Hasse–Witt and Cartier–Manin matrices: A warning and a request

Jeffrey D. Achter and Everett W. Howe

Abstract. Let X be a curve in positive characteristic. A *Hasse–Witt matrix* for X is a matrix that represents the action of the Frobenius operator on the cohomology group $H^1(X, \mathcal{O}_X)$ with respect to some basis. A *Cartier–Manin matrix* for X is a matrix that represents the action of the Cartier operator on the space of holomorphic differentials of X with respect to some basis. The operators that these matrices represent are adjoint to one another, so Hasse–Witt matrices and the Cartier–Manin matrices are related to one another, but there seems to be a fair amount of confusion in the literature about the exact nature of this relationship. This confusion arises from differences in terminology, from differing conventions about whether matrices act on the left or on the right, and from misunderstandings about the proper formulæ for iterating semilinear operators. Unfortunately, this confusion has led to the publication of incorrect results. In this paper we present the issues involved as clearly as we can, and we look through the literature to see where there may be problems. We encourage future authors to clearly distinguish between Hasse–Witt and Cartier–Manin matrices, in the hope that further errors can be avoided.

Prologue

An example. Consider the genus-2 hyperelliptic curve X over $\mathbb{F}_{125}$ with affine model

$$y^2 = f(x) = x^5 + x^4 + \alpha^{92}x^3 + \alpha^{18}x^2 + \alpha^{56}x\,, \tag{0.1}$$

where $\alpha \in \mathbb{F}_{125}$ satisfies $\alpha^3+3\alpha+3 = 0$. Let us compute the 5-rank of (the Jacobian of) X.

On one hand, we can follow Yui [14] and compute the effect of the Cartier operator on the space of regular one-forms. Let c_m be the coefficient of x^m in $f(x)^{(5-1)/2}$. Yui [14, p. 381] constructs a matrix (denoted A in her paper, but

2010 *Mathematics Subject Classification.* Primary 11G20, 14Q05; Secondary 14G10, 14G15, 14G17.

Key words and phrases. Cartier–Manin, Hasse–Witt, p-rank, zeta-function, semi-linear operator.

JDA's work partially supported by NSA grant H98230-16-1-0046.

denoted here by Y to prevent a conflict of notation later on) given by

$$\begin{aligned} Y &= \begin{pmatrix} c_{5\cdot 1-1} & c_{5\cdot 1-2} \\ c_{5\cdot 2-1} & c_{5\cdot 2-2} \end{pmatrix} \\ &= \begin{pmatrix} \alpha^{41} & \alpha^{105} \\ 2 & \alpha^{95} \end{pmatrix}. \end{aligned}$$

We compute as well that the image of Y under the Frobenius automorphism σ of $\mathbb{F}_{125}$ is given by

$$\begin{aligned} Y^\sigma &= \begin{pmatrix} c^\sigma_{5\cdot 1-1} & c^\sigma_{5\cdot 1-2} \\ c^\sigma_{5\cdot 2-1} & c^\sigma_{5\cdot 2-2} \end{pmatrix} \\ &= \begin{pmatrix} \alpha^{81} & \alpha^{29} \\ 2 & \alpha^{103} \end{pmatrix}, \end{aligned}$$

and the product $Y \cdot Y^\sigma$ is

$$Y \cdot Y^\sigma = \begin{pmatrix} \alpha^{32} & \alpha^{104} \\ \alpha^{22} & \alpha^{94} \end{pmatrix}.$$

Since this last matrix has rank one, according to Yui's Lemma E [14, p. 387] we should be able to conclude that X has 5-rank one.

On the other hand, X is actually supersingular; indeed, its L-polynomial is $(1 + 125T^2)^2$, and thus the only slope of its normalized 5-adic Newton polygon is $1/2$. In particular, X has 5-rank zero.

Our aim in this note is to tease out the source of this dissonance.

Genesis of this project. We noticed this discrepancy while attempting to obtain numerical data in support of some earlier work [1]. Moreover, we found that one of us invoked an erroneous formula in a separate project [63] (see Section 5.2).

Works such as Yui's 1978 paper [14], as well as its antecedents (including works by Manin [7, 8]) and consequents, rely on the construction and analysis of certain semilinear operators. Since the work of Hasse and Witt [4], it has been understood that there is such an operator, acting on some subquotient of the de Rham cohomology of a given curve X in characteristic p, that encodes information about the p-torsion group scheme of the Jacobian of X. The ideas of Hasse and Witt are beautifully clear, but one must navigate around several potential sources of error in order to arrive at a correct formula. Indeed, one must decide whether to work with the summand $H^0(X, \Omega^1_X)$ or the quotient $H^1(X, \mathcal{O}_X)$ of $H^1_{\mathrm{dR}}(X)$; this choice, in turn, determines whether the operator in question is σ-linear or σ^{-1}-linear, where σ is the p-th powering map on the base field. One is given a further opportunity to make a "sign error" when one chooses bases for these vector spaces and then decides whether the semilinear operator acts on the right or on the left.[1] Given these multiple opportunities for mistake, it is hardly surprising that there are occasional misstatements in the literature.

Conversations with others suggest to us that the community has an interest in (re)documenting these semilinear methods, especially in view of the continuing

[1] Of course, there is no literal "sign" to get wrong in any of the formulæ we discuss, but the terminology is suggestive of the fact that two such errors will typically cancel one another out. We will continue to use the the term "sign error" in this sense throughout the paper.

expansion of the role of computing in arithmetic geometry. With this backdrop, we offer the following survey of Cartier–Manin and Hasse–Witt matrices.

In Section 1 we review basic facts about the representation of semilinear operators by matrices. In Section 2 we define the Cartier operator on the space of holomorphic differentials of a curve X and the Frobenius operator on the cohomology group $H^1(X, \mathcal{O}_X)$, in its guise as a quotient group of the space of répartitions of X. The Cartier–Manin and Hasse–Witt matrices represent these two operators. In Section 3 we follow the work of Manin [9, 10] and Yui [14] to explicitly calculate the Cartier–Manin matrix of a hyperelliptic curve, and we resolve the problem posed by the example in our Prologue. In Section 4 we review the papers of Manin and Yui, keeping a watchful eye out for sign errors. We close in Section 5 with a review of the literature that cites Manin and Yui, to see whether any sign errors have propagated. Fortunately, there are only a few papers that contain results or examples that are in error.

Of course, it is unpleasant to find any errors at all in published papers. We have a suggestion for the community, which we hope will help prevent this type of sign error in the future: Please be careful with terminology. If you are working with the Cartier operator on differentials, refer to the matrix representation as the *Cartier–Manin* matrix; if you are working with the Frobenius operator on $H^1(X, \mathcal{O}_X)$, refer to the matrix representation as the *Hasse–Witt* matrix. These matrices are *related* to one another, but they are not *equal* to one another, and they represent semilinear operators with different properties.

Acknowledgments. We thank Yuri Manin, Noriko Yui, Arsen Elkin, Pierrick Gaudry, Takehiro Hasegawa, Rachel Pries, Andrew Sutherland, Saeed Tafazolian, Doug Ulmer, Felipe Voloch, and Yuri Zarhin, as well as the referees, for their comments on draft versions of this paper.

1. Matrices and semilinear algebra

We start with some notation concerning the use of matrices to represent semilinear algebra.

Let K be a field; we work exclusively with finite-dimensional K-vector spaces.

