J. reine angew. Math. **627** (2009), 183—212
DOI 10.1515/CRELLE.2009.015

Journal für die reine und angewandte Mathematik
© Walter de Gruyter
Berlin · New York 2009

Correspondences with split polynomial equations

By *E. Izadi* at Athens, *H. Lange* at Erlangen, and *V. Strehl* at Erlangen

Abstract. We introduce endomorphisms of special jacobians and show that they satisfy polynomial equations with all integer roots which we compute. The eigen-abelian varieties for these endomorphisms are generalizations of Prym-Tyurin varieties and naturally contain special curves representing cohomology classes which are not expected to be represented by curves in generic abelian varieties.

Introduction

Let A be an abelian variety of dimension g and Θ a divisor on A representing a principal polarization. The minimal cohomology class for curves in A is

$$\frac{[\Theta]^{g-1}}{(g-1)!}.$$

By a well-known result of Matsusaka [M] the minimal class is represented by a curve C in A if and only if (A, Θ) is the polarized jacobian of C. Welters [W2] classified the abelian varieties in which twice the minimal class is represented by a curve. More generally, Prym-Tyurin varieties of index m contain curves representing m times the minimal class.

A Prym-Tyurin variety P of index m is, by definition, the image of $D - \mathrm{id}$ in the jacobian $\mathrm{J}C$ of a curve C where D is an endomorphism of $\mathrm{J}C$ satisfying the equation $(D - \mathrm{id})\big(D + (m-1)\,\mathrm{id}\big) = 0$. The image of an Abel embedding of C in $\mathrm{J}C$ by the map $(D - \mathrm{id}) : \mathrm{J}C \to P$ is a curve representing m times the minimal class in P [W2].

There are few explicit constructions of Prym-Tyurin varieties in the literature.

In this paper we consider the more general situation where the jacobian of a curve admits endomorphisms satisfying polynomials of higher degree that can be decomposed

This work was done while E. Izadi was visiting the Mathematisches Institut in Erlangen at the invitation of H. Lange and as part of the Faculty Exchange Program between the University of Georgia and the University of Erlangen. E. Izadi is greatly indebted to H. Lange for his generous hospitality and to the Universities of Georgia and Erlangen for their support.

The first author was partially supported by a grant from the National Security Agency.

into products of linear factors with integer coefficients which we compute. So our endomorphisms have integer eigen-values and, after isogeny, the jacobians of our curves split into the product of the eigen-abelian varieties of the endomorphism. The images of Abel embeddings of our curves will, after isogeny (to obtain principally polarized abelian varieties), give curves representing multiples of the minimal class in the eigen-abelian varieties. In a future paper, we will compute the multiples of the minimal class that one obtains. As in the case of Prym-Tyurin varieties, these multiples will be computable from the coefficients of the polynomial equations of the endomorphisms.

The curves that we consider are immediate generalizations of constructions of Recillas, Donagi and Beauville (see e.g. [R], [D], [B]). Roughly speaking, they are defined as follows (for details see Section 1). Suppose given a ramified covering $\rho_n : X \to Y$ of degree n of smooth projective curves and an étale double cover $\tilde{X} \to X$. Then a covering $\tilde{C} \to Y$ of degree 2^n can be defined as the curve parametrizing the liftings of fibres of ρ_n to $\tilde{X}$. Moreover, the involution on $\tilde{X}$ induces an involution σ on the curve $\tilde{C}$. Assuming the ramification of ρ_n is simple, we show that the curve $\tilde{C}$ is smooth and that it has either one or two connected components. We concentrate on the case where $\tilde{C}$ consists of two smooth connected components $\tilde{C}_1$ and $\tilde{C}_2$. The computations in the case where $\tilde{C}$ is irreducible yield polynomial equations similar to those obtained for the case n odd below. We shall not address this case in this paper.

