computations of Manin (cf. [34], p. 77–78). Namely, the family of hyperelliptic curves

$$Y^2 = X^7 + \lambda X + 1$$

parametrized by λ has nilpotent Hasse-Witt matrix. Since Manin's example ($\lambda = -1$) has Newton polygon $NP_1 = NP((1,3))$, it follows by the Grothendieck specialization theorem that the generic point of the family has Newton polygon NP_1. But the specialization $\lambda = 0$ is supersingular. Hence the specialization from NP_1 to NP_2 occurs in characteristic 3.

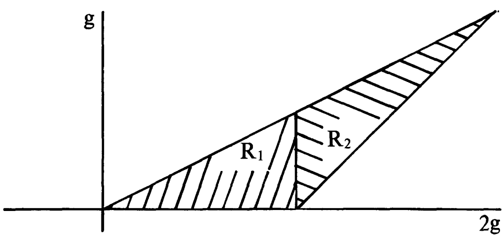
LEMMA 15: *The length of any maximal totally ordered sequence of Newton polygons of genus g is equal to*

$$1 + \sum_{i=1}^{g} \left[\frac{i+1}{2}\right] = \begin{cases} \frac{1}{4}g^2 + \frac{1}{2}g + 1 & \text{if } g \text{ is even} \\ \frac{1}{4}(g+1)^2 + 1 & \text{if } g \text{ is odd.} \end{cases}$$

PROOF: Let

$$R_1 = \{(a,b) \in \mathbb{Z}^2 | 0 < a \leqq g,\ 0 \leqq b < \tfrac{1}{2}a\};$$

$$R_2 = \{(a,b) \in \mathbb{Z}^2 | g \leqq a \leqq 2g, a - g \leqq b < \tfrac{1}{2}a\}.$$



Define the isomorphism $(a,b) \mapsto (a,b)'$ from R_1 to R_2 by

$$(a,b)' = (2g - a, g - a + b).$$

Define a map Φ from Newton polygons to subsets of R_1 and a map φ from Newton polygons to $\mathbb{Z}_+$ by

$$\Phi : NP \mapsto \{\text{points in } R_1 \text{ strictly below } NP\}$$
$$\varphi : NP \mapsto \#\,(\Phi(NP)).$$

Note that Φ and φ are strictly order-preserving, i.e.,

$$NP_1 < NP_2 \Rightarrow \Phi(NP_1) \subsetneqq \Phi(NP_2) \quad \text{and} \quad \varphi(NP_1) < \varphi(NP_2),$$

because a Newton polygon is determined by the points in $\mathbb{Z}^2$ through which it passes, so that at least one of the lattice points on NP_1 must be strictly below NP_2. Since

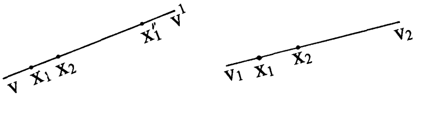
$$\varphi\ (\text{Hodge polygon}) = 0$$
$$\varphi\ (\text{supersingular Newton polygon}) = \#\, R_1 = \sum_{i=1}^{g} \left[\frac{i+1}{2}\right],$$

the lemma follows if we show that, if $NP_1 < NP_2$, then

$$\exists NP_3 \quad \text{with} \quad NP_1 < NP_3 < NP_2 \Leftrightarrow \varphi(NP_2) - \varphi(NP_1) > 1.$$

$\Rightarrow$ This follows immediately from the fact that φ is strictly order preserving.

$\Leftarrow$ Let x_1, x_2 be two lattice points in $\Phi(NP_2) - \Phi(NP_1)$. For $j = 1, 2$, let $NP_{3,j}$ be the convex hull of NP_2 and the two points x_j, x'_j. Clearly, $NP_{3,j}$ is an admissible Newton polygon, i.e., it has the required symmetry. Moreover, $N_{3,j} < NP_2$. In addition, $NP_{3,j} \geqq NP_1$, since NP_1 is convex and passes on or below x_j, x'_j and all points of NP_2. We must show that this inequality is strict for $j = 1$ or 2. It suffices to show that $NP_{3,1} \neq NP_{3,2}$. If $NP_{3,1} = NP_{3,2}$, then x_1 is on a segment joining x_2 either to x'_2 or to a vertex of NP_2, and x_2 is on a segment joining x_1 either to x'_1 or to a vertex of NP_2. In all possible cases, x_1 and x_2



are both on some segment joining two vertices of NP_2. By the convexity of NP_2, x_1 and x_2 can not be strictly below NP_2, a contradiction. QED

COROLLARY: *The analogous conjecture for the* $(3g-3)$*-dimensional moduli space of stable curves is false.*

In fact, if $g \geqq 9$, then the length of a maximal totally ordered sequence of Newton polygons is greater than $(3g-3)+1$, so there are not enough dimensions in the moduli space for the intersection in the conjecture to be nonempty. That is, there must be other criteria besides the Grothendieck specialization theorem for the possibility of sequences of specializations of stable curves.