1.1. Bases, matrices, and linear operators. Let W be a vector space with basis $\mathcal{C} = \{w_1, \cdots, w_n\}$. Any $w \in W$ is expressible as $w = \sum c_i w_i$; let $[w]_{\mathcal{C}}$ denote the corresponding column vector

$$[w]_{\mathcal{C}} = \begin{pmatrix} c_1 \\ c_2 \\ \vdots \\ c_n \end{pmatrix}.$$

Now let V be an m-dimensional vector space with chosen basis $\mathcal{B}$, and let $f\colon W \to V$ be a linear transformation. Define numbers a_{ij} by

$$f(w_j) = \sum_{i=1}^{m} a_{ij} v_i \,.$$

The matrix of f relative to the chosen bases $\mathcal{C}$ and $\mathcal{B}$ is

$$[f]_{\mathcal{B}\leftarrow\mathcal{C}} = (a_{ij}) \in \mathrm{Mat}_{m\times n}(K)\,.$$

Matrix multiplication is defined so that, with this notation,

$$[f(w)]_{\mathcal{B}} = [f]_{\mathcal{B}\leftarrow\mathcal{C}} \cdot [w]_{\mathcal{C}} \ .$$

Change of basis works as follows. Let $f\colon V \to V$ be an endomorphism, and let $\mathcal{B}$ and $\mathcal{D}$ be two different bases for V. Then

$$[f]_{\mathcal{D}\leftarrow\mathcal{D}} = [\mathrm{id}]_{\mathcal{D}\leftarrow\mathcal{B}}\, [f]_{\mathcal{B}\leftarrow\mathcal{B}}\, [\mathrm{id}]_{\mathcal{B}\leftarrow\mathcal{D}} \ ;$$

if $S = [\mathrm{id}]_{\mathcal{B}\leftarrow\mathcal{D}}$, then

$$[f]_{\mathcal{D}\leftarrow\mathcal{D}} = S^{-1}\, [f]_{\mathcal{B}\leftarrow\mathcal{B}}\, S\,.$$

(Of course, if one prefers that matrices act on the right, then one consistently writes elements of the vector space as row vectors, and the matrix that represents the action of a linear operator is the *transpose* of the matrix described above.)

1.2. Semilinear algebra. Let ϵ be an automorphism of K. Now suppose that $f\colon V \to V$ is ϵ-linear, in the sense that for $a \in K$ and $v \in V$,

$$f(av) = a^{\epsilon} f(v)\,.$$

Naturally, f is determined by its effect on a basis, but the use of the matrices changes a little bit. Let $\mathcal{B} = \{v_1, \cdots, v_n\}$ be a basis, and again define numbers a_{ij} by

$$f(v_j) = \sum_i a_{ij} v_i\,.$$

If $v = \sum_j c_j v_j$ then

$$f(v) = \sum_j f(c_j v_j) = \sum_j c_j^{\epsilon} f(v_j) = \sum_j \Big(\sum_i a_{ij} v_i \Big) c_j^{\epsilon}$$

and so

$$[f(v)]_{\mathcal{B}} = [f]_{\mathcal{B}\leftarrow\mathcal{B}} \cdot [v]_{\mathcal{B}}^{\epsilon} \ ,$$

where B^{ϵ} is the matrix obtained by applying ϵ to each entry of B.

Similarly, change of basis is accomplished with ϵ-twisted conjugacy:

$$\begin{aligned} [f]_{\mathcal{D}\leftarrow\mathcal{D}} &= [\mathrm{id}]_{\mathcal{D}\leftarrow\mathcal{B}}\, [f]_{\mathcal{B}\leftarrow\mathcal{B}}\, [\mathrm{id}]_{\mathcal{B}\leftarrow\mathcal{D}}^{\epsilon} \\ &= S^{-1}\, [f]_{\mathcal{B}\leftarrow\mathcal{B}}\, S^{\epsilon}. \end{aligned}$$

If we suppress our subscripts for a moment, then the iterates of f are represented by

$$\begin{aligned} [f \circ f] &= [f]\, [f]^{\epsilon} \\ [f^{\circ r}] &= [f]\, [f]^{\epsilon}\, [f]^{\epsilon^2} \cdots [f]^{\epsilon^{r-1}} \ . \end{aligned}$$

(Again, if one wants matrices to act on the right, then the highest iterate of ϵ is applied to the *leftmost* factor in the r-fold product.)

1.3. Adjointness. Let V^* be the dual vector space of V and let $(\cdot,\cdot)\colon V \times V^* \to K$ be the natural pairing. Continue to let $f\colon V \to V$ be ϵ-linear, and let $\delta = \epsilon^{-1}$. The adjoint f^* of f with respect to the pairing $(\cdot,\cdot)$ is δ-linear and is characterized by the relation

$$(v, f^*w^*) = (fv, w^*)^\delta$$

for all $v \in V$ and $w^* \in V^*$. Let $\mathcal{B}^* = \{v_1^*, \cdots, v_n^*\}$ be the basis dual to $\mathcal{B}$. Since for $1 \le j, \ell \le n$ we have

$$(v_j, f^*v_\ell^*) = (fv_j, v_\ell^*)^\delta = \big(\sum_i a_{ij}v_i, v_\ell^*\big)^\delta = a_{\ell j}^\delta\,,$$

we find that

$$f^*v_\ell^* = \sum_j a_{\ell j}^\delta v_j^*$$

and therefore

$$[f^*]_{\mathcal{B}^*\leftarrow\mathcal{B}^*} = \big([f]_{\mathcal{B}\leftarrow\mathcal{B}}^\delta\big)^{\intercal} \tag{1.1}$$

where $^{\intercal}$ indicates the transpose of a matrix.

2. Hasse–Witt and Cartier–Manin matrices

We record here some properties of the Frobenius and Cartier operators and their representations by Hasse–Witt and Cartier–Manin matrices, deferring a complete exposition to, for example, Serre [13]. Let k be a perfect field of characteristic $p > 0$. Let $\sigma\colon k \to k$ be the Frobenius automorphism, and let τ be its inverse. Finally, let X/k be a smooth, projective curve of genus $g > 0$.

2.1. Cohomology groups. The Hodge to de Rham spectral sequence gives a canonical exact sequence

$$0 \longrightarrow H^0(X, \Omega_X^1) \longrightarrow H^1_{\mathrm{dR}}(X) \longrightarrow H^1(X, \mathcal{O}_X) \longrightarrow 0\,.$$

There is a canonical duality between the g-dimensional k-vector spaces $H^0(X, \Omega_X^1)$ and $H^1(X, \mathcal{O}_X)$. This duality is realized by cup product and the trace map:

$$H^0(X, \Omega_X^1) \times H^1(X, \mathcal{O}_X) \longrightarrow H^1(X, \Omega_X^1) \xrightarrow{\sim} k\,.$$

If k is algebraically closed, Serre [13, § 8] gives the following explicit description of this pairing. Let $\mathcal{R} = \mathcal{R}(X)$ be the ring of répartitions on X — that is, the subring of $\prod_{P\in X(k)} k(X)$ consisting of those elements $\{r_P\}$ for which, for all but finitely many P, the function r_P is regular at P. Let $\mathcal{R}(0)$ be the subring consisting of those répartitions such that each r_P is regular at P. Then there is an isomorphism

$$H^1(X, \mathcal{O}_X) \cong \frac{\mathcal{R}}{\mathcal{R}(0) + k(X)}\,,$$

where we view $k(x)$ as a subring of $\mathcal{R}$ via the diagonal embedding. The duality between this space and $H^0(X, \Omega_X^1)$ then admits the description

$$\begin{aligned} H^0(X, \Omega_X^1) \times H^1(X, \mathcal{O}_X) &\longrightarrow k \\ (\omega, r) &\longmapsto \textstyle\sum_{P\in X(k)} \mathrm{res}_P(r_P\omega)\,, \end{aligned} \tag{2.1}$$

where res_P denotes the residue at the point P.

2.2. The Cartier operator and the Cartier–Manin matrix. Cartier [2] (see also Katz [5, §7]) defines an operator on the de Rham complex of a smooth proper variety of arbitrary dimension. In the special case of a curve X, this give rise to a map from $H^0(X,\Omega^1_X)$ to itself. We follow here the explicit description given by Serre [13, §10].