To be more precise, suppose first that $n = 2k + 1 \geqq 3$. In this case σ induces an isomorphism $\tilde{C}_1 \to \tilde{C}_2$ and we denote $C = \tilde{C}_1$. Using the involution on $\tilde{X}$ we introduce a correspondence D on C. Our first result is Theorem 2.4, which says that D satisfies an equation of degree k, integral over the integers, whose coefficients are given by explicit recursion relations. Denoting the induced endomorphism of the jacobian by the same letter, clearly any integer zero of this equation yields an eigen-abelian subvariety of D on $\mathrm{J}C$. Our main result for odd n is that all zeros of this equation are integers. In fact, we have

Theorem 1. *Suppose $n = 2k + 1$, $k \geqq 1$. The correspondence D satisfies the equation*

$$\prod_{i=0}^{k} \bigl(X + (-1)^{i+k+1}(2i+1)\bigr) = 0$$

which obviously does not have any multiple root.

Suppose now $n = 2k \geqq 2$. Then the involution σ induces an involution on each component $\tilde{C}^i$ for $i = 1$ and 2, which we denote by the same letter. Hence $\mathrm{J}\tilde{C}_i$ decomposes up to isogeny into the product of the Prym variety $P_i^\sigma := \mathrm{im}(\sigma - \mathrm{id})$ of σ and its complement $B_i^\sigma := \mathrm{im}(\sigma + \mathrm{id})$. In this case we introduce a correspondence $\tilde{D}_i$ on the curve $\tilde{C}_i$ which for $n \geqq 6$ decomposes the abelian varieties B_i^σ and P_i^σ further. Again we compute the equation for the correspondence $\tilde{D}_i$. This is a polynomial equation in $\tilde{D}_i$ and $\sigma\tilde{D}_i$. Setting $\sigma = 1$, respectively $\sigma = -1$, we obtain an equation for the endomorphism induced on B_i^σ, respectively P_i^σ, the coefficients of which are given by explicit recursion relations (see Theorems 3.6 and 3.7). Again we prove that all zeros of these equations are integers and thus lead to decompositions of the abelian varieties B_i^σ and P_i^σ for $n \geqq 6$ into eigen-abelian subvarieties.

Theorem 2. (1) *Suppose $n = 4k$ with $k \geqq 1$. For $i = 1$ and 2 the correspondence $\tilde{D}_i$ induces endomorphisms on B_i^σ and P_i^σ satisfying the equations*

- *on* B_i^σ: $$\prod_{j=0}^{k} \big(X - 8(k-j)^2 + 2k\big) = 0,$$

- *on* P_i^σ: $$\prod_{j=0}^{k-1} \big(X + 8(k-j)^2 - 10k + 8j + 2\big) = 0.$$

(2) *Suppose* $n = 4k - 2$ *with* $k \geqq 2$. *For* $i = 1$ *and* 2 *the correspondence* $\tilde{D}_i$ *induces endomorphisms on* B_i^σ *and* P_i^σ *satisfying the equations*

- *on* B_i^σ: $$\prod_{j=0}^{k-1} \big(X - 8(k-j)^2 + 10k - 8j - 3\big) = 0,$$

- *on* P_i^σ: $$\prod_{j=0}^{k-1} \big(X + 8(k-j)^2 - 18k + 16j + 9\big) = 0.$$

It is easy to see that the polynomials involved do not have multiple roots. The main idea of the proofs of Theorems 1 and 2 is to identify the fibres of the coverings $f : C \to Y$ and $f_i : \tilde{C}_i \to Y$ with sub-vector spaces of the space of bit vectors of length n. This gives an additional structure on the fibres, namely that of a Hamming scheme, as known from algebraic combinatorics and coding theory (not to be confused with a scheme in the algebro-geometric sense). Using this we associate to D and $\tilde{D}_i$ endomorphisms of vector spaces for which we can explicitly determine the eigenvalues and eigenvectors.

The contents of the paper are as follows: In Section 1 we recall the n-gonal construction. In Section 2 we introduce the correspondence D and compute its equation in the odd-degree case. Section 3 contains the analogous computations for even n. In section 4 we provide the combinatorial tools needed for the proofs of Theorems 1 and 2, which are given in Section 5. In Section 6 we give a system of equations for the dimensions of the eigen-abelian varieties involved. We use these equations to compute these dimensions explicitly for $n \leqq 10$. Finally, section 7 contains a combinatorial remark related to the situation of Theorem 1 which is worth noting.

