ALGEBRAIC CYCLES AND EVEN UNIMODULAR LATTICES

NEIL DUMMIGAN

The number (up to isomorphism) of positive-definite, even, unimodular lattices of rank $8r$ grows rapidly with r. However, Bannai [1] has shown that, when counted according to weight, those with non-trivial automorphisms make up a fraction of the whole, which goes rapidly to zero as $r \to \infty$. Therefore it is of some interest to produce families of positive-definite, even, unimodular lattices with large automorphism groups and unbounded ranks.

Suppose that G is a finite group and V is an irreducible $\mathbb{Q}[G]$-module such that $V \otimes \mathbb{R}$ is still irreducible. Then, as observed by Gross [8], the space of G-invariant symmetric bilinear forms on V is one-dimensional and is necessarily generated by a positive-definite form, unique up to scaling by non-zero positive rationals. Thompson [23] showed that, if V is also irreducible mod p for all primes p, then it contains an invariant lattice (unique up to scaling) which is even and unimodular with appropriate scaling of the quadratic form. Examples arising in this manner are the E_8-lattice of rank 8, the Leech lattice of rank 24 and the Thompson–Smith lattice of rank 248. Gow [6] has also constructed some examples associated with the basic spin representations of $2A_n$ and $2S_n$.

Gross [8] showed how one may obtain more examples by generalising Thompson's method to deal with the possibility that V is not absolutely irreducible. Thus he reconstructed the Barnes–Wall lattices of ranks 2^{f+1} (which are unimodular when f is even). He also obtained families of lattices associated with the Weil representations of finite symplectic groups (some of which had previously been constructed by Gow [7]) and families of even unimodular lattices of ranks $2p^2(p^2-1)$ associated with the cuspidal unipotent representation of the finite projective unitary group $\mathrm{PU}(3, p^2)$. Tiep [25, 26] has investigated further examples of the 'globally irreducible' representations which give rise to special lattices in this way.

The examples considered by Gross are closely related to the Mordell–Weil lattices of Elkies and Shioda [4, 20]. These are the groups of rational points on certain constant (or potentially constant) elliptic curves over the function fields of algebraic curves over finite fields. The finite group action comes from automorphisms of the algebraic curve and the quadratic form comes from a scaling of the canonical height pairing.

Elkies [5] has constructed the Barnes–Wall lattices as sublattices of certain Mordell–Weil lattices arising from hyperelliptic curves in characteristic 2 (and the square of the index is the order of the Shafarevich–Tate group). In [3] we showed how the symplectic group lattices may be viewed as sublattices of Mordell–Weil lattices arising from hyperelliptic curves in odd characteristic, thus obtaining a lower bound for the minimal norm.

The purpose of this paper is to generalise the families of invariant even unimodular lattices associated with $\mathrm{PU}(3, p^2)$ to the case $G := \mathrm{PU}(n+2, q)$ for any odd $n \geqslant 1$ and any even power $q = p^f$ of a prime number; G acts naturally by automorphisms defined over $\mathbb{F}_{q^2}$ on the n-dimensional projective hypersurface

$$X_n : x_0^{q+1} + x_1^{q+1} + \cdots + x_{n+1}^{q+1} = 0.$$

We construct the desired lattices as sublattices of the groups of primitive codimension $(n+1)/2$ algebraic cycles (modulo numerical equivalence) on $X_n \times E$, where the E are elliptic curves chosen in a suitable isogeny class. The rank is $2(q^{n+1} - q^n + \cdots + q^2 - q)$ and the quadratic form comes from a scaling of the intersection pairing. That it is a definite quadratic form follows from the observation of Gross mentioned in the second paragraph. Notice that this provides examples for which Grothendieck's 'Hodge-style' standard conjecture [9] is true. Similarly the conjecture is true for codimension $n/2$ cycles on X_n when n is even. These X_n were also used by Tate [21] as examples for which his conjecture on algebraic cycles and poles of zeta functions may be confirmed.

When $n = 1$ these lattices are sublattices of the familiar Mordell–Weil lattices arising from Fermat curves of degree $q + 1$. When $n = 1$ and $f = 2$ they are the examples of Gross already mentioned, but when $n = 1$ and $f > 2$ they do not come from globally irreducible representations of any groups. Tiep has explained to me how this follows from his work [24, 26]. (See [3, Section 10].)

Contents
1. Fermat hypersurfaces and finite unitary groups
2. The definite intersection form
3. Almost global irreducibility
4. The crystalline cohomology of X_n
5. The range of the cycle class map
6. An even unimodular sublattice
7. Invariance of the sublattice
8. Some remarks

1. *Fermat hypersurfaces and finite unitary groups*

Let p be any prime and $q = p^f$ a power of p. Let k be the finite field $\mathbb{F}_{q^2}$ and let $\bar{k}$ be an algebraic closure. For each $n \geqslant 1$ one may consider the n-dimensional Fermat hypersurface of degree $q + 1$ in $\mathbb{P}^{n+1}/k$. Then

$$X_n : x_0^{q+1} + x_1^{q+1} + \cdots + x_{n+1}^{q+1} = 0$$

is its equation in homogeneous coordinates. One checks immediately that X_n is nonsingular.

The group $\mathrm{GL}(n+2, q^2)$ of all invertible $(n+2) \times (n+2)$ matrices over k acts on $\mathbb{P}^{n+1}/k$ by its natural action on homogeneous coordinates. We may define a finite unitary group $U(n+2, q)$ as follows:

$$U(n+2, q) = \{A \in \mathrm{GL}(n+2, q^2) : A^{(q)t}A = I\}.$$

Here I is the identity matrix, $A^{(q)}$ is the matrix obtained from A by applying the non-trivial automorphism of $k/\mathbb{F}_q$ to all entries, and B^t denotes the transpose of a matrix B. While $\mathrm{GL}(n+2, q^2)$ acts on the projective space $\mathbb{P}^{n+1}/k$ the subgroup $U(n+2, q)$

preserves the hypersurface X_n. Since the subgroup of scalar matrices acts trivially on projective space we mod out by it to obtain an action of the finite projective unitary group $G := \mathrm{PU}(n+2, q)$ on X_n. Although X_n is clearly defined over $\mathbb{F}_p$ we generally consider it as a variety over $k = \mathbb{F}_{q^2}$ since G acts on X_n by automorphisms defined over k.