Let P be a closed point on X and let t be a uniformizing parameter at P. Then the functions $1, t, \cdots, t^{p-1}$ form a p-basis for the local ring $\mathcal{O}_{X,P}$, that is, a basis for $\mathcal{O}_{X,P}$ as a module over $\mathcal{O}^p_{X,P}$. Any 1-form holomorphic at P admits an expression

$$\omega = \left(\sum_{j=0}^{p-1} f_j^p t^j \right) dt$$

for certain $f_j \in \mathcal{O}_{X,P}$, and one declares that

$$\mathcal{C}(\omega) = f_{p-1}\, dt\,.$$

The value of $\mathcal{C}(\omega)$ does not depend on the choice of uniformizer t, and the map $\mathcal{C}$ can be extended to give a map $\Omega^1_{k(X)/k} \to \Omega^1_{k(X)/k}$.

It is not hard to see that, for ω, ω_1, and ω_2 in $\Omega^1_{k(X)/k}$ and for $f \in k(X)$, one has

$$\begin{aligned} \mathcal{C}(\omega_1 + \omega_2) &= \mathcal{C}(\omega_1) + \mathcal{C}(\omega_2) \\ \mathcal{C}(f^p \omega) &= f \mathcal{C}(\omega)\,. \end{aligned}$$

In particular, the Cartier operator restricts to give a τ-linear operator

$$H^0(X,\Omega^1_X) \xrightarrow{\mathcal{C}} H^0(X,\Omega^1_X)\,.$$

(Yui [14] refers to this as the *modified* Cartier operator.) A matrix associated to $\mathcal{C}$ and a choice of basis for $H^0(X,\Omega^1_X)$ is called a *Cartier*, or *Cartier–Manin*, matrix for X.

2.3. The Frobenius operator and the Hasse–Witt matrix. There is also a Frobenius operator

$$H^1(X,\mathcal{O}_X) \xrightarrow{\mathcal{F}} H^1(X,\mathcal{O}_X)$$

which, under the isomorphism $H^1(X,\mathcal{O}_X) \cong \mathcal{R}/(\mathcal{R}(0) + k(X))$, takes the class of a répartition $r = \{r_P\}$ to the class of $\{r_P^p\}$. In particular, $\mathcal{F}$ is a σ-linear operator. Following Serre, we call any matrix associated to $\mathcal{F}$ and a choice of basis a *Hasse–Witt* matrix for X.

Like the Cartier operator, the Frobenius operator admits a generalization to varieties of arbitrary dimension. For a smooth variety for which the Hodge to de Rham spectral sequence degenerates at E_1, Katz defines [66, (2.3.4.1.3), p. 27] a σ-linear operator on each cohomology group of the structure sheaf. In the special case of a smooth projective hypersurface Y/k of dimension n, Katz gives an explicit formula for the action of this operator on $H^n(Y,\mathcal{O}_Y)$ in terms of a defining polynomial for Y [66, Algorithm (2.3.7.14), p. 35].

2.4. Adjointness. Serre goes on to show [13, Proposition 9, p. 40] that $\mathcal{F}$ and $\mathcal{C}$ are adjoint with respect to the pairing $(\cdot,\cdot)$ of (2.1), in the sense (see Section 1.3) that

$$(\omega, \mathcal{F}r) = (\mathcal{C}\omega, r)^{\sigma}. \tag{2.2}$$

By (1.1), if B is a Cartier–Manin matrix for X, then $(B^{\sigma})^{\intercal}$ is a Hasse–Witt matrix for X. Conversely, if A is a Hasse–Witt matrix for X, then $(A^{\tau})^{\intercal}$ is a Cartier–Manin matrix for X.

2.5. Zeta functions. Now suppose X is a curve over $\mathbb{F}_{q^e}$, the field with $q = p^e$ elements. The zeta function of X has the form

$$Z_{X/\mathbb{F}_q}(T) = \frac{L(T)}{(1-T)(1-qT)},$$

where $L(T) \in \mathbb{Z}[T]$. The e-fold iterate of $\mathcal{F}$ is $\mathbb{F}_q$-linear, and its characteristic polynomial satisfies the congruence

$$\operatorname{charpoly}_{\mathcal{F}^e}(T) \equiv L(T) \bmod p$$

([7, Theorem 1], [8, Theorem 1], [6, Théorème 3.1]). Consequently, if A is any Hasse–Witt matrix for X, then

$$\det(\mathrm{id} - AA^{\sigma}\cdots A^{\sigma^{e-1}}T) \equiv L(T) \bmod p.$$

Using (1.1), we find that $\mathcal{C}^e$ and $\mathcal{F}^e$ are adjoint $\mathbb{F}_q$-linear operators. In particular, if B is any Cartier–Manin matrix for X, then

$$\det(\mathrm{id} - BB^{\tau}\cdots B^{\tau^{e-1}}T) \equiv L(T) \bmod p.$$

Similarly, the characteristic polynomial $\chi_{X/\mathbb{F}_q}(T)$ of the relative Frobenius endomorphism of $\operatorname{Jac} X$ satisfies

$$\chi_{X/\mathbb{F}_q}(T) \equiv (-1)^g T^g \det([\mathcal{F}^e] - T\cdot\mathrm{id}) \equiv (-1)^g T^g \det([\mathcal{C}^e] - T\cdot\mathrm{id}) \bmod p.$$

3. Cartier–Manin matrices for hyperelliptic curves

We use the methods of Manin [9, 10] and Yui [14] to give a formula for a Cartier–Manin matrix of a hyperelliptic curve. We then use this formula to compute such a matrix for the curve (0.1), and independently compute a Hasse–Witt matrix to verify our work.

3.1. An explicit formula. Let k be a perfect field of odd characteristic p, and let X/k be a hyperelliptic curve of genus g with affine equation $y^2 = f(x)$, where $f(x) \in k[x]$ is square-free of degree $2g+1$ or $2g+2$.

As a basis for $H^0(X, \Omega^1_X)$ we choose

$$\mathcal{B} = \left\{ \omega_i = x^{i-1}\frac{dx}{y} : 1 \le i \le g \right\}. \tag{3.1}$$

If we write $f(x)^{\frac{p-1}{2}} = \sum c_m x^m$, we obtain the following equalities of differentials on X:

$$\begin{aligned}\frac{dx}{y} &= \frac{(y^2)^{\frac{p-1}{2}}}{y^p}dx \\ &= \frac{f(x)^{\frac{p-1}{2}}}{y^p}dx \\ &= y^{-p}\Big(\sum_{m\geq 0} c_m x^m\Big)dx\,.\end{aligned}$$

We find that

$$\omega_j = x^{j-1}\frac{dx}{y} = y^{-p}\Big(\sum_{m\geq 0} c_m x^{m+j-1}\Big)dx\,.$$

If we apply the Cartier operator to ω_j, the only terms that will make a contribution are the terms where $m+j-1 \equiv p-1 \bmod p$. In particular, we only need consider m of the form $ip-j$, for $i = 1,\dots,g$. We find that

$$\begin{aligned}\mathcal{C}(\omega_j) &= \mathcal{C}\Big(y^{-p}\Big(\sum_{i=1}^{g} c_{ip-j}x^{ip-p}\Big)x^{p-1}\,dx\Big) \\ &= \sum_{i=1}^{g}\mathcal{C}\Big(\left(c_{ip-j}^{\tau}x^{i-1}/y\right)^p x^{p-1}\,dx\Big) \\ &= \sum_{i=1}^{g} c_{ip-j}^{\tau}x^{i-1}/y\,dx \\ &= \sum_{i\geq 1} c_{ip-j}^{\tau}\omega_i\,.\end{aligned}$$

If we let $B \in \mathrm{Mat}_g(k)$ be the matrix with entries $B_{ij} = c_{ip-j}^{\tau}$, then left-multiplication by B calculates the effect of $\mathcal{C}$ in the basis $\mathcal{B}$.