1. The *n*-gonal construction

1.1. The set up. Let Y be a smooth curve of genus g_Y, X a cover of degree n of Y of genus g_X and $\tilde{X}$ an étale double cover of X which is *not* obtained by base change from a double cover of Y:

$$\tilde{X} \xrightarrow{\kappa} X \xrightarrow{\rho_n} Y.$$

Then Y embeds into the symmetric power $X^{(n)}$ via the map sending a point y of Y to the divisor obtained as the sum of its preimages in X. Let $\tilde{C} \subset \tilde{X}^n$ be the curve defined by the fiber product diagram

$$\begin{tikzcd} \tilde{C} \arrow[r] \arrow[d] & \tilde{X}^{(n)} \arrow[d, "\kappa^{(n)}"] \\ Y \arrow[r] & X^{(n)}. \end{tikzcd} \tag{1.1}$$

In other words, the curve $\tilde{C}$ parametrizes the liftings of points of Y to $\tilde{X}$.

Lemma 1.1. *If ρ_n is at most simply ramified, then the curve $\tilde{C}$ is smooth.*

Proof. Since $\tilde{C}$ was defined by the fiber product diagram (1.1), the tangent space to $\tilde{C}$ is the pull-back of the tangent space of Y. Away from the branch points of ρ_n, the map $\tilde{C} \to Y$ is étale and hence $\tilde{C}$ is smooth. The ramification points of $\tilde{C}$ over Y can be described as follows. Let $y \in Y$ be a branch point of ρ_n. Let $\bar{x}$ be the ramification point of ρ_n above y and let $\bar{x}_1, \dots, \bar{x}_{n-2}$ be the remaining (distinct) points of X above y. Then a point of $\tilde{C}$ above y is a ramification point if and only if it is of the form $x + x' + x_1 + \cdots + x_{n-2} \in \tilde{X}^{(n)}$ where x and x' are the two points of $\tilde{X}$ above $\bar{x}$ and x_i is a point of $\tilde{X}$ above $\bar{x}_i$ for $i = 1, \dots, n-2$. The tangent space to $\tilde{X}^{(n)}$ at $x + x' + x_1 + \cdots + x_{n-2} \in \tilde{X}^{(n)}$ can be canonically identified with

$$\mathcal{O}_x(x) \oplus \mathcal{O}_{x'}(x') \bigoplus_{i=1}^{n-2} \mathcal{O}_{x_i}(x_i)$$

and the tangent space to $X^{(n)}$ at $2\bar{x} + \bar{x}_1 + \cdots + \bar{x}_{n-2}$ can be canonically identified with

$$\mathcal{O}_{2\bar{x}}(2\bar{x}) \bigoplus_{i=1}^{n-2} \mathcal{O}_{\bar{x}_i}(\bar{x}_i).$$

The differential of $\kappa^{(n)}$ sends $\mathcal{O}_{x_i}(x_i)$ isomorphically to $\mathcal{O}_{\bar{x}_i}(\bar{x}_i)$ and sends $\mathcal{O}_x(x)$ and $\mathcal{O}_{x'}(x')$ both isomorphically to the subspace $\mathcal{O}_{\bar{x}}(\bar{x})$ of $\mathcal{O}_{2\bar{x}}(2\bar{x})$. Its kernel is therefore one-dimensional and it follows that $\tilde{C}$ is smooth at $x + x' + x_1 + \cdots + x_{n-2}$ if and only if the image of the tangent space $\mathcal{O}_y(y)$ of Y at y is not contained in the subspace

$$\mathcal{O}_{\bar{x}}(\bar{x}) \bigoplus_{i=1}^{n-2} \mathcal{O}_{\bar{x}_i}(\bar{x}_i).$$

Equivalently, if and only if the composite map

$$\mathcal{O}_y(y) \to \mathcal{O}_{2\bar{x}}(2\bar{x}) \bigoplus_{i=1}^{n-2} \mathcal{O}_{\bar{x}_i}(\bar{x}_i) \to \mathcal{O}_{\bar{x}}(2\bar{x}) \tag{1.2}$$

where the second map is the quotient by the image of the tangent space of $\tilde{X}^{(n)}$ is not zero.