Fix l to be any prime different from p. Then one may consider the l-adic cohomology groups $H^i(\overline{X_n}, \mathbb{Q}_l)$, which vanish except for $0 \leqslant i \leqslant 2n$. Here $\overline{X_n}$ is just X_n considered as a variety over $\overline{k}$. Each of these groups is a finite-dimensional vector space over the field $\mathbb{Q}_l$ of l-adic numbers. Let β_i be the dimension of $H^i(\overline{X_n}, \mathbb{Q}_l)$.

PROPOSITION 1. *We have*
(1) $\beta_i = 0$ *if i is odd and $i \neq n$;*
(2) $\beta_i = 1$ *if i is even and $i \neq n$;*
(3) $\beta_n = \begin{cases} q^{n+1} - q^n + \cdots + q^2 - q & \text{if } n \text{ is odd;} \\ q^{n+1} - q^n + \cdots + q^3 - q^2 + q + 1 & \text{if } n \text{ is even.} \end{cases}$

This is obtained by comparison with characteristic zero and by using well-known results about the Betti numbers of diagonal hypersurfaces [14].

The q^2-power geometric Frobenius morphism ϕ acts on $\overline{X_n}$ and hence, by functoriality, on each $H^i(\overline{X_n}, \mathbb{Q}_l)$. By counting k-rational points on X_n as in [28] and using the l-adic cohomological formula for $\#X_n(k)$ one obtains the following.

PROPOSITION 2. *The morphism ϕ acts on $H^n(\overline{X_n}, \mathbb{Q}_l)$ as the scalar $(-q)^n$.*

Let E/k be an elliptic curve such that ϕ is the multiplication map $[-q]$. It is known that such an E may be chosen and is unique up to isogeny over k. Further, all the endormorphisms of E are defined over k and the endomorphism ring is isomorphic to some maximal order R (strictly speaking, any of a conjugacy class of isomorphic maximal orders) in K, the definite quaternion algebra over $\mathbb{Q}$ ramified at p and ∞. For each maximal order R there are one or two possible choices of E in the isogeny class according as the two-sided ideal class group of R is trivial or not. See [27] for details. Observe that E is supersingular. For each q we imagine that a choice of E has been fixed.

2. *The definite intersection form*

Henceforth we suppose that n is odd. Let $Y_n = X_n \times E$ so Y_n is an $(n+1)$-dimensional proper smooth variety defined over k. Let $m = (n+1)/2$. Let A^m be the free abelian group generated formally by closed irreducible subvarieties, defined over k, of codimension m in Y_n. Let $B^m = A^m \otimes_{\mathbb{Z}} \mathbb{Q}$. There is a $\mathbb{Q}$-linear cycle-class map (choosing an identification of $\mathbb{Q}_l/\mathbb{Z}_l$ with the l-power roots of unity)

$$c : B^m \longrightarrow H^{2m}(\overline{Y_n}, \mathbb{Q}_l).$$

By the Künneth formula we have

$$H^{2m}(\overline{Y_n}, \mathbb{Q}_l) \simeq H^n(\overline{X_n}, \mathbb{Q}_l) \otimes H^1(\overline{E}, \mathbb{Q}_l) \oplus H^{n+1}(\overline{X_n}, \mathbb{Q}_l) \otimes H^0(\overline{E}, \mathbb{Q}_l)$$
$$\oplus H^{n-1}(\overline{X_n}, \mathbb{Q}_l) \otimes H^2(\overline{E}, \mathbb{Q}_l).$$

There is a bilinear intersection pairing $\cdot : A^m \times A^m \to \mathbb{Z}$ which extends to $\cdot : B^m \times B^m \to \mathbb{Q}$. There is also the cup-product $\cdot : H^{2m}(\overline{Y_n}, \mathbb{Q}_l) \times H^{2m}(\overline{Y_n}, \mathbb{Q}_l) \to \mathbb{Q}_l$. We use the

same notation twice without risk of confusion, particularly since intersection and cup-products are compatible: for any $b_1, b_2 \in B^m$ we have $b_1 \cdot b_2 = c(b_1) \cdot c(b_2)$. An element $b \in B^m$ is said to be l-cohomologically equivalent to zero if $c(b) = 0$. It is said to be numerically equivalent to zero if $b \cdot b' = 0$ for all $b' \in B^m$. The above compatibility clearly implies that if a cycle is l-cohomologically equivalent to zero then it is numerically equivalent to zero. We denote this $B_l^m \subset B_{\text{num}}^m$.

The q^2-power geometric Frobenius morphism ϕ acts on $H^{2m}(\overline{Y_n}, \mathbb{Q}_l)$ as the scalar q^{n+1}. A conjecture of Tate [21] then predicts that $c(B^m)\mathbb{Q}_l = H^{2m}(\overline{Y_n}, \mathbb{Q}_l)$.

PROPOSITION 3.   *We have*
(1) $c(B^m)\mathbb{Q}_l = H^{2m}(\overline{Y_n}, \mathbb{Q}_l)$,
(2) $B_l^m = B_{\text{num}}^m$,
(3) *c induces an isomorphism* $(B^m / B_{\text{num}}^m) \otimes \mathbb{Q}_l \simeq H^{2m}(\overline{Y_n}, \mathbb{Q}_l)$.

Proof.   One may prove (1) by directly imitating the argument of Katsura and Shioda [13, Section 2] using Tate's theorem on homomorphisms of abelian varieties over finite fields [22] and the inductive structure of Fermat varieties. Given this, (2) and (3) follow from Proposition 8.4 of [18].

Recall that $H^{2m}(\overline{Y_m}, \mathbb{Q}_l)$ is a direct sum of three summands, listed above. The second and third summands are each one-dimensional, generated by the classes of cycles $x, y \in B^m$ respectively; x may be taken to be the product with E of the intersection of m hyperplane sections of X_n and y may be taken to be the product with a point of E of the intersection of $m-1$ hyperplane sections of X_n. Then $x \cdot x = y \cdot y = 0$ and $x \cdot y \neq 0$. Define

$$C^m = \{b \in B^m : b \cdot x = b \cdot y = 0\}.$$

Since the first summand of $H^{2m}(\overline{Y_n}, \mathbb{Q}_l)$ is clearly orthogonal to the other two with respect to cup-product, we find that

$$c(C^m)\mathbb{Q}_l = H^n(\overline{X_n}, \mathbb{Q}_l) \otimes H^1(\overline{E}, \mathbb{Q}_l).$$

DEFINITION 1. $V = C^m / (C^m \cap B_{\text{num}}^m)$.