3.2. The example, revisited. We reconsider the curve (0.1) and the associated matrix Y. Then

$$B = Y^{\tau} = \begin{pmatrix}\alpha^{33} & \alpha^{21}\\ 2 & \alpha^{19}\end{pmatrix}.$$

We compute the effect of the second iterate of the Cartier operator as

$$[\mathcal{C}^{\circ 2}]_{\mathcal{B}\leftarrow\mathcal{B}} = [\mathcal{C}][\mathcal{C}]^{\tau} = BB^{\tau} = \begin{pmatrix}0 & 0\\ 0 & 0\end{pmatrix};$$

this reflects the supersingularity of our original curve.

For thoroughness, we will use direct computation to find the Hasse–Witt matrix for this example as well. Let k be an algebraic closure of $\mathbb{F}_{125}$. By the strong approximation theorem, the vector space $H^1(X,\mathcal{O}_X) \cong \mathcal{R}/(\mathcal{R}(0)+k(X))$ can be represented by the classes of répartitions supported only at the point at infinity ∞ on the curve X. In fact, the répartitions $r = \{r_P\}_{P\in X(k)}$ and $s = \{s_P\}_{P\in X(k)}$ defined by

$$r_P = \begin{cases}2y/x & \text{if } P=\infty;\\ 0 & \text{otherwise}\end{cases} \qquad \text{and} \qquad S_P = \begin{cases}2y/x^2 & \text{if } P=\infty;\\ 0 & \text{otherwise}\end{cases}$$

give a basis for $\mathcal{R}/(\mathcal{R}(0)+k(X))$ that is dual to the basis $\{\omega_1,\omega_2\}$ of $H^0(X,\Omega^1_X)$ given in (3.1) under the pairing (2.1); we see this as follows. Let $z=x^2/y$, so that z is a uniformizing parameter for X at ∞. We compute that

$$\begin{aligned}\omega_1 &= \quad dx/y = \bigl(3z^2+O(z^4)\bigr)\,dz\\ \omega_2 &= x\,dx/y = \bigl(3+3z^2+O(z^4)\bigr)\,dz\\ r_\infty &= 2y/x \quad = 2z^{-3}+3z^{-1}+O(z)\\ s_\infty &= 2y/x^2 \;= 2z^{-1}.\end{aligned}$$

It follows easily that $(\omega_1,r)=(\omega_2,s)=1$ and $(\omega_1,s)=(\omega_2,r)=0$.

We compute also that

$$\begin{aligned}r_\infty^5 &= (2x^5+4x^4+\alpha^2x^3+\alpha^{69}x^2+\alpha^{77}x+\alpha^{94})y+\alpha^{41}r_\infty+\alpha^{105}s_\infty+O(z)\\ s_\infty^5 &= 2y+2r_\infty+\alpha^{95}s_\infty+O(z),\end{aligned}$$

and it follows that the Hasse–Witt matrix for our curve X is given by

$$A=\begin{pmatrix}\alpha^{41} & 2\\ \alpha^{105} & \alpha^{95}\end{pmatrix}.$$

As expected, we see that A is the transpose of Yui's matrix Y, that $B=(A^\tau)^\intercal$, and that $AA^\sigma=\left(\begin{smallmatrix}0&0\\0&0\end{smallmatrix}\right)$.

3.3. A generalization. Garcia and Tafazolian generalize Manin and Yui's computation, and calculate a matrix [3, p. 212] such that left-multiplication by this matrix gives the effect of the n-th iterate of the Cartier operator in terms of the basis $\mathcal{B}$; the (i,j) entry of their matrix is the p^n-th root of the coefficient of x^{ip^n-j} in the polynomial $f(x)^{(p^n-1)/2}$. The penultimate displayed equation on page 212 of their paper shows this matrix acting on the right, but the formulæ presented elsewhere in in their paper make it clear that it acts on the left.

4. Hasse–Witt matrices through the ages

As noted in the introduction, Hasse and Witt [4] showed that various properties of a curve X can be read off from the action of Frobenius on $H^1(X,\mathcal{O}_X)$, the equivalence classes of répartitions of the curve, and they associated a matrix to this semilinear operator. In the paper in which he defined his operator on differential forms, Cartier [2] already noted a connection to the Hasse–Witt matrix of the curve; Serre [13, § 10] explains this well. Over the years, different authors have made this connection more and more computationally explicit. In this section, we focus on the work of Manin and of Yui, because their papers are the ones referred to most often when present-day authors write about computational aspects of the Cartier operator.

4.1. The work of Manin. Manin published three works relevant to our discussion here. We treat them each in turn.

In the first of these works [7] (available also in an English translation [8]), Manin develops explicit formulæ for computing the action of $\mathcal{F}$ on $H^1(X,\mathcal{O}_X)$. On one hand, the definition of the matrix A in the second displayed equation on page 153 of [7] assumes a *right* action.[2] This is further emphasized in the first

[2]The second displayed equation on page 245 of the English translation.

displayed equation on page 154.[3] On the other hand, the change of basis formula in the last displayed formula on page 153, and the formula for the g-fold iterate of $\mathcal{F}$ on page 154, are valid provided matrices act on the *left*.[4]

The main result of this work ([7, Theorem 1, p. 155], [8, Theorem 1, p. 247]) considers a curve X over a field with $q = p^e$ elements, and relates the characteristic polynomial of the Frobenius endomorphism of $\operatorname{Jac} X$ to the characteristic polynomial of a matrix representing the linear, e-fold iterate $\mathcal{F}^e$. The theorem as stated is correct, but only if we take A to be the matrix representing the Frobenius endomorphism of $H^1(X, \mathcal{O}_X)$ *acting on the left*. However, since the matrix A as defined in the text before the theorem is taken to act on the *right*, the theorem is incorrect if it is taken in the larger context of the paper.

In the second paper we would like to discuss, Manin [9, 10] reconsiders some of these operators. He works with the Cartier operator $\mathcal{C}$, observes that it is τ-linear, and that it acts on the space $H^0(X, \Omega^1_X)$. He explicitly calculates a basis for the space of differentials on a particular hyperelliptic curve and computes the action of the Cartier operator in terms of this basis, using the same techniques that we reproduce here in Section 3.1. No matrices are written down, so there are no obvious sign errors in this paper. Note, however, that in this paper Manin considers the Cartier operator on $H^0(X, \Omega^1_X)$, while in the preceding paper he considered the Frobenius operator on $H^1(X, \mathcal{O}_X)$.

In Section IV.5.2 of his paper on formal groups [11, 12], Manin computes an operator that he *calls* the Hasse–Witt matrix — and thus, in theory, should represent the action of $\mathcal{F}$ on $H^1(X, \mathcal{O}_X)$ — but which actually *represents* the action of $\mathcal{C}$ on $H^0(X, \Omega^1_X)$, as in the paper discussed in the preceding paragraph. The formula Manin uses for iterates of this operator implicitly (and incorrectly) assumes that it is σ-linear. This leads to errors in Section IV.5.2; there are several problems with the displayed group of equations that deduce conditions on the formal group of a curve's Jacobian from conditions on the equation of the curve ([11, p. 86], [12, p. 79]). It seems to us that this paper may be the original source of a recurrent conflation in the literature of "Hasse–Witt" and "Cartier–Manin" matrices.