Now choose a general map $Y \to \mathbb{P}^1$ of degree m with simple ramification disjoint from the branch locus of ρ_n. Let $p \in \mathbb{P}^1$ be the image of y by this map. Define $\hat{C}$ by the pull-back diagram

$$\begin{tikzcd}
\hat{C} \arrow[r] \arrow[d] & \tilde{X}^{(mn)} \arrow[d, "\kappa^{(mn)}"] \\
\mathbb{P}^1 \arrow[r] & X^{(mn)}.
\end{tikzcd}$$

By [W1], 8.13, a) p. 107, the curve $\hat{C}$ is singular exactly above the ramification of the map $Y \to \mathbb{P}^1$. In particular, it is smooth above p. Applying our analysis above to this case, this means that the composite map

$$\mathcal{O}_p(p) \to \mathcal{O}_{2\bar{x}}(2\bar{x}) \bigoplus_{i=1}^{mn-2} \mathcal{O}_{\bar{x}_i}(\bar{x}_i) \to \mathcal{O}_{\bar{x}}(2\bar{x})$$

is an isomorphism. Here $\bar{x}_i$, $i = n-2, \ldots, mn-2$ are the other points of X above p. It is now easy to see that after identifying $\mathcal{O}_p(p)$ with $\mathcal{O}_y(y)$ via the differential of $Y \to \mathbb{P}^1$, this map is equal to the map (1.2) which is therefore also an isomorphism. This shows that $\tilde{C}$ is smooth. □

Now we investigate the number of connected components of the curve $\tilde{C}$. We first have

Lemma 1.2. *If ρ_n is unramified, then the curve $\tilde{C}$ is a union of $2n$ disjoint copies of Y.*

Proof. This follows immediately from the fact that, locally, a small loop in Y will lift to n disjoint loops in X and $2n$ disjoint loops in $\tilde{X}$. □

So the case where ρ_n is unramified is uninteresting from the point of view of construction of abelian subvarieties of jacobians. *From now on we will assume that ρ_n is ramfied with simple ramification.*

Recall that the Norm map $\mathrm{Nm} : \mathrm{Pic}^n(\tilde{X}) \to \mathrm{Pic}^n(X)$ is defined as $\mathcal{O}_{\tilde{X}}(D) \mapsto \mathcal{O}_X(\kappa_* D)$ and that its kernel has two connected components that are translates of the Prym variety P of the double cover $\kappa : \tilde{X} \to X$. Therefore the fibers of the induced map

$$\mathrm{Nm}|_Y : \mathrm{Nm}^{-1}(Y) \to Y \subset X^{(n)} \to \mathrm{Pic}^n(X)$$

are disjoint unions of two translates of P. Let $\tilde{Y} \to Y$ be the étale double cover parametrizing the components of the fibers of $\mathrm{Nm}|_Y$. Then, by the definition of $\tilde{C}$, the composite map

$$\tilde{C} \hookrightarrow \tilde{X}^{(n)} \to \mathrm{Pic}^n(\tilde{X})$$

induces a map $\tilde{C} \to \tilde{Y}$ whose composition with $\tilde{Y} \to Y$ is the natural map $\tilde{C} \to Y$ from (1.1). We have

Lemma 1.3. *The curves $\tilde{C}$ and $\tilde{Y}$ have the same number of connected components.*

Proof. As in the proof of [W1], Proposition 8.8, p. 100 (also see [I], p. 109), it can be seen that any two points in a fiber of $\tilde{C} \to \tilde{Y}$ can be joined by a path in $\tilde{C}$. □

From now on we make the following assumption.

Hypothesis 1.4. The map ρ_n is simply ramified and the double cover $\tilde{Y} \to Y$ is trivial.