Thus V is a $\mathbb{Q}$-vector space of dimension $2(q^{n+1} - q^n + \cdots + q^2 - q)$. We have

$$V \otimes \mathbb{Q}_l \simeq H^n(\overline{X_n}, \mathbb{Q}_l) \otimes H^1(\overline{E}, \mathbb{Q}_l).$$

Further, the natural action of $G = \mathrm{PU}(n+2, q)$ on X_n endows V with the structure of $\mathbb{Q}[G]$-module. The intersection pairing gives us a G-invariant symmetric bilinear form $\langle,\rangle : V \times V \to \mathbb{Q}$. The faithful action of the quaternion algebra K on $H^1(\overline{E}, \mathbb{Q}_l)$ commutes with the action of G on $H^n(\overline{X_n}, \mathbb{Q}_l)$ so K is naturally contained in the endomorphism algebra $\mathrm{End}_{\mathbb{Q}[G]}(V)$.

PROPOSITION 4.   *We have*
(1) *V is an irreducible $\mathbb{Q}[G]$-module,*
(2) *$V \otimes \mathbb{R}$ is an irreducible $\mathbb{R}[G]$-module,*
(3) *$\langle,\rangle$ is definite.*

Proof.   (1) According to [11], the $\mathbb{Q}_l[G]$-module $H^n(\overline{X_n}, \mathbb{Q}_l)$ is absolutely irreducible with character ψ, say. It follows that the $\mathbb{Q}[G]$-module V has character 2ψ.

If it were reducible (over $\mathbb{Q}$) its endomorphism algebra $\mathrm{End}_{\mathbb{Q}[G]}(V)$ would be $M_2(\mathbb{Q})$, which is impossible since we know that it contains (in fact is equal to) the quaternion algebra K.

(2) Similarly $V \otimes \mathbb{R}$ is irreducible since $K \otimes \mathbb{R}$, the Hamiltonian quaternion algebra, is not $M_2(\mathbb{R})$.

(3) Since $V \otimes \mathbb{R}$ is irreducible it follows from [8, Section 2] that the space of G-invariant symmetric bilinear forms on $V \otimes \mathbb{R}$ is one-dimensional and is generated by a positive-definite form. The extension of $\langle , \rangle$ to $V \otimes \mathbb{R}$ is G-invariant and is not zero (by definition of numerical equivalence) so must be a definite form.

As noted in the introduction, (3) is what is predicted by a conjecture of Grothendieck [9]. Actually, the space of primitive codimension m cycles (modulo numerical equivalence) on Y_n, with respect to a natural ample divisor, is a little larger than V, containing also the class of $x - y$. However, V is the interesting part.

3. Almost global irreducibility

Recall that R is a maximal order in K and is the endomorphism ring of E. The group ring $R[G]$ acts naturally on V and we let M be some $R[G]$-invariant lattice in V. For definiteness we may take M to be the image in V of $A^m \cap C^m$.

PROPOSITION 5. (1) *The character ψ is absolutely irreducible* $\mod l$ *for each prime* $l \neq p$.

(2) *The quotient M/lM is an irreducible $(R/lR)\,[G]$-module for each prime $l \neq p$.*

(3) *After rescaling $\langle , \rangle$ by some non-zero rational number coprime to p, we may assume that it is integral on M and that* $\det M$ *(that is,* $\det(\langle v_i, v_j \rangle)$*, where $\{v_i\}$ is a $\mathbb{Z}$-basis for M) is purely a power of p.*

Proof. Suppose that $l \neq p$ is a prime such that ψ is not absolutely irreducible $\mod l$. Then $H^n(\overline{X_n}, \mathbb{Q}_l)$ provides a representation with coefficients in $\mathbb{Q}_l$ affording the character ψ. Let S be a G-stable $\mathbb{Z}_l$-lattice in $H^n(\overline{X_n}, \mathbb{Q}_l)$. Our supposition (stated more precisely) is that the $\mathbb{F}_l[G]$-module S/lS is not absolutely irreducible. Observe that $q^{n+1} - q^n + \cdots + q^2 - q$ is the smallest dimension of an absolutely irreducible, nontrivial representation of G in any characteristic not equal to p [15]. Hence the only possibility is that for some sufficiently large d the irreducible composition factors of the $\mathbb{F}_{l^d}[G]$-module $(S/lS) \otimes_{\mathbb{F}_l} \mathbb{F}_{l^d}$ are all trivial. (Recall that if $l | \#G$ then representations of G in characteristic l are not necessarily completely reducible.)

Choosing a suitable basis, the action of G on $(S/lS) \otimes \mathbb{F}_{l^d}$ is by upper-triangular, unipotent matrices over $\mathbb{F}_{l^d}$. Letting U be the group of such matrices, we have a homomorphism $\theta \colon G \to U$. Now $\#U$ is a power of l so the restriction of θ to any subgroup H of G of order prime to l is trivial. Let $S' = S \otimes_{\mathbb{Z}_l} W(\mathbb{F}_{l^d})$, where $W(\mathbb{F}_{l^d})$ is the ring of integers in the unramified extension of degree d of $\mathbb{Q}_l$. We have just seen that if H is a subgroup of G of order prime to l than H acts trivially on S'/lS'. By induction and using a similar argument about homomorphisms of H to groups of l-power order being trivial, we see that H acts trivially on $S'/l^r S'$ for all $r \geqslant 1$, hence that H acts trivially on S and on $H^n(\overline{X_n}, \mathbb{Q}_l)$.

Now we make a special choice of H. There is a subgroup of G isomorphic to the symmetric group S_{n+2}, which acts on X_n by permuting the coordinates $x_0, x_1, \ldots, x_{n+1}$.