4.2. The work of Yui. Yui [14] analyzes hyperelliptic curves with affine model $y^2 = f(x)$, and computes the Cartier operator $\mathcal{C}$ on $H^0(X, \Omega^1_X)$. (We remind the reader that Yui refers to the object we call the *Cartier operator* as the *modified Cartier operator*, and that she denotes it by $\mathcal{C}'$.) In Theorem 2.1 [14, p. 382] and Theorem 2.2 [14, p. 384], the formula for iterates is appropriate for a σ-linear operator, but $\mathcal{C}$ is τ-linear. Moreover, Lemma D [14, p. 386] exploits the semilinear adjointness (1.1) between $\mathcal{C}$ and $\mathcal{F}$, but overlooks the transpose necessary for such matrix calculations. Because of sign errors like these, Theorem 2.2 [14, p. 384] and Lemma E [14, p. 387] are incorrect; the curve we discussed in the Prologue gives a counterexample to both.

Although several explicit examples are worked out in Yui's paper, none of them can detect these inconsistencies. Indeed, in Example 3.3 [14, p. 391] both $\mathcal{C}$ and $\mathcal{F}$ are diagonalized by the natural basis, which hides ambiguity between left- and right-multiplication. Moreover, both this example and Example 5.4 [14, p. 400] are

[3] The final displayed equation on page 245 of the English translation.

[4] The third displayed formula on page 245, and the g-fold iterate formula on the top of page 246, of the English translation.

worked out for curves over $\mathbb{F}_p$, in which case σ- and τ-linear operators are simply linear.

Yui writes at the end of the paper's introduction that the article stemmed from her working through Manin's papers [9, 10, 11, 12], so some of the sign errors in Yui's paper are reflections of Manin's earlier ambiguities between left actions and right actions and between σ-linear and τ-linear operators. This paper also encourages the unfortunate conflation of the concepts of the Hasse–Witt matrix and the Cartier–Manin matrix that began with Manin; we have already noted Lemma D [14, p. 386], which says that the two matrices are "identified" with one another.

5. Subsequent developments

Explicit computational methods are becoming increasingly useful in arithmetic geometry, and this utility is reflected in the large number of citations of the articles of Manin and Yui that we discussed in the preceding section. Indeed, by consulting MathSciNet and the Web of Science, we found 92 works that refer to Yui's paper [14] or Manin's paper on Hasse–Witt matrices [7, 8], and by personal knowledge we found one more. These works are listed below in a separate section of our bibliography.

It is somewhat worrisome to see so many citations, because — as we have noted above — these papers of Manin and Yui contain sign errors that invalidate some of their results. To determine whether these sign errors have propagated to other papers, we went through the 93 articles we found to see how they applied the results of Manin and Yui. Of course, we could not go through all of these articles with great care; for the most part, we limited ourselves to looking at how they made use of the work of Manin and Yui described above, and it is possible we missed some subtleties.

In the vast majority of these works, we did not find any obvious errors stemming from the citation of the papers of Manin and Yui. For example:

- Sometimes the papers of Manin and Yui were given as general references (for the computation of Hasse–Witt matrices or for something else), and no particular results from the papers were used.
- In some cases, specific results from Manin or Yui *were* quoted, but either they were not applied, or they did not contain any sign errors, or the sign errors were silently corrected.
- In some cases, statements containing sign errors (quoted from Manin or Yui or elsewhere, or derived independently) *were* applied to specific examples, but in these examples the sign errors in the general formulæ did not lead to errors in the specific cases. Incorrect formulæ might not lead to errors, for example,
  - if the genus of the curve is 1;
  - or, more generally, if the Hasse–Witt matrix is diagonal, so that A commutes with all of its Galois conjugates;
  - or if the base field is $\mathbb{F}_p$, so that no iteration is necessary;
  - or if the base field is $\mathbb{F}_{p^2}$, so that $A \cdot A^\sigma = A \cdot A^\tau$;
  - or in a number of other situations.

But in eight of these papers, incorrect results *were* used in ways that we felt required further investigation. We look at these papers here.

5.1. Combining a theorem of Manin with a formula of Yui. The paper of Gaudry and Harley [51], as well as the papers of Bostan, Gaudry, and Schost [27, 28], all quote a result of Manin ([7, Theorem 1, p. 155], [8, Theorem 1, p. 247]; see also §2.5) that relates the mod-p reduction of the Weil polynomial of a curve over $\mathbb{F}_{p^e}$ to the characteristic polynomial of a matrix

$$H_\pi = HH^{(p)} \cdots H^{(p^{e-1})},$$

where H is the Hasse–Witt matrix for the curve. As we noted earlier, Manin's theorem is only correct as written if we take our matrices to act on the left. However, the papers of Bostan, Gaudry, Harley, and Schost under discussion take H to be the matrix computed by Yui [14, p. 381]. Yui does intend for this matrix to act on the left, but it represents the Cartier operator on differentials, not the Frobenius operator on répartitions, so Yui's matrix must be transposed to give the Hasse–Witt matrix. In other words, the naïve combination of Yui's matrix with Manin's theorem gives incorrect results.

This can be seen very concretely. Consider the genus-2 curve X over $\mathbb{F}_{27}$ defined by $y^2 = x^5 + a^2x^2 + ax$, where $a^3 - a + 1 = 0$. On one hand, the matrices H and H_π from the cited papers are

$$H = \begin{bmatrix} a^2 & a \\ 1 & 0 \end{bmatrix} \quad \text{and} \quad H_\pi = HH^{(3)}H^{(9)} = \begin{bmatrix} a^{12} & a^{14} \\ a^{15} & a^{15} \end{bmatrix},$$

and the characteristic polynomial $\kappa(t)$ of H_π is $t^2 + t + 1$. On the other hand, the characteristic polynomial of Frobenius for X is $\chi(t) = t^4 + 6t^3 + 52t^2 + 162t + 729$, and it is visibly *not* the case that $\chi(t) \equiv (-1)^2t^2\kappa(t) \bmod 3$, as the cited theorems claim.

However, we suspect that Bostan, Gaudry, and Schost must have implemented the computation of H_π with the matrices in the opposite order (or they transposed H, or something similar), because the example they present [27, §5] satisfies the basic sanity check that several randomly-chosen points on the Jacobian are annihilated by the integer they give as the order of the Jacobian.

Likewise, Gaudry and Harley present an example [51, §7.2] of a computation over $\mathbb{F}_{p^4}$ in which they explicitly mention the order of the Jacobian modulo p computed by Manin's result, and the numerical value they get shows that their computation must have involved either transposing H or computing H_π with the factors reversed.

5.2. Supersingular genus-2 curves. We found three papers that use Yui's computation of the iterated Cartier operator to determine when a genus-2 curve is supersingular.

Elkin [42, §9] gives a characterization of supersingular genus-2 curves that includes a sign error. This incorrect characterization does not affect the main part of his work (for example, Theorems 1.1, 1.6, and 1.7 [42, pp. 54–56]), but we have not checked to see whether it affects the validity of his examples [42, §9].

Howe [63] uses Yui's Lemma E [14, p. 387] in the proof of his Theorem 2.1 [63, p. 51], which claims that all supersingular genus-2 curves over a field of characteristic 3 can be put into a certain standard form. The proof as written is invalid, because the criterion for supersingularity has a sign error; however, the proof can easily be repaired by using the correct criterion, and one can check that the theorem as stated is true.

Zarhin [108] also studies supersingular genus-2 curves in characteristic 3. In the proof of his Lemma 6.1 [108, p. 629] he correctly characterizes when a genus-2 curve is supersingular in terms of a matrix that specifies the action of the Cartier operator. Unfortunately, in a later paper [15, §5, p. 213] he provides a "correction" to this proof that replaces the correct characterization with an incorrect one. Fortunately, this did not require changing the statement of the result he was proving; the statement of his Lemma 6.1 [108, p. 629] is correct.