By the above lemmas, this is equivalent to the fact that $\tilde{C}$ is smooth with two connected components. Note that when $Y \cong \mathbb{P}^1$, the double cover $\tilde{Y} \to Y$ is always trivial.

One situation (see [D], Section 2.2) in which $\tilde{Y} \to Y$ is trivial is when $\tilde{X} \to X \to Y$ is simple of type D_n, i.e., has the following properties.

Definition 1.5. We say that the covering $\tilde{X} \xrightarrow{\kappa} X \xrightarrow{\rho_n} Y$ is a simple covering of type D_n if:

(i) $\rho_n : X \to Y$ is simply ramified of degree n with branch divisor $\mathscr{D} \neq \emptyset$ and $\kappa : \tilde{X} \to X$ an étale double covering.

(ii) $\rho_n : X \to Y$ is a primitive covering.

(iii) The monodromy map of the covering $\rho_n \circ \kappa : \tilde{X} \to Y$ can be decomposed as

$$\pi_1(Y \backslash \mathscr{D}, y_0) \to W(D_n) \hookrightarrow S_{2n}.$$

Here $y_0 \in Y \backslash \mathscr{D}$ is a base point, $\mathrm{W}(D_n)$ denotes the Weyl group of type D_n and $\mathrm{W}(D_n) \hookrightarrow S_{2n}$ the standard embedding. Recall that a covering is called primitive if it is not the composition of two coverings of degree $\geqq 2$. The simply ramified covering ρ_n is primitive if and only if the canonical map $\pi_1(X, *) \to \pi_1(Y, *)$ is surjective. According to [D], Corollary 2.4, any covering $\tilde{X} \xrightarrow{\kappa} X \xrightarrow{\rho_n} \mathbb{P}^1$ satisfying (i) and (ii) is a simple covering of type $\mathrm{W}(D_n)$.

In general the curve $\tilde{C}$ can be irreducible. For examples see [KL] and use, in particular, Remark 2.10.

The involution σ exchanging complementary liftings of the same point of Y acts on $\tilde{C}$ and we let C be the quotient of $\tilde{C}$ by this involution. This means the following. Let $\bar{z} := \bar{x}_1 + \cdots + \bar{x}_n$ be the sum of the points in a fiber of ρ_n, and, for each i, let x_i and x_i' be the two preimages of $\bar{x}_i$ in $\tilde{X}$. Then

$$z := x_1 + \cdots + x_n$$

is a point of $\tilde{C}$ and

$$\sigma(z) = x_1' + \cdots + x_n'.$$

The degrees of the maps $\tilde{C} \to Y$ and $C \to Y$ are 2^n and 2^{n-1} respectively. Since the ramification of ρ_n is simple, it is easily seen that σ is fixed-point-free if $n \geqq 3$. Also, we can see that for each ramification point $\bar{x}_1 = \bar{x}_2$ of ρ_n there are 2^{n-2} ramification points in a fiber of $\tilde{C} \to Y$ obtained as $x_1 + x_1' + D_{n-2}$ where D_{n-2} is one of the 2^{n-2} divisors on $\tilde{X}$ lifting $\bar{x}_3 + \cdots + \bar{x}_n$.

Let $\tilde{C}_1$ and $\tilde{C}_2$ be the two connected components of $\tilde{C}$. Then half of the divisors $x_1 + x_1' + D_{n-2}$ lie in $\tilde{C}_1$ and the other half lie in $\tilde{C}_2$.