If $l \neq 2$ we let H be the cyclic subgroup generated by some arbitrary fixed transposition. If $l = 2$ we use a 3-cycle instead. It follows from Section 5, Proposition 8, that the crystalline cohomology $H^n_{\mathrm{crys}}(X_n)$ provides a representation with coefficients in $W = W(\mathbb{F}_{q^2})$ affording the character ψ. Therefore H acts trivially on $H^n_{\mathrm{crys}}(X_n)$ and on its reduction mod p, the algebraic de Rham cohomology $H^n_{dR}(X_n)$. But the next section contains explicit bases for the subfactors of the Hodge filtration of $H^n_{dR}(X_n)$ and it is clear that the action of H (permuting coordinates) is not trivial. This contradiction shows that (1) must be true.

(2) follows from (1) and [**8**, Proposition 4.2(3)]. Then (3) follows from the arguments of Sections 3 and 5 of [**8**] (note that $\langle,\rangle$ does come from a G-invariant K-Hermitian form since the one-dimensional space of such forms is identified with the one-dimensional space of G-invariant symmetric bilinear forms).

Although R and M depend on the particular choice of E, the $\mathbb{Q}[G]$-module V does not, since an irreducible $\mathbb{Q}[G]$-module is determined by its character, and the character 2ψ is determined without reference to E as twice the character of the $\mathbb{Q}_l[G]$-module $H^n(\overline{X_n}, \mathbb{Q}_l)$. By choosing the sign of the scaling factor appropriately, we may assume that $\langle,\rangle$ is *positive*-definite. Our goal in the rest of the paper is to produce an $R[G]$-invariant sublattice of M which, after rescaling $\langle,\rangle$ by a power of p, is even and unimodular, at least in the case that f is even. To get a suitable model of $V \otimes \mathbb{Q}_p$ we need to use crystalline cohomology, for which a good concise reference is [**12**].

4. *The crystalline cohomology of* X_n

Let W be the ring of infinite Witt vectors over k. Thus W is the ring of integers in the unramified extension L of degree $2f$ of $\mathbb{Q}_p$. Its maximal ideal is pW and $W/pW \simeq k$. Let σ be the automorphism of $W/\mathbb{Z}_p$ which lifts the pth-power automorphism of k. Associated with any proper, smooth variety Z/k of dimension d are finitely generated W-modules $H^i(Z) = H^i_{\mathrm{crys}}(Z)$ which are trivial except for $0 \leqslant i \leqslant 2d$. The dimension of $H^i(Z)$ is equal to the dimension of $H^i(\overline{Z}, \mathbb{Q}_l)$ for any prime $l \neq p$. There is a cup-product structure and if Z is a hypersurface then $H^i(Z)$ is a free W-module. If Z^*/W is a proper smooth scheme whose special fiber is Z/k, then there is a natural isomorphism $H^i(Z) \simeq H^i_{dR}(Z^*)$, the ith algebraic de Rham cohomology of Z^*. We always choose X_n^* to be the natural lifting of X_n defined by the same equation as X_n. The action of the diagonal subgroup T of G on X/k lifts to X^*/W though the action of the whole group G does not.

The identification of $H^n(X_n)$ with $H^n_{dR}(X_n^*)$ endows it with a Hodge filtration

$$H^n(X_n) = M_0 \supset \ldots \supset M_{n+1} = \{0\},$$

and for all $0 \leqslant k \leqslant n$ we have $M_k/M_{k+1} \simeq H^{n-k}(X_n^*, \Omega^k)$, the cohomology of the kth exterior power of the sheaf of differentials on X_n^*.

PROPOSITION 6.   (1) *The cohomology* $H^{n-k}(X_n^*, \Omega^k)$ *has a W-basis consisting of elements which may be written*

$$w_{m_0, m_1, \ldots, m_{n+1}} = x_0^{m_0} x_1^{m_1} \ldots x_{n+1}^{m_{n+1}} dx_0 \ldots dx_{n+1},$$

where $(m_0, \ldots, m_{n+1})$ *ranges over all* $(n+2)$-*tuples such that* $0 \leqslant m_i \leqslant q-1$ *for each i and* $\sum m_i = (n+1-k)q - (k+1)$.

(2) *An element* $\mathrm{diag}(a_0, \ldots, a_{n+1})$ *of* T *acts on* $w_{m_0 \ldots, m_{n+1}}$ *as the scalar*

$$a_0^{m_0+1} \ldots a_{n+1}^{m_{n+1}+1}.$$

(3) *The* $w_{m_0, m_1, \ldots, m_{n+1}}$ *lift to a* W-*basis for* $H^n(X_n)$ *consisting of simultaneous eigenvectors for* T *with distinct characters.* (*We also denote these basis elements* $w_{m_0, \ldots, m_{n+1}}$.)

Proof. (1) follows from [**19**, Section 3]. Then (2) is obvious. Observing that the characters of T arising are all distinct, (3) then follows from the fact that p does not divide the order of T.

DEFINITION 2. If $\sum m_i = (n+1-k)q - (k+1)$ we say that $w_{m_0, \ldots, m_{n+1}}$ (or any nonzero multiple of it) is of type k.

The absolute pth-power Frobenius morphism of the scheme X_n to itself (defined to be the identity on points and the pth power on the structure sheaf) gives rise, by functoriality, to a σ-linear map F from $H^n(X_n)$ to itself. Thus $F(av) = a^\sigma F(v)$ for any $a \in W$ and $v \in H^n(X_n)$.

PROPOSITION 7. (1) *If* w *is one of our standard basis elements for* $H^n(X_n)$ *then* $Fw = cw'$ *for some* $c \in W$ *and* w' *some standard basis element. The character of* T *associated to* w' *is* p *times that associated to* w.
(2) *If* w *is of type* k *then* $\mathrm{ord}_p(c) = k$.
(3) *If* w *is of type* k *then* $F^f w$ *is of type* $n-k$.