5.3. Genus-3 curves of p-rank 0. We found one paper, by Elkin and Pries [44], that uses Yui's results to compute the moduli space of hyperelliptic genus-3 curves of p-rank 0 in characteristic 3 and characteristic 5. The notation in their Lemma 2.2 [44, p. 246] is ambiguous, but when they apply this lemma in the proofs of Lemmas 3.3 and 3.6 [44, pp. 248 and 250] they multiply the matrices in the wrong order. This invalidates their calculations of the defining equations of the moduli spaces. Pries reports that Theorem 4.2 [44, p. 251] still holds.

5.4. Supersingularity versus superspeciality. Yui's 1986 paper [105] cites her 1978 paper [14], as well as a paper of Nygaard [80], in the course of the proof of Theorem 2.5 [105, p. 113]. In particular, Yui cites these papers to show that a curve over $\overline{\mathbb{F}}_p$ has supersingular Jacobian (that is, its Jacobian is isogenous to a power of a supersingular elliptic curve) if and only if the Cartier operator on its differentials is zero. In fact, Nygaard shows that the vanishing of the Cartier operator is equivalent to the Jacobian being *superspecial* (that is, *isomorphic* to a power of a supersingular elliptic curve) [80, Theorem 4.1, p. 388]. Furthermore, Yui herself gives examples showing that while the vanishing of the Cartier operator implies that the curve is supersingular, the converse is not true [14, Example 5.4, p. 400]. Thus, Theorem 2.5 [105, p. 113] is incorrect.

6. Conclusion

As we noted, most of the 93 papers that cite Manin [7, 8] or Yui [14] do not seem to have inherited any errors in their main results. However, it might be prudent for authors who have used results from these 93 papers to double check that the results they quoted are indeed free of sign errors.

We conclude by repeating our supplication from the introduction: Please be careful with terminology, and make a clear distinction between the Cartier operator on differentials (represented by the Cartier–Manin matrix) and the Frobenius operator on $H^1(X, \mathcal{O}_X)$ (represented by the Hasse–Witt matrix). We hope that if such care is taken, there will be no need in the future for another paper like this one.

References

[1] J. D. Achter and E. W. Howe. Split abelian surfaces over finite fields and reductions of genus-2 curves. *Algebra Number Theory*, 11(1):39–76, 2017.

[2] P. Cartier. Une nouvelle opération sur les formes différentielles. *C. R. Acad. Sci. Paris*, 244:426–428, 1957.

[3] A. Garcia and S. Tafazolian. Certain maximal curves and Cartier operators. *Acta Arith.*, 135(3):199–218, 2008.

[4] H. Hasse and E. Witt. Zyklische unverzweigte Erweiterungskörper vom Primzahlgrade p über einem algebraischen Funktionenkörper der Charakteristik p. *Monatsh. Math. Phys.*, 43(1):477–492, 1936.

[5] N. M. Katz. Nilpotent connections and the monodromy theorem: Applications of a result of Turrittin. *Inst. Hautes Études Sci. Publ. Math.*, (39):175–232, 1970.
[6] N. M. Katz. Une formule de congruence pour la fonction ζ. In *Groupes de monodromie en géométrie algébrique. II*, Lecture Notes in Mathematics, Vol. 340, pages 401–438. Springer-Verlag, Berlin–New York, 1973. Séminaire de Géométrie Algébrique du Bois-Marie 1967–1969 (SGA 7 II), dirigé par P. Deligne et N. Katz.
[7] J. I. Manin. The Hasse–Witt matrix of an algebraic curve. *Izv. Akad. Nauk SSSR Ser. Mat.*, 25:153–172, 1961.
[8] J. I. Manin. The Hasse–Witt matrix of an algebraic curve. *Amer. Math. Soc. Transl. (2)*, 45:245–264, 1965. Translated by J. W. S. Cassels.
[9] J. I. Manin. On the theory of Abelian varieties over a field of finite characteristic. *Izv. Akad. Nauk SSSR Ser. Mat.*, 26:281–292, 1962.
[10] J. I. Manin. On the theory of Abelian varieties over a field of finite characteristic. *Amer. Math. Soc. Transl. (2)*, 50:127–140, 1966. Translated by G. Wagner.
[11] J. I. Manin. Theory of commutative formal groups over fields of finite characteristic. *Uspehi Mat. Nauk*, 18(6):3–90, 1963.
[12] J. I. Manin. Theory of commutative formal groups over fields of finite characteristic. *Russian Math. Surveys*, 18(6):1–83, 1963.
[13] J.-P. Serre. Sur la topologie des variétés algébriques en caractéristique p. In *Symposium internacional de topología algebraica*, pages 24–53. Universidad Nacional Autónoma de México and UNESCO, Mexico City, 1958.
[14] N. Yui. On the Jacobian varieties of hyperelliptic curves over fields of characteristic $p > 2$. *J. Algebra*, 52(2):378–410, 1978.
[15] Y. G. Zarhin. Homomorphisms of abelian varieties. In *Arithmetic, geometry and coding theory (AGCT 2003)*, volume 11 of *Sémin. Congr.*, pages 189–215. Soc. Math. France, Paris, 2005.

For the reader's convenience, we gather together here a list of all of the papers that we are aware of that cite Manin's 1961 paper [7, 8] or Yui's 1978 paper [14]. We omit Yui's paper [14] itself, even though it cites Manin [8].

Works that cite Manin (1961) or Yui (1978)

[16] A. Adolphson. The U_p-operator of Atkin on modular functions of level three. *Illinois J. Math.*, 24(1):49–60, 1980.
[17] A. Álvarez. The p-rank of the reduction mod p of Jacobians and Jacobi sums. *Int. J. Number Theory*, 10(8):2097–2114, 2014.
[18] N. Anbar and P. Beelen. A note on a tower by Bassa, Garcia and Stichtenoth. *Funct. Approx. Comment. Math.*, 57(1):47–60, 2017.
[19] M. Asada. On the action of the Frobenius automorphism on the pro-l fundamental group. *Math. Z.*, 199(1):15–28, 1988.
[20] M. H. Baker. Cartier points on curves. *Internat. Math. Res. Notices*, (7):353–370, 2000.
[21] S. Ballet, C. Ritzenthaler, and R. Rolland. On the existence of dimension zero divisors in algebraic function fields defined over $\mathbb{F}_q$. *Acta Arith.*, 143(4):377–392, 2010.
[22] E. Ballico. On the automorphisms of surfaces of general type in positive characteristic. II. *Atti Accad. Naz. Lincei Cl. Sci. Fis. Mat. Natur. Rend. Lincei (9) Mat. Appl.*, 5(1):63–68, 1994.
[23] A. Bassa and P. Beelen. The Hasse–Witt invariant in some towers of function fields over finite fields. *Bull. Braz. Math. Soc. (N.S.)*, 41(4):567–582, 2010.
[24] M. Bauer, M. J. Jacobson, Jr., Y. Lee, and R. Scheidler. Construction of hyperelliptic function fields of high three-rank. *Math. Comp.*, 77(261):503–530, 2008.
[25] M. Bauer, E. Teske, and A. Weng. Point counting on Picard curves in large characteristic. *Math. Comp.*, 74(252):1983–2005, 2005.
[26] J.-B. Bost. Algebraization, transcendence, and D-group schemes. *Notre Dame J. Form. Log.*, 54(3–4):377–434, 2013.
[27] A. Bostan, P. Gaudry, and E. Schost. Linear recurrences with polynomial coefficients and computation of the Cartier–Manin operator on hyperelliptic curves. In *Finite fields and*

applications, volume 2948 of *Lecture Notes in Comput. Sci.*, pages 40–58. Springer, Berlin, 2004.

[28] A. Bostan, P. Gaudry, and E. Schost. Linear recurrences with polynomial coefficients and application to integer factorization and Cartier–Manin operator. *SIAM J. Comput.*, 36(6):1777–1806, 2007.

[29] I. I. Bouw, C. Diem, and J. Scholten. Ordinary elliptic curves of high rank over $\overline{\mathbb{F}}_p(x)$ with constant j-invariant. *Manuscripta Math.*, 114(4):487–501, 2004.