Note that Lemma 15 does *not* contradict the conjecture for principally polarized abelian varieties, which have enough moduli, namely $\frac{1}{2}g(g+1)$. In general, the question of stratification for stable curves is probably much more complicated than for principally polarized abelian varieties. One preliminary step might be to extend the Grothendieck specialization theorem to all (not necessarily smooth) stable curves.

The first problem in doing this is that even the degree of the numerator of $Z(C;t)$ drops when the genus g curve develops singularities. For example, as remarked on p. 147, the simplest example of curves of triangular genera $g = \frac{1}{2}(d-1)(d-2)$ with invertible Hasse-Witt matrix is the union $C = L_1 \cup \ldots \cup L_d$ of d lines in general position in $\mathbb{P}^2$. But consider its actual zeta-function, which is easily computed by the 'exclusion-inclusion principle':

$$Z(C;t) = \prod_i Z(L_i;t) / \prod_{i,j} Z(L_i \cap L_j;t),$$

where the zeta-functions are computed over a common field of definition $\mathbb{F}_q$ of all the L_i's. Thus

$$Z(C/\mathbb{F}_q;t) = \frac{(1-t)^g}{(1-t)(1-qt)^d}.$$

On the one hand, the mod p zeta-function looks like the mod p zeta-function of any nonsingular genus g curve; in fact, the base-changing theorem for coherent cohomology, applied in Chapter I, shows that no mod p 'discontinuity' can be expected at singular curves. On the other hand, the definition of $P_1(C;t)$ on p. 122 as the numerator of $Z(C;t)$ must be modified if we want to attach the genus g Hodge polygon to this curve.

In this way, for a possibly singular stable curve C, considerations of reciprocity (i.e., the roots permute under $t \mapsto q/t$) force us to make the following definition of $P_1(C;t)$:

$$P_1(C;t) = Z(C;t)(1-t)(1-qt)^{1+\#\text{ of singular points}}$$

It is easy to see that this is the correct definition. In fact, suppose C is a stable curve with r irreducible components $C_1, \ldots, C_r$ and with s singular points. Let $N_1, \ldots, N_r$ be normalizations of $C_1, \ldots, C_r$, respectively. Then clearly

$$g = \text{genus }(C) = \sum_{i=1}^{r} \text{genus }(N_i) + s + 1 - r.$$

On the other hand,

$$Z(C/\mathbb{F}_q;t) = (1-t)^s \prod_{i=1}^{r} Z(N_i/\mathbb{F}_q;t)$$

and

$$Z(C/\mathbb{F}_q;t)(1-t)(1-qt)^{1+s}$$
$$= \prod_{i=1}^{r} [Z(N_i/\mathbb{F}_q;t)(1-t)(1-qt)] \cdot [(1-t)(1-qt)]^{g-\Sigma\,\text{genus}(N_i)}$$

is a polynomial of degree $2g$ with the right reciprocity.

CONJECTURE: With this definition of the Newton polygon of $P_1(C;t)$ for a stable curve C, the Grothendieck specialization theorem applies to the moduli space of stable curves of genus g.

One further question is the extent to which the Newton polygon stratification depends on the characteristic p. The 'geometrical' as opposed to 'arithmetic' nature of the techniques and results in this paper support the following

CONJECTURE: In the set M_g of g-dimensional principally polarized abelian varieties, the dimensions of the sets $S(NP)$ and of any set

$$\overline{S(NP_1) \cap S(NP_2)} \cap S(NP_3) \cap \ldots \cap S(NP_h)$$

is independent of p. (The analogous conjecture for stable curves also seems reasonable.)

However, certain other properties of the stratification clearly depend on p: (1) the number of components in an $S(NP)$ (that this depends on p is already clear from the fact that the number of supersingular elliptic curves depends on p); (2) the nature of the singularities of an $S(NP)$ (that this depends on p was apparent in the computations in section 11 of Chapter IV of the singularities of $M_{2;0}$, which is a curve in M_2 with $(p+1)$-crossings).