Proof. (1) For any fixed $t \in T$ suppose that $t.w = \lambda w$. Then $t.Fw = F(t.w) = F(\lambda w) = \lambda^\sigma Fw = \lambda^p Fw$ since λ is a root of unity. Thus Fw is a simultaneous eigenvector for T, its associated character being p times that for w. It must be a multiple of one of our standard basis of elements since their associated characters are all distinct, c.f. [**10**, **19**, **20**].
(2) Ogus explains near the end of this paper [**19**] how this follows from Mazur's work on Frobenius and the Hodge filtration [**16**, **17**].
(3) By (1), F^f multiplies characters by $p^f = q$ but T has exponent $q+1$ so F^f multiplies characters by -1. Since $(q-1-m_i)+1 = (q+1)-(m_i+1)$, one sees that

$$w_{q-1-m_0, \ldots, q-1-m_{n+1}}$$

has minus the character of $w_{m_0, \ldots, m_{n+1}}$. If $\sum m_i = (n+1-k)q - (k+1)$ one easily checks that $\sum(q-1-m_j) = (n+1-(n-k))q - ((n-k)+1)$.

Adopting a new notation, suppose that w_1 is some standard basis element in $H^n(X_n)$. Then there are standard basis elements w_i for $i \geq 1$ and elements $c_i \in W$ such that $Fw_i = c_i w_{i+1}$ for each i and $\mathrm{ord}_p(c_i) = k_i$, where w_i is of type k_i. It follows from the crystalline cohomological formula for $\#X_n(k)$ that F^{2f} acts as multiplication by $(-q)^n$ on $H^n(X_n)$. Hence $w_{i+2f} = w_i$ and subscripts may be thought of mod $2f$. We get cyclic 'F-orbits' of basis elements of lengths dividing $2f$. Note that $k_i + k_{f+i} = n$. Incidentally, it follows fairly easily from the fact that X_n is really defined over $\mathbb{F}_p$ that all the c_i are actually in $\mathbb{Z}_p$.

5. *The range of the cycle class map*

Let $c: B^m \to H^{2m}(Y_n) \otimes_W L$ be the cycle map constructed by Milne in Section 2 of [**18**]. Then c is compatible with intersection and cup products and $c(B^m) \subset H^{2m}(Y_n)^{F=p^m} \otimes_{\mathbb{Z}_p} \mathbb{Q}_p$. As for l-adic cohomology, there is a Künneth formula (use [**12**, 3.3] and the fact that everything is torsion-free) and $c(C^m) \subset H^n(X_n) \otimes H^1(E) \otimes L$, so that $c(C^m) \subset (H^n(X_n) \otimes H^1(E))^{F=p^m} \otimes_{\mathbb{Z}_p} \mathbb{Q}_p$.

PROPOSITION 8.   (1) $c(C^m)\mathbb{Q}_p = (H^n(X_n) \otimes H^1(E))^{F=p^m} \otimes_{\mathbb{Z}_p} \mathbb{Q}_p$.
(2) $V \otimes_{\mathbb{Q}} \mathbb{Q}_p \simeq (H^n(X_n) \otimes H^1(E))^{F=p^m} \otimes \mathbb{Q}_p$.

Proof. We shall see soon that the dimension of the right-hand side is $2(q^{n+1} - q^n + \cdots + q^2 - q)$. The action of $K \otimes \mathbb{Q}_p$ on $H^1(E)$ commutes with F, as does the action of G on $H^n(X_n)$, so $K \otimes \mathbb{Q}_p$ acts by $\mathbb{Q}_p[G]$-endomorphisms on the right-hand side. Since $K \otimes \mathbb{Q}_p \neq M_2(\mathbb{Q}_p)$, we find that the right-hand side is an irreducible $\mathbb{Q}_p[G]$-module. (The $W[G]$-module $H^n(X_n)$ must be absolutely irreducible, nontrivial of minimal degree, since the trivial character of T does not occur.) Now $c(C_m)\mathbb{Q}_p$ is a $\mathbb{Q}_p[G]$-submodule so is either zero or the whole thing. But C^m contains elements which are not numerically equivalent to zero, so $c(C^m)\mathbb{Q}_p$ cannot be zero and must be the whole thing. Hence we obtain (1), and (2) now follows by comparing dimensions.

LEMMA 1.   *The cohomology $H^1(E)$ has a W-basis $\{e_0, e_1\}$ such that $Fe_0 = e_1$ and $Fe_1 = \gamma e_0$ with $\mathrm{ord}_p(\gamma) = 1$.*

For the proof see [**2**, Lemma 4].

DEFINITION 3. $S := (H^n(X_n) \otimes H^1(E))^{F=p^m}$.

Our next task is to identify this $\mathbb{Z}_p$-module. The condition $F = p^m$ can be dealt with one F-orbit at a time. Given an F-orbit $J = \{w_1, w_2, \ldots, w_{2f}\}$ (note that this list may involve repetition) we define H_J to be the W-submodule of $H^n(X_n)$ generated by J. Let $S_J = S \cap (H_J \otimes H^1(E))$. Then $S = \bigoplus_J S_J$ and it suffices to examine each S_J.

Now F^f inverts characters and one may check that no self-inverse character occurs, so f is not divisible by the length of any F-orbit. Hence the length of the F-orbit J is of the form $2l$ for some $l \mid f$. Suppose that $w \in S_J$, say

$$w = \sum_{i=1}^{2l} (a_i w_i \otimes e_0 + b_i w_i \otimes e_1).$$

Then $Fw = \sum (a_i^\sigma c_i w_{i+1} \otimes e_1 + b_i^\sigma c_i \gamma w_{i+1} \otimes e_0)$. Since we require $Fw = p^m w = p^{(n+1)/2} w$ we have the conditions

$$a_i^\sigma c_i = p^m b_{i+1}, \tag{1}$$

$$b_i^\sigma c_i \gamma = p^m a_{i+1}, \tag{2}$$

hence

$$a_i^{\sigma^2} c_i c_{i+1} \gamma = p^{2m} a_{i+2} = p^{n+1} a_{i+2}, \tag{3}$$

$$b_i^{\sigma^2} c_i c_{i+1} \gamma^\sigma = p^{2m} b_{i+2} = p^{n+1} b_{i+2},$$

so

$$\mathrm{ord}_p(a_{i+2}) = \mathrm{ord}_p(a_i) + k_i + k_{i+1} - n, \tag{5}$$

$$\mathrm{ord}_p(b_{i+2}) = \mathrm{ord}_p(b_i) + k_i + k_{i+1} - n. \tag{6}$$

Henceforth we assume that f is even.