[30] A. Buium and J. F. Voloch. Reduction of the Manin map modulo p. *J. Reine Angew. Math.*, 460:117–126, 1995.

[31] B. Cais, J. S. Ellenberg, and D. Zureick-Brown. Random Dieudonné modules, random p-divisible groups, and random curves over finite fields. *J. Inst. Math. Jussieu*, 12(3):651–676, 2013.

[32] G. Cardona and E. Nart. Zeta function and cryptographic exponent of supersingular curves of genus 2. In *Pairing-based cryptography—Pairing 2007*, volume 4575 of *Lecture Notes in Comput. Sci.*, pages 132–151. Springer, Berlin, 2007.

[33] J. W. S. Cassels. Diophantine equations with special reference to elliptic curves. *J. London Math. Soc.*, 41:193–291, 1966.

[34] P. Cassou-Noguès, T. Chinburg, B. Erez, and M. J. Taylor. Derived category invariants and L-series. *J. Lond. Math. Soc. (2)*, 92(2):265–283, 2015.

[35] W. Castryck, M. Streng, and D. Testa. Curves in characteristic 2 with non-trivial 2-torsion. *Adv. Math. Commun.*, 8(4):479–495, 2014.

[36] J.-P. Cherdieu. Remarks on the zeta function of some diagonal hyperelliptic curves. *J. Pure Appl. Algebra*, 190(1–3):31–43, 2004.

[37] G. Cornelissen, F. Oort, I. Bouw, T. Chinburg, C. Gasbarri, D. Glass, C. Lehr, M. Matignon, R. Pries, and S. Wewers. Problems from the Workshop on Automorphisms of Curves. *Rend. Sem. Mat. Univ. Padova*, 113:129–177, 2005.

[38] B. Ditters and S. Hoving. Sur la composante connexe du module de Tate covariant de la famille des courbes, donnée par l'équation $y^2 = 1 + \mu x^N$. *C. R. Acad. Sci. Paris Sér. I Math.*, 306(14):621–624, 1988.

[39] B. Ditters and S. J. Hoving. On the connected part of the covariant Tate p-divisible group and the ζ-function of the family of hyperelliptic curves $y^2 = 1+\mu x^N$ modulo various primes. *Math. Z.*, 200(2):245–264, 1989.

[40] E. J. Ditters. On the classification of commutative formal group laws over p-Hilbert domains and a finiteness theorem for higher Hasse–Witt matrices. *Math. Z.*, 202(1):83–109, 1989.

[41] I. Dolgachev and D. Lehavi. On isogenous principally polarized abelian surfaces. In *Curves and abelian varieties*, volume 465 of *Contemp. Math.*, pages 51–69. Amer. Math. Soc., Providence, RI, 2008.

[42] A. Elkin. Hyperelliptic Jacobians with real multiplication. *J. Number Theory*, 117(1):53–86, 2006.

[43] A. Elkin. The rank of the Cartier operator on cyclic covers of the projective line. *J. Algebra*, 327:1–12, 2011.

[44] A. Elkin and R. Pries. Hyperelliptic curves with a-number 1 in small characteristic. *Albanian J. Math.*, 1(4):245–252, 2007.

[45] A. Elkin and R. Pries. Ekedahl–Oort strata of hyperelliptic curves in characteristic 2. *Algebra Number Theory*, 7(3):507–532, 2013.

[46] J. Estrada Sarlabous. On the Jacobian varieties of Picard curves defined over fields of characteristic $p > 0$. *Math. Nachr.*, 152:329–340, 1991.

[47] S. Farnell and R. Pries. Families of Artin–Schreier curves with Cartier–Manin matrix of constant rank. *Linear Algebra Appl.*, 439(7):2158–2166, 2013.

[48] F. Fité and A. V. Sutherland. Sato–Tate groups of $y^2 = x^8 + c$ and $y^2 = x^7 - cx$. In *Frobenius distributions: Lang–Trotter and Sato-Tate conjectures*, volume 663 of *Contemp. Math.*, pages 103–126. Amer. Math. Soc., Providence, RI, 2016.

[49] E. Furukawa, M. Kawazoe, and T. Takahashi. Counting points for hyperelliptic curves of type $y^2 = x^5 + ax$ over finite prime fields. In *Selected areas in cryptography*, volume 3006 of *Lecture Notes in Comput. Sci.*, pages 26–41. Springer, Berlin, 2004.

[50] S. D. Galbraith. *Mathematics of public key cryptography*. Cambridge University Press, Cambridge, 2012.

[51] P. Gaudry and R. Harley. Counting points on hyperelliptic curves over finite fields. In *Algorithmic number theory (Leiden, 2000)*, volume 1838 of *Lecture Notes in Comput. Sci.*, pages 313–332. Springer, Berlin, 2000.
[52] A. Ghosh and K. Ward. The number of roots of polynomials of large degree in a prime field. *Int. Math. Res. Not. IMRN*, (4):898–926, 2015.
[53] D. Glass and R. Pries. Hyperelliptic curves with prescribed p-torsion. *Manuscripta Math.*, 117(3):299–317, 2005.
[54] H. Goodson. A complete hypergeometric point count formula for Dwork hypersurfaces. *J. Number Theory*, 179:142–171, 2017.
[55] H. Goodson. Hypergeometric functions and relations to Dwork hypersurfaces. *Int. J. Number Theory*, 13(2):439–485, 2017.
[56] R. Granger, F. Hess, R. Oyono, N. Thériault, and F. Vercauteren. Ate pairing on hyperelliptic curves. In *Advances in cryptology—EUROCRYPT 2007*, volume 4515 of *Lecture Notes in Comput. Sci.*, pages 430–447. Springer, Berlin, 2007.
[57] P. Guerzhoy. The Ramanujan differential operator, a certain CM elliptic curve and Kummer congruences. *Compos. Math.*, 141(3):583–590, 2005.
[58] D. Harvey and A. V. Sutherland. Computing Hasse–Witt matrices of hyperelliptic curves in average polynomial time. *LMS J. Comput. Math.*, 17(suppl. A):257–273, 2014.
[59] D. Harvey and A. V. Sutherland. Computing Hasse–Witt matrices of hyperelliptic curves in average polynomial time, II. In *Frobenius distributions: Lang–Trotter and Sato–Tate conjectures*, volume 663 of *Contemp. Math.*, pages 127–147. Amer. Math. Soc., Providence, RI, 2016.
[60] T. Hasegawa. Some remarks on superspecial and ordinary curves of low genus. *Math. Nachr.*, 286(1):17–33, 2013.
[61] K.-i. Hashimoto and N. Murabayashi. Shimura curves as intersections of Humbert surfaces and defining equations of QM-curves of genus two. *Tohoku Math. J. (2)*, 47(2):271–296, 1995.
[62] W. A. Hawkins, Jr. The étale cohomology of p-torsion sheaves. I. *Trans. Amer. Math. Soc.*, 301(1):163–188, 1987.
[63] E. W. Howe. Supersingular genus-2 curves over fields of characteristic 3. In *Computational arithmetic geometry*, volume 463 of *Contemp. Math.*, pages 49–69. Amer. Math. Soc., Providence, RI, 2008.
[64] T. Ibukiyama, T. Katsura, and F. Oort. Supersingular curves of genus two and class numbers. *Compositio Math.*, 57(2):127–152, 1986.
[65] F. A. Izadi and V. K. Murty. Counting points on an abelian variety over a finite field. In *Progress in cryptology—INDOCRYPT 2003*, volume 2904 of *Lecture Notes in Comput. Sci.*, pages 323–333. Springer, Berlin, 2003.
[66] N. M. Katz. Algebraic solutions of differential equations (p-curvature and the Hodge filtration). *Invent. Math.*, 18:1–118, 1972.
[67] H. A. W. M. Kneppers. The Hasse–Witt matrix of a formal group. *Math. Z.*, 189(2):151–165, 1985.
[68] T. Kodama and T. Washio. On class numbers of hyperelliptic function fields with Hasse–Witt-invariant zero. *Arch. Math. (Basel)*, 49(3):208–213, 1987.
[69] T. Kodama and T. Washio. Hasse–Witt matrices of Fermat curves. *Manuscripta Math.*, 60(2):185–195, 1988.
[70] T. Kodama and T. Washio. A family of hyperelliptic function fields with Hasse–Witt-invariant zero. *J. Number Theory*, 36(2):187–200, 1990.
[71] M. Kudo and S. Harashita. Superspecial curves of genus 4 in small characteristic. *Finite Fields Appl.*, 45:131–169, 2017.
[72] C. Lennon. Trace formulas for Hecke operators, Gaussian hypergeometric functions, and the modularity of a threefold. *J. Number Theory*, 131(12):2320–2351, 2011.
[73] D. J. Madden. Arithmetic in generalized Artin–Schreier extensions of $k(x)$. *J. Number Theory*, 10(3):303–323, 1978.
[74] K. Matsuo, J. Chao, and S. Tsujii. An improved baby step giant step algorithm for point counting of hyperelliptic curves over finite fields. In *Algorithmic number theory (Sydney, 2002)*, volume 2369 of *Lecture Notes in Comput. Sci.*, pages 461–474. Springer, Berlin, 2002.