Writing the degree of the ramification divisor of ρ_n as

$$\deg(R_{X/Y}) = 2g_X - 2 - n(2g_Y - 2),$$

this shows that the genus of $\tilde{C}_1$ and $\tilde{C}_2$ is

$$g_{\tilde{C}_i} = 2^{n-3}\big(g_X - 1 - (n-4)(g_Y - 1)\big) + 1.$$

If n is odd, the involution σ exchanges the two components of $\tilde{C}$, hence induces isomorphisms

$$\tilde{C}_1 \cong \tilde{C}_2 \cong C.$$

So we have the following diagram

$$\begin{tikzcd} \tilde{C}_1 \cup \tilde{C}_2 \arrow[d, "2:1"'] & \tilde{X} \arrow[d, "2:1"] \\ C = \tilde{C}_1 = \tilde{C}_2 \arrow[dr, "2^{n-1}:1"'] & X \arrow[d, "n:1"] \\ & Y. \end{tikzcd} \tag{1.3}$$

If n is even, the involution σ acts on each component of $\tilde{C}$ hence C also has two connected components, say C_1 and C_2. For $n \geqq 4$, since σ is fixed-point-free, we compute the genus of C_1 and C_2 to be

$$g_{C_i} = 2^{n-4}\big(g_X - 1 - (n-4)(g_Y - 1)\big) + 1.$$

In this case we obtain the diagram

$$\begin{tikzcd} \tilde{C}_1 \arrow[d, "2:1"'] & \tilde{X} \arrow[d, "2:1"] & \tilde{C}_2 \arrow[d, "2:1"] \\ C_1 \arrow[dr, "2^{n-2}:1"'] & X \arrow[d, "n:1"] & C_2 \arrow[dl, "2^{n-2}:1"] \\ & Y. & \end{tikzcd}$$

If $n = 2$, the degree of each component C_i over Y is 1 so

$$C_1 \cong C_2 \cong Y.$$

1.2. Notation. For each $k \in \{0, \dots, n\}$, we denote by

$$[k + (n-k)'](z)$$

the sum of all the points where k of the x_i are added to $(n-k)$ of the x_i', the indices i being all distinct. For instance

$$[1 + (n-1)'](z) = \sum_{1 \leqq i \leqq n} x_1' + \cdots + x_{i-1}' + x_i + x_{i+1}' + \cdots + x_n'.$$

and

$$[2 + (n-2)'](z) = \sum_{1 \leqq i < j \leqq n} x_1' + \cdots + x_{i-1}' + x_i + x_{i+1}' + \cdots + x_{j-1}' + x_j + x_{j+1}' + \cdots + x_n'.$$

2. The correspondence for n odd

2.1. Definition of D. For $i = 1$ or 2, we define a correspondence D_i on $\tilde{C}_i$ as the reduced curve

$$D_i := \{(x_1 + \cdots + x_n, x_1 + x_2' + \cdots + x_n')\} \subset \tilde{C}_i \times \tilde{C}_i$$

and we define

$$D \subset C \times C$$

as the image of D_i in $C \times C$. Note that the image of D_1 in $C \times C$ is equal to the image of D_2. The correspondence D defines an endomorphism of the jacobian JC whose "eigenspaces" are proper abelian subvarieties of JC. We call these the eigen-abelian varieties of D. The aim of this section is to determine the polynomial equation satisfied by this endomorphism. To study this correspondence, we work on the curve C which we consider as C_1.

For any $z = x_1 + \cdots + x_n \in C$ we define as usual

$$D(z) = p_{2_*}\big((p_1^* z) \cdot D\big)$$

as divisors on C, where p_1 and p_2 are the first and second projections. The points of C in the support of $D(z)$ are sums of x_i or x_i'. It is immediate that

$$D(z) = [1 + (n-1)'](z) \tag{2.1}$$

and

$$D^2(z) = nz + 2[2' + (n-2)](z) \tag{2.2}$$

where D^i is the composition of D with itself i times.

2.2. The general equation for n odd. Applying D to successive equations, we can find polynomial equations for D for any n odd. First we have

Proposition 2.1. (1) *For any even integer k, $0 \leqq k \leqq \dfrac{n-2}{2}$, there are integers a_j^ℓ satisfying an equation*

$$D^k(z) = a_0^k z + a_2^k D^2(z) + \cdots + a_{k-2}^k D^{k-2}(z) + k![k' + (n-k)](z). \tag{2.3}$$

(2) *For any odd integer $1 \leqq k \leqq \dfrac{n-2}{2}$, there are integers a_j^ℓ satisfying an equation*

$$D^k(z) = a_1^k D(z) + a_3^k D^3(z) + \cdots + a_{k-2}^k D^{k-2}(z) + k![k + (n-k)'](z). \tag{2.4}$$

Note that the integers a_j^ℓ are defined only for $\ell \equiv j \bmod 2$, $0 \leqq j < \ell \leqq \dfrac{n-2}{2}$.