The F-orbit $J = \{w_1, w_2, \ldots, w_{2l}\}$ may be divided into two 'complementary' F^2-orbits $J_0 = \{w_1, w_3, \ldots, w_{2l-1}\}$ and $J_e = \{w_2, w_4, \ldots, w_{2l}\}$. (Here w_1 has been chosen arbitrarily.) We see from the above equations that the coefficient a_1 determines all the a_i for i odd and all the b_i for i even. But a particular choice of a_1 will not lead to an element of S_J unless

$$a_1^{\sigma^{2l}} c_1 c_2 \ldots c_{2l} \gamma \gamma^{\sigma^2} \ldots \gamma^{\sigma^{2l-2}} = p^{l(n+1)} a_1.$$

Using the fact that F^{2f} acts as $-q^n$ on $H^n(X_n)$ and as $-q$ on $H^1(E)$, combined with Hilbert's Theorem 90, one easily checks that the possible coefficients a_1 form a $\mathbb{Z}_p$-submodule of rank $2l$ of W. Similar remarks apply to b_1. Hence we obtain the following.

LEMMA 2. *The $\mathbb{Z}_p$-module S_J is free of rank $4l$ and S is a free $\mathbb{Z}_p$-module of rank twice the W-rank of $H^n(X_n)$, namely $2(q^{n+1} - q^n + \cdots + q^2 - q)$.*

In order for all the $\mathrm{ord}_p(a_i)$ and $\mathrm{ord}_p(b_i)$ to be nonnegative there are certain nonnegative integers n_i and m_i such that necessarily $\mathrm{ord}_p(a_i) \geqslant n_i$ and $\mathrm{ord}_p(b_i) \geqslant m_i$. We have

$$m_{i+1} = n_i + k_i - m, \tag{7}$$

$$n_{i+1} = m_i + k_i + 1 - m, \tag{8}$$

$$n_{i+2} = n_i + k_i + k_{i+1} - n, \tag{9}$$

$$m_{i+2} = m_i + k_i + k_{i+1} - n. \tag{10}$$

Then $S_J \otimes_{\mathbb{Z}_p} W = S_J W$ may be decomposed according to characters of T and has a basis

$$\{p^{n_i} w_i \otimes e_0, p^{m_i} w_i \otimes e_1 : 1 \leqslant i \leqslant 2l\}.$$

LEMMA 3. (1) *For a given F-orbit J the quantity $n_i + m_{f+i}$ depends only on $i \bmod 2$.*

(2) *In fact, $n_i + m_{f+i}$ depends only on J.*

Proof. (1) Using equations (9) and (10) we get

$$(n_{i+2} + m_{f+i+2}) - (n_i + m_{f+i}) = k_i + k_{f+i} + k_{i+1} + k_{f+i+1} - 2n,$$

but this is zero since $k_j + k_{f+j} = n$ for all j.

(2) Recall that f is even. We check that

$$(n_i + m_{f+i}) - (n_{f+i+1} + m_{i+1}) = (n_i - m_{i+1}) + (m_{f+i} - n_{f+i+1})$$
$$= (m - k_i) + (m - 1 - k_{f+i}) = 2m - 1 - (k_i + k_{f+i}) = n - n = 0.$$

DEFINITION 4. (1) $d_J := n_i + m_{f+i}$,

(2) $d_{\max} = \max_J d_J$,

(3) $r_J = d_{\max} - d_J$.

6. *An even unimodular sublattice*

The W-modules $H^1(E)$ and $H^n(X_n)$ are self-dual with respect to the cup-product pairings. This is Poincaré duality (use [12, 3.5.4] and the fact that everything is torsion-free).

LEMMA 4. (1) *We have $e_0 \cdot e_0 = e_1 \cdot e_1 = 0$ and $e_0 \cdot e_1$ is a unit in W.*

(2) *If we and w' are standard basis elements for $H^n(X_n)$ then $w \cdot w' = 0$ unless the characters of T associated to w and w' form an inverse pair. If this happens (that is, if w and w' belong to the same F-orbit and are of the form w_i, w_{f+i}) then $w \cdot w'$ is a p-adic unit.*

Proof. (1) follows from the fact that the cup-product pairing on $H^1(E)$ is skew-symmetric and perfect. (2) follows from the fact that the cup-product pairing on $H^n(X_n)$ is T-invariant and perfect.

LEMMA 5. (1) *If J is an F-orbit and $v, v' \in S_J$ then $v \cdot v'$ is divisible by p^{d_J}.*

(2) *Moreover, $\det S_J = p^{d_J \operatorname{rank} S_J}$. (This is the determinant of the restriction of the cup-product pairing and is well defined as a power of p.)*

Proof. (1) is an easy consequence of the previous lemma and $\det S_J$ may be calculated using our basis for $S_J \otimes_{\mathbb{Z}_p} W$.

Recall that $R = \operatorname{End}(E)$ is a maximal order in K, the definite quaternion algebra over $\mathbb{Q}$ ramified at p and ∞. So there is a two-sided maximal ideal $\mathfrak{p}$ of R such that $pR = \mathfrak{p}^2$. Choose $\pi \in \mathfrak{p}$ such that $\pi \notin pR$. The action of R on $H^1(E)$ commutes with F so R acts on S.

LEMMA 6. *We have*
(1) $\det \pi^{r_J} S_J = p^{d_{\max} \operatorname{rank} S_J}$,
(2) *up to a p-adic unit, $(\pi v) \cdot (\pi v') = p v \cdot v'$ for all $v, v' \in S$,*
(3) *$v \cdot v'$ is divisible by $p^{d_{\max}}$ for all $v, v' \in \pi^{r_J} S_J$.*

Proof. (1) follows from (2) of the previous lemma. (3) follows from (2) combined with (1) of the previous lemma. To prove (2) we note that $S \otimes \mathbb{Q}_p = V \otimes \mathbb{Q}_p$ and cup-product on the left agrees with $\langle , \rangle$ on the right (up to a p-adic unit). The symmetric bilinear form such that $(v, v') \mapsto \langle \pi v, \pi v' \rangle$ for all $v, v' \in V$ is G-invariant, so is necessarily of the form $(v, v') \mapsto c. \langle v, v' \rangle$ for some non-zero rational number c. Since $\mathfrak{p}^2 = pR$ we find that $\operatorname{ord}_p(c) = 1$, as desired.