[75] K. Matsuo, J. Chao, and S. Tsujii. Baby step giant step algorithms in point counting of hyperelliptic curves. *IEICE Trans. Fundamentals*, E86-A(5):1127–1134, 2003.
[76] B. Mazur. Frobenius and the Hodge filtration. *Bull. Amer. Math. Soc.*, 78:653–667, 1972.
[77] L. Miller. Curves with invertible Hasse–Witt-matrix. *Math. Ann.*, 197:123–127, 1972.
[78] L. Miller. Über gewöhnliche Hyperflächen. I. *J. Reine Angew. Math.*, 282:96–113, 1976.
[79] L. Miller. Über gewöhnliche Hyperflächen. II. *J. Reine Angew. Math.*, 283/284:402–420, 1976.
[80] N. O. Nygaard. Slopes of powers of Frobenius on crystalline cohomology. *Ann. Sci. École Norm. Sup. (4)*, 14(4):369–401 (1982), 1981.
[81] N. O. Nygaard. On supersingular abelian varieties. In *Algebraic geometry (Ann Arbor, Mich., 1981)*, volume 1008 of *Lecture Notes in Math.*, pages 83–101. Springer, Berlin, 1983.
[82] L. D. Olson. Hasse invariants and anomalous primes for elliptic curves with complex multiplication. *J. Number Theory*, 8(4):397–414, 1976.
[83] Ë. Onishi. Generalized Bernoulli–Hurwitz numbers and universal Bernoulli numbers. *Uspekhi Mat. Nauk*, 66(5):47–108, 2011.
[84] Ë. Onishi. Generalized Bernoulli–Hurwitz numbers and universal Bernoulli numbers. *Russian Math. Surveys*, 66(5):871–932, 2011.
[85] A. l. Pacheco. A note on relations between the zeta-functions of Galois coverings of curves over finite fields. *Canad. Math. Bull.*, 33(3):282–285, 1990.
[86] R. J. Pries. Jacobians of quotients of Artin–Schreier curves. In *Recent progress in arithmetic and algebraic geometry*, volume 386 of *Contemp. Math.*, pages 145–156. Amer. Math. Soc., Providence, RI, 2005.
[87] R. Pries. The p-torsion of curves with large p-rank. *Int. J. Number Theory*, 5(6):1103–1116, 2009.
[88] R. Pries and K. Stevenson. A survey of Galois theory of curves in characteristic p. In *WIN—Women in numbers*, volume 60 of *Fields Inst. Commun.*, pages 169–191. Amer. Math. Soc., Providence, RI, 2011.
[89] H.-G. Rück. Class groups and L-series of function fields. *J. Number Theory*, 22(2):177–189, 1986.
[90] P. Sarkar and S. Singh. A simple method for obtaining relations among factor basis elements for special hyperelliptic curves. *Appl. Algebra Engrg. Comm. Comput.*, 28(2):109–130, 2017.
[91] J. H. Silverman. *The arithmetic of elliptic curves*, volume 106 of *Grad. Texts in Math.* Springer, Dordrecht, second edition, 2009.
[92] G. Sohn. Computing the number of points on genus 3 hyperelliptic curves of type $Y^2 = X^7 + aX$ over finite prime fields. *J. Appl. Math. Inform.*, 32(1–2):17–26, 2014.
[93] G. Sohn and H. Kim. Explicit bounds of polynomial coefficients and counting points on Picard curves over finite fields. *Math. Comput. Modelling*, 49(1–2):80–87, 2009.
[94] K.-O. Stöhr and J. F. Voloch. A formula for the Cartier operator on plane algebraic curves. *J. Reine Angew. Math.*, 377:49–64, 1987.
[95] F. J. Sullivan. p-torsion in the class group of curves with too many automorphisms. *Arch. Math. (Basel)*, 26:253–261, 1975.
[96] Y. Sung. Rational points over finite fields on a family of higher genus curves and hypergeometric functions. *Taiwanese J. Math.*, 21(1):55–79, 2017.
[97] S. Tafazolian. A family of maximal hyperelliptic curves. *J. Pure Appl. Algebra*, 216(7):1528–1532, 2012.
[98] Y. Takeda. Groups of Russell type and Tango structures. In *Affine algebraic geometry*, volume 54 of *CRM Proc. Lecture Notes*, pages 327–334. Amer. Math. Soc., Providence, RI, 2011.
[99] Y. Takeda and K. Yokogawa. Pre-Tango structures on curves. *Tohoku Math. J. (2)*, 54(2):227–237, 2002.
[100] Y. Takizawa. Some remarks on the Picard curves over a finite field. *Math. Nachr.*, 280(7):802–811, 2007.
[101] D. L. Ulmer. On universal elliptic curves over Igusa curves. *Invent. Math.*, 99(2):377–391, 1990.
[102] R. C. Valentini. Hyperelliptic curves with zero Hasse–Witt matrix. *Manuscripta Math.*, 86(2):185–194, 1995.
[103] T. Washio. On class numbers of algebraic function fields defined by $y^2 = x^5 + ax$ over GF(p). *Arch. Math. (Basel)*, 41(6):509–516, 1983.

[104] N. Yui. On the Jacobian variety of the Fermat curve. *J. Algebra*, 65(1):1–35, 1980.
[105] N. Yui. The arithmetic of the product of two algebraic curves over a finite field. *J. Algebra*, 98(1):102–142, 1986.
[106] N. Yui. Jacobi quartics, Legendre polynomials and formal groups. In *Elliptic curves and modular forms in algebraic topology (Princeton, NJ, 1986)*, volume 1326 of *Lecture Notes in Math.*, pages 182–215. Springer, Berlin, 1988.
[107] L. Zapponi. On the 1-pointed curves arising as étale covers of the affine line in positive characteristic. *Math. Z.*, 258(4):711–727, 2008.
[108] Y. G. Zarhin. Non-supersingular hyperelliptic Jacobians. *Bull. Soc. Math. France*, 132(4):617–634, 2004.

E-mail address: j.achter@colostate.edu

Department of Mathematics, Colorado State University, Fort Collins, CO 80523
URL: http://www.math.colostate.edu/~achter

E-mail address: however@alumni.caltech.edu

Center for Communications Research, 4320 Westerra Court, San Diego, CA 92121-1967
URL: http://alumnus.caltech.edu/~however