Proof. According to equations (2.1) and (2.2) the proposition is valid for $k = 0, 1$ and 2. Applying D to (2.3), we obtain

$$D^{k+1}(z) = a_0^k D(z) + a_2^k D^3(z) + \cdots + a_{k-2}^k D^{k-1}(z) + k!(n-k+1)[(k-1) + (n-k+1)'](z) + (k+1)![(k+1) + (n-k-1)'](z).$$

Using (2.4) to substitute for $[(k-1)' + (n-k+1)](z)$, this becomes

$$\begin{aligned} D^{k+1}(z) = {} & \big(a_0^k - k(n-k+1)a_1^{k-1}\big)D(z) \\ & + \big(a_2^k - k(n-k+1)a_3^{k-1}\big)D^3(z) + \cdots \\ & + \big(a_{k-4}^k - k(n-k+1)a_{k-3}^{k-1}\big)D^{k-3}(z) \\ & + \big(a_{k-2}^k + k(n-k+1)\big)D^{k-1}(z) \\ & + (k+1)![(k+1) + (n-k-1)'](z). \end{aligned} \tag{2.5}$$

Similarly, applying D to (2.4) and using (2.3) to substitute for

$$[(k-1)' + (n-k+1)](z),$$

we obtain

$$\begin{aligned} D^{k+1}(z) = {} & -k(n-k+1)a_0^{k-1}z + \big(a_1^k - k(n-k+1)a_2^{k-1}\big)D^2(z) + \cdots \\ & + \big(a_{k-4}^k - k(n-k+1)a_{k-3}^{k-1}\big)D^{k-3}(z) \\ & + \big(a_{k-2}^k + k(n-k+1)\big)D^{k-1}(z) \\ & + (k+1)![(k+1)' + (n-k-1)](z). \end{aligned} \tag{2.6}$$

By induction this completes the proof. □

The proof of the proposition gives the following recursion relations for the integers a_j^ℓ.

Corollary 2.2. *Setting $a_\ell^\ell = -1$ for $0 \leqq \ell \leqq \frac{n-4}{2}$ and $a_1^{-1} = a_{-1}^\ell = 0$ for odd ℓ, we have for all $i \equiv k+1 \bmod 2$ and $0 \leqq i \leqq k-1$,*

$$a_i^{k+1} = a_{i-1}^k - k(n-k+1)a_i^{k-1}. \tag{2.7}$$

Using this we obtain

Proposition 2.3. *With the above notation we have*

$$a_{k-2i}^k = (-1)^{i+1} \sum_{j_1=j_0+2}^{k-2i+1} j_1(n-j_1+1) \cdot \sum_{j_2=j_1+2}^{k-2i+3} j_2(n-j_2+1) \cdot \ldots \cdot \sum_{j_{i+1}=j_i+2}^{k-1} j_{i+1}(n-j_{i+1}+1)$$

for $0 \leqq i \leqq \frac{k+1}{2}$ and $k \leqq \frac{n-2}{2}$, where we set $j_0 = -1$.

Proof. We prove the formula by induction. The formula holds trivially for $k = 0$ and 1. Assume now that it holds for all $\ell \leqq k - 1$ and all i, $0 \leqq i \leqq \frac{\ell + 1}{2}$. We need to prove it for $\ell = k$ and all i, $0 \leqq i \leqq \frac{k + 1}{2}$. From (2.7) we deduce