We define a $\mathbb{Z}_p$-submodule $\mathscr{L}$ of S by

$$\mathscr{L} = \bigoplus_J \pi^{r_J} S_J.$$

Then $\mathscr{L}$ is a $\mathbb{Z}_p$-lattice in $V \otimes \mathbb{Q}_p$. Recall that we have a $\mathbb{Z}$-lattice M in V and that $\langle , \rangle$ is normalised, so that M is an integral lattice and $\det M$ is a power of p.

DEFINITION 5. Let L be the lattice in V such that $L \otimes \mathbb{Z}_l = M \otimes \mathbb{Z}_l$ for all primes $l \neq p$ but $L \otimes \mathbb{Z}_p = \mathscr{L}$.

PROPOSITION 9. (1) *For all $v \in L$ we have $\langle v, v \rangle \in 2 p^{d_{\max}} \mathbb{Z}$.*
(2) *Also, $\det L = p^{d_{\max} \operatorname{rank} L}$.*

Proof. (2) follows from (1) of the previous lemma. Suppose that $v \in L$. To show that $\langle v, v \rangle \in 2\mathbb{Z}_l$ for all primes $l \neq p$ just copy the argument in the proof of [**8**, Proposition 8.3], that is, use the fact that $\langle , \rangle$ is the trace of a Hermitian form. It

remains to show that $\langle v, v \rangle \in 2p^{q_{\max}} \mathbb{Z}_p$. For this recall the basis for S obtained in Section 5. If we express v in terms of this basis and consider $v \cdot v$ we see that only the cross terms survive and each appears twice. Hence we get the factor 2, and the power of p comes from (3) of the previous lemma.

Now we simply rescale $\langle , \rangle$ by dividing it by $p^{q_{\max}}$ to obtain L as an even, unimodular lattice in V. In other words, $\langle v, v \rangle \in 2\mathbb{Z}$ for all $v \in L$ and $\det L = 1$. Also L is R-stable. It remains to prove that it is G-invariant.

7. Invariance of the sublattice

The group A^m, of codimension m cycles on Y_n, is clearly G-invariant, so the lattice M in V is G-invariant. Moreover, $L \otimes \mathbb{Z}_l = M \otimes \mathbb{Z}_l$ for all primes $l \neq p$, so it remains to show that $L \otimes \mathbb{Z}_p$ is G-invariant. Let J and J' be two F-orbits. Any fixed element $g \in G$ maps S to itself. Restricting the domain to S_J and projecting the range to $S_{J'}$ we obtain a map $\theta_g : S_J \to S_{J'}$. It suffices to show that $\theta_g(\pi^{r_J} S_J) \subset \pi^{r_{J'}} S_{J'}$, that is, that $\theta_g(S_J) \subset \pi^{d_J - d_{J'}} S_{J'}$. This is obvious if $d_J \leqslant d_{J'}$ so we suppose that $d_J > d_{J'}$. The following proposition then does the trick.

PROPOSITION 10. $\quad \theta_g(S_J \otimes W) \subset p^{d_J - d_{J'}}(S_{J'} \otimes W)$.

Proof. Let $J = \{w_i\}$ with associated numbers $\{n_i, m_i\}$ (as in Section 5) and $J' = \{w_i'\}$ with associated numbers $\{n_i', m_i'\}$. We may choose w_1 so that either $n_1 = 0$ or $m_1 = 0$. We suppose that $m_1 = 0$ since the other case is similar. For any i we have $n_{f+i} - n_i = (\sum_{j=i}^{f+i-1} k_j) - nf/2$ so that $F^f(p^{n_i} w_i) = p^{n_{f+i} + nf/2} w_{f+i}$ up to multiplication by a p-adic unit. Similar statements hold for the m_i, n_i' and m_i'.

For an arbitrary fixed j suppose that the coefficient of w_j' in $g.p^{n_1} w_1$ is exactly divisible by p^a. Now $F^f(p^{n_1} w_1)$ is divisible by $p^{n_{f+1} + nf/2}$ so $g.F^f(p^{n_1} w_1)$ is divisible by $p^{n_{f+1} + nf/2}$. But g commutes with F^f so certainly the coefficient of w_{f+j}' in $F^f g.p^{n_1} w_1$ is divisible by $p^{n_{f+1} + nf/2}$. Hence

$$a + n_{f+j}' - n_j' + nf/2 \geqslant n_{f+1} + nf/2.$$

Hence (since $m_1 = 0$) we have

$$a \geqslant n_j' + n_{f+1} - n_{f+j}' \geqslant n_j' + (n_{f+1} + m_1) - (n_{f+j}' + m_j') = n_j' + d_J - d_{J'}.$$

This implies that $\theta_g(p^{n_1} w_1 \otimes e_0) \subset p^{d_J - d_{J'}}(S_{J'} \otimes W)$. In fact, since g is acting only on $H^n(X_n)$, we have $\theta_g(p^{n_1} w_1 \otimes e_0) \subset p^{d_J - d_{J'}}(H_{J'} \otimes W e_0)$.

Up to p-adic units, $p^{m_{i+1}} w_{i+1} = F p^{n_i} w_i / p^m$ and $p^{n_{i+2}} w_{i+2} = F p^{m_{i+1}} w_{i+1} / p^{m-1}$. Similar statements apply with J replaced by J'. Repeatedly applying F/p^m and F/p^{m-1} to the case $i = 1$ we obtain

$$\theta_g(p^{n_i} w_i \otimes e_0) \subset p^{d_J - d_{J'}}(S_{J'} \otimes W) \quad \text{for } i \text{ odd,}$$
$$\theta_g(p^{m_i} w_i \otimes e_1) \subset p^{d_J - d_{J'}}(S_{J'} \otimes W) \quad \text{for } i \text{ even.}$$

That takes care of half the basis elements for $S_J \otimes W$. But we also have $m_i = 0$ for some even i or $n_i = 0$ for some odd i so we may take care of the rest similarly. This is because our basis elements for $S_J \otimes W$ come in two F-orbits and for each orbit there is a minimum n_i or m_i equal to zero.