REFERENCES

[1] M. Artin: Supersingular $K3$ Surfaces (to appear).
[2] J. Ax: Zeroes of Polynomials over Finite Fields. *Amer. J. Math.*, *86*, 1964.
[3] N. Bourbaki: *Algèbre commutative.* Paris: Hermann, 1961.
[4] P. Cartier: Une nouvelle opération sur les formes différentielles. *C. R. Acad. Sci. Paris 244*, 1957.
[5] P. Deligne: Théorème de Lefschetz et critères de dégénérescence de suites spectrales. *Publ. Math. I.H.E.S. 35*, 1969.
[6] P. Deligne and D. Mumford: The Irreducibility of the Space of Curves of Given Genus. *Publ. Math. I.H.E.S. 36*, 1969.
[7] M. Demazure: *Lectures on p-Divisible Groups*, Lecture Notes in Mathematics 302, Berlin-Heidelberg-New York: Springer, 1972.
[8] B. Dwork: On the Congruence Properties of the Zeta Function of Algebraic Varieties. *J. für die Reine und Angewandte Math. 203*, 1960.
[9] B. Dwork: Normalized Period Matrices I and II. *Annals of Math. 94, 2nd series*, 1971, and *Annals of Math. 98, 2nd series*, 1973.
[10] B. Dwork: On the Rationality of the Zeta Function of an Algebraic Variety. *Amer. J. Math. 82*, 1960.
[11] B. Dwork: On the Zeta Function of a Hypersurface II. *Annals of Math. 80, 2nd series*, 1964.
[12] A. Grothendieck: Fondements de la géométrie algébrique, Secrétariat Mathématique, 11 rue Pierre Curie, Paris 5^e, France, 1962.
[13] A. Grothendieck: Séminaire de géométrie algébrique, 1, Lecture Notes in Mathematics 224, Berlin-Heidelberg-New York: Springer, 1971.
[14] A. Grothendieck: Séminaire de géométrie algébrique, 2, I.H.E.S., 1962.
[15] H. Hasse: Existenz Separabler Zyklischer Unverzweigter Erweiterungskörper vom Primzahlgrade p über Elliptischen Funktionenkörpern der Charakteristik p. *J. Reine Angew. Math. 172*, 1934.
[16] H. Hasse and E. Witt: Zyklische Unverzweigte Erweiterungskörper vom Primzahlgrade p über einem Algebraischen Funktionenkörper der Charakteristik p. *Monatsh. für Math. u. Phys. 43*, 1936.
[17] T. Honda: Isogeny Classes of Abelian Varieties over Finite Fields. *J. Math. Soc. Japan 20*, 1968.
[18] J. Igusa: Arithmetic Variety of Moduli for Genus Two. *Annals of Math. 72*, 2nd series, 1960.
[19] J. Igusa: Class Number of a Definite Quaternion with Prime Discriminant. *Proc. Natl. Acad. Sci. 44*, 1958.
[20] N. Katz: Algebraic Solutions of Differential Equations (p-Curvature and the Hodge Filtration), *Inventiones Math. 18*, 1972.
[21] N. Katz: *Une formule de congruence pour la fonction* ζ. S.G.A. 7 II, Lecture Notes in Mathematics 340, Berlin-Heidelberg-New York: Springer, 1973.
[22] N. Katz: Nilpotent Connections and the Monodromy Theorem: Applications of a Result of Turrittin. *Publ. Math. I.H.E.S. 39*, 1971.
[23] N. Katz: *Le niveau de la cohomologie des intersections complètes*, S.G.A. 7 II, Lecture Notes in Mathematics 340, Berlin-Heidelberg-New York: Springer, 1973.
[24] N. Katz: A Note on a Theorem of *Ax*. *Amer. J. Math.*, *93*, 1971.
[25] N. Katz: *Pinceaux de Lefschetz: théorème d'existence.* S.G.A. 7 II, Lecture Notes in Mathematics 340, Berlin-Heidelberg-New York: Springer, 1973.
[26] N. Katz: Review of Gauss Sums à la Stickelberger (unpublished notes).
[27] N. Katz: *Travaux de Dwork.* Exp. 409. Séminaire Bourbaki 1971/72, Lecture Notes in Mathematics 317, Berlin-Heidelberg-New York: Springer, 1973.
[28] N. Katz and T. Oda: On the Differentiation of De Rham Cohomology Classes with Respect to Parameters. *J. Math. Kyoto Univ. 8*, 1968.
[29] S. Kleiman: Weil Cohomologies in *Dix exposés sur la théorie des schémas.* Amsterdam: North-Holland, 1969.

[30] S. LANG: *Algebra.* Reading, Mass.: Addison-Wesley, 1965.
[31] JU. MANIN: Algebraic Curves over Fields with Differentiation. *A.M.S. Translations (2) 37*, 1964.
[32] JU. MANIN: The Hasse-Witt Matrix of an Algebraic Curve. *A.M.S. Translations (2) 45*, 1965.
[33] JU. MANIN: *Lekcii po Algebraičeskoĭ Geometrii.* Moscow: Izd. Mosk. Univ., 1970.
[34] JU. MANIN: The Theory of Commutative Formal Groups over Fields of Finite Characteristic. Translated in *Russian Math. Surv. 18*, 1963.
[35] B. MAZUR: Frobenius and the Hodge Filtration. *Bull. A.M.S. 78*, 1972.
[36] B. MAZUR: Frobenius and the Hodge Filtration (Estimates), *Annals of Math. 98*, 2nd series, 1973.
[37] B. MAZUR and W. MESSING: *Universal Extensions and One Dimensional Crystalline Cohomology.* Lecture Notes in Mathematics 370, Berlin-Heidelberg-New York: Springer, 1974.
[38] W. MESSING: *The Crystals Associated to Barsotti-Tate Groups: With Applications to Abelian Schemes.* Lecture Notes in Mathematics 264, Berlin-Heidelberg-New York: Springer, 1972.
[39] L. MILLER: Curves over a Finite Field with Invertible Hasse-Witt Matrix. *Math. Annalen 197*, 1972.
[40] L. MILLER: Über Gewöhnliche Projektive Hyperflächen (preprint).
[41] P. MONSKY: *P-adic Analysis and Zeta Functions.* Lectures in Mathematics No. 4, Tokyo: Kinokuniya Book-Store Ltd., 1970.
[42] D. MUMFORD: *Abelian Varieties.* Bombay: Oxford University Press, 1970.
[43] D. MUMFORD: *Geometric Invariant Theory.* New York: Academic Press, 1965.
[44] D. MUMFORD: *Introduction to Algebraic Geometry* (preliminary version of first three chapters). Harvard University.
[45] D. MUMFORD: Prym Varieties (to appear).
[46] D. MUMFORD and K. SUOMINEN: Introduction to the Theory of Moduli, in *Proc. 5th Nordic Summer Sch.* The Netherlands: Wolters-Noordhoff Pub., 1970.
[47] T. ODA: The First De Rham Cohomology Group and Dieudonné Modules. *Annales sci. de l'École Norm. Sup., 4e serie 2*, 1969.
[48] A. OGUS and G. BERGMAN: Nakayama's Lemma for Half-Exact Functors. *Proc. of the A.M.S. 31*, 1972.
[49] F. OORT: Finite Group Schemes, Local Moduli for Abelian Varieties, and Lifting Problems, in *Proc. 5th Nordic Summer Sch.* The Netherlands: Wolters-Noordhoff Pub., 1970.
[50] F. OORT: Subvarieties of Moduli Spaces. *Inventiones math. 24, 1974.*
[51] I. ŠAFAREVIČ: Foundations of Algebraic Geometry. translated in *Russian Math. Surv. 24*, 1969.
[52] M. SCHLESSINGER: Functors of Artin Rings. *Trans. A.M.S. 130*, 1968.
[53] J.-P. SERRE: *Algèbre Locale. Multiplicités.* Lecture Notes in Mathematics 11, Berlin-Heidelberg-New York: Springer, 1965.
[54] J.-P. SERRE: Faisceaux algébriques cohérents. *Annals of Math. 61*, 2nd series, 1955.
[55] J.-P. SERRE: *Sur la topologie des variétés algébriques en caractéristique p.* Symposio Intern. de Top. Alg., Mexico, 1958.
[56] L. STICKELBERGER: Über eine Verallgemeinerung der Kreistheilung. *Math. Ann. 37*, 1890.
[57] J. TATE: Algebraic Cycles and Poles of Zeta Functions, in *Arithmetical Algebraic Geometry* (Proc. of Purdue Conf.), New York: Harper and Row, 1965.
[58] J. TATE: *Classes d'isogénie des variétés abéliennes sur un corps fini (d'après T. Honda).* Exp. 352, Séminaire Bourbaki 1968/69, Lecture Notes in Mathematics 179, Berlin-Heidelberg-New York: Springer, 1971.
[59] J. TATE: Endomorphisms of Abelian Varieties over Finite Fields. *Inventiones Math. 2*, 1966.

[60] E. Warning: Bemerkung zur Verstehenden Arbeit von Herr Chevalley, Abh. Math. Sem. Univ. Hamburg, *11*, 1936.

[61] A. Weil: Jacobi Sums as 'Grössencharaktere', Trans. *A.M.S. 73*, 1952.

[62] A. Weil: Numbers of Solutions of Equations in Finite Fields. *Bull. A.M.S. 55*, 1949.

[63] P. Deligne and M. Rapoport: Les schémas de modules de courbes elliptiques, in Lecture Notes in Mathematics 349 (Proc. Intern. Summer Sch. on Modular Functions), Berlin-Heidelberg-New York: Springer, 1973.

[64] H. W. Lenstra Jr. and F. Oort: Simple Abelian Varieties Having a Prescribed Formal Isogeny Type. *Univ. of Amsterdam Math. Inst. Report 73–02*, 1973.

(Oblatum 14–XI–1974 & 5–VI–1975)

Dept. Math.
Princeton University
Fine Hall
Box 37
Princeton NJ 08540

Dept. Math.
Harvard University
1 Oxford Street
Cambridge Mass. 02138