8. *Some remarks*

(1) There remains the problem of obtaining a reasonable lower bound for the minimal norm of L. This leads to several problems. One needs to know the relationship between $M \otimes \mathbb{Z}_p$ and $(H^n(X_n) \otimes H^1(E))^{F=p^m}$. Are they always equal as in the case $n = 1$? Is $\det M$ a pure power of p before rescaling the intersection pairing? Then one needs a lower bound for the self-intersection number of a cycle in $C^m \cap A^m$. In the case $n = 1$ one divides $\#X_1(k)$ by $\#E(k)$ and obtains the bound $2(q-1)$. In the case $n = 1$ a lower bound for the minimal norm of L is $2(q-1)/p^{f/2}$ (since $d_{\max} = f/2$). I do not know what to do for $n > 1$.

(2) When f is odd it is easy to adapt the above methods to produce an R-stable, G-invariant, even integral lattice L in V with $\det L = p^{(\mathrm{rank}\, L)/2}$.

(3) Remember that L (and R, up to conjugacy) depend on the particular choice of E in a fixed k-isogeny class. For a given maximal order R in K, does every even, unimodular, $R[G]$-stable lattice in V arise from our construction for some choice of E with endomorphism ring R?

(4) When n is even, primitive codimension $n/2$ cycles on X_n give an irreducible $\mathbb{Q}[G]$-module V of dimension $q^{n+1} - q^n + \cdots + q^3 - q^2 + q$ as a vector space. The intersection pairing endows V with a G-invariant, definite, symmetric bilinear form. Our method breaks down since when n is even the minimal degree of an absolutely irreducible, nontrivial representation of G in characteristic not equal to p is $q^{n+1} - q^n + \cdots + q^3 - q^2 + q - 1$ [15]. This is just as well since otherwise we would be able to produce even unimodular lattices of rank not divisible by 8, which is impossible.

(5) If $p \geqslant n+1$ the reduction $\mathrm{mod}\, p$ of $H^n(X_n)$ (namely $H^n_{dR}(X_n)$) has $(n+1)^f$ irreducible $k[G]$-module composition factors, each occurring with multiplicity one.

References

1. E. BANNAI, 'Positive definite unimodular lattices with trivial automorphism groups', *Mem. Amer. Math. Soc.* 429 (1990) 1–70.
2. N. DUMMIGAN, 'The determinants of certain Mordell–Weil lattices', *Amer. J. Math.* 117 (1995) 1409–1429.
3. N. DUMMIGAN, 'Symplectic group lattices as Mordell–Weil sublattices', *J. Number Theory* 61 (1996) 365–387.
4. N. D. ELKIES, 'Mordell–Weil lattices in characteristic 2: I. Construction and first properties, *Internat. Math. Res. Notices* 8 (1994) 343–360.
5. N. D. ELKIES, Papers in preparation on Mordell–Weil lattices.
6. R. GOW, 'Unimodular integral lattices associated with the basic spin representations of $2A_n$ and $2S_n$', *Bull London Math. Soc.* 21 (1989) 257–262.
7. R. GOW, 'Even unimodular lattices associated with the Weil representation of the finite symplectic group', *J. Algebra* 122 (1989) 510–519.
8. B. H. GROSS, 'Group representations and lattices', *J. Amer. Math. Soc* 3 (1990) 929–960.
9. A. GROTHENDIECK, 'Standard conjectures on algebraic cycles', *Algebraic geometry*, Bombay 1968 (Oxford University Press, 1969) 193–199.
10. B. HAASTERT and J. C. JANTZEN, 'Filtrations of the discrete series of $SL_2(q)$ via crystalline cohomology', *J. Algebra* 132 (1990) 77–103.
11. R. HOTTA and K. MATSUI, 'On a lemma of Tate–Thompson', *Hiroshima Math. J.* 8 (1978) 255–268.
12. L. ILLUSIE, 'Report on crystalline cohomology', *Proc. Sympos. Pure Math.* 29 (1975) 459–478.
13. T. KATSURA and T. SHIODA, 'On Fermat varieties', *Tôhoku Math. J.* 31 (1979) 97–115.
14. N. KATZ, 'On the intersection matrix of a hypersurface', *Ann. Sci. École Norm. Sup* (4) t.2 (1969) 583–598.
15. V. LANDAZURI AND J. SEITZ, 'On the minimal degrees of projective representations of finite Chevalley groups', *J. Algebra* 32 (1974) 418–443.
16. B. MAZUR, 'Frobenius and the Hodge filtration', *Bull. Amer. Math. Soc.* 78 (1972) 653–667.
17. B. MAZUR, 'Frobenius and the Hodge filtration (estimates)', *Ann. of Math.* 98 (1973) 58–95.

18. J. S. MILNE, 'Values of zeta functions of varieties over finite fields', *Amer. J. Math.* 108 (1986) 297–360.
19. A. OGUS, 'Griffiths transversality in crystalline cohomology', *Ann. of Math.* 108 (1978) 395–419.
20. T. SHIODA, 'Mordell–Weil lattices and sphere-packings', *Amer. J. Math.* 113 (1991) 931–948.
21. J. TATE, 'Algebraic cycles and poles of zeta functions', *Arithmetical algebraic geometry*, (ed. O. F. G. Schilling; Harper and Row, New York, 1965) 93–110.
22. J. TATE, 'Endomorphisms of abelian varieties over finite fields', *Invent. Math.* 2 (1966) 134–144.
23. J. G. THOMPSON, 'Finite groups and even lattices', *J. Algebra* **38** (1976) 523–524.
24. P. H. TIEP, 'The automorphism groups of some Mordell–Weil lattices', *Izv. Akad. Nauk SSSR Ser. Mat.* 56 (1992) 509–537.
25. P. H. TIEP, 'Basic spin representations of $2S_n$ and $2A_n$ as globally irreducible representations', *Arch. Math.* 64 (1995) 103–112.
26. P. H. TIEP, 'Weil representations as globally irreducible representations', *Math. Nachr.* 184 (1997) 313–327.
27. W. C. WATERHOUSE, 'Abelian varieties over finite fields', *Ann. Sci. École Norm. Sup.* (4) t.2 (1969) 521–560.
28. A. WEIL, 'Numbers of solutions of equations in finite fields', *Bull Amer. Math. Soc.* 55 (1949) 497–508.

Department of Mathematics
University of Michigan
Ann Arbor
Michigan 48109
USA

Current address:
Department of Mathematical Sciences
Northern Illinois University
De Kalb
Illinois 60115
USA