$$\begin{aligned} a^k_{k-2i} &= a^{k-1}_{k-2i-1} - (k-1)(n-k+2)a^{k-2}_{k-2i} \\ &= (-1)^{i+1}\sum_{j_1=1}^{k-2i} j_1(n-j_1+1)\cdot\sum_{j_2=j_1+2}^{k-2i+2} j_2(n-j_1+1)\cdot\ldots\cdot\sum_{j_{i+1}=j_i+2}^{k-2} j_{i+1}(n-j_{i+1}+1) \\ &\quad + (-1)^{i+1}(k-1)(n-k+2)\sum_{j_1=1}^{k-2i+1} j_1(n-j_1+1) \\ &\quad \cdot \sum_{j_2=j_1+2}^{k-2i+3} j_2(n-j_1+1)\cdot\ldots\cdot\sum_{j_i=j_{i-1}+2}^{k-1} j_i(n-j_i+1). \end{aligned}$$

Note that in the expression in the proposition, if we remove the last term, i.e., $(k-1)(n-k+2)$, all the upper bounds of the former sums go down by 1. This gives us the second line above. The rest will then be the third line above, which proves the proposition. □

2.3. The final equations for *n* odd. With these coefficients a^ℓ_j the following theorem gives the equation for the correspondence D.

Theorem 2.4. *Suppose $n = 2k + 1$.*

(1) *For k even D satisfies the equation*

$$X^k + (k+1)\sum_{i=0}^{k-2} a^k_i X^i - \sum_{i=1}^{k-1} a^{k+1}_i X^i = 0. \tag{2.8}$$

(2) *For k odd D satisfies the equation*

$$X^k + (k+1)\sum_{i=0}^{k-1} a^k_i X^i - \sum_{i=1}^{k} a^{k+1}_i X^i = 0. \tag{2.9}$$

Proof. (1) If $n = 2k + 1$ with k even, then

$$[(k+1) + (n-k-1)'](z) = [k' + (n-k)](z)$$

and we can use (2.3) to substitute in equation (2.5) which then becomes

$$\begin{aligned} D^{k+1}(z) &= -(k+1)a^k_0 z + \left(a^k_0 - k(k+2)a^{k-1}_1\right)D(z) + \cdots \\ &\quad - (k+1)a^k_{k-4}D^{k-4}(z) + \left(a^k_{k-4} - k(k+2)a^{k-1}_{k-3}\right)D^{k-3}(z) \\ &\quad - (k+1)a^k_{k-2}D^{k-2}(z) + \left(a^k_{k-2} + k(k+2)\right)D^{k-1}(z) + (k+1)D^k(z). \end{aligned}$$

From the recursion relations (2.7) we see that this equation is just (2.8).

(2) If $n = 2k+1$ with k odd, then $[(k+1)' + (n-k-1)](z) = [k + (n-k)'](z)$ and we can use (2.4) to substitute in equation (2.6) which then becomes (2.9), again using the recursion relations (2.7). $\square$

3. The correspondence $\tilde{D}_i$ for $n \geqq 4$ even

3.1. Definition of $\tilde{D}_i$. For $i = 1$ or 2, we define a correspondence $\tilde{D}_i$ on $\tilde{C}_i$ as the reduced curve

$$\tilde{D}_i := \{(x_1 + \cdots + x_n, x_1 + x_2 + x_3' + \cdots + x_n')\} \subset \tilde{C}_i \times \tilde{C}_i.$$

For $n \geqq 6$ the map from $\tilde{D}_i$ onto its image in $C_i \times C_i$ is of degree 2 and we define

$$D_i \subset C_i \times C_i$$

as the reduced image of $\tilde{D}_i$ in $C_i \times C_i$. For $n = 4$, the map from $\tilde{D}_i$ onto its image in $C_i \times C_i$ is of degree 4 and we define

$$D_i \subset C_i \times C_i$$

to be twice the reduced image of $\tilde{D}_i$ in $C_i \times C_i$.

The correspondences D_i and $\tilde{D}_i$ define endomorphisms of the jacobians JC_i and $J\tilde{C}_i$ whose eigen-abelian varieties are proper abelian subvarieties of JC_i and $J\tilde{C}_i$. The aim of this section is to determine the polynomial equations satisfied by these endomorphisms.

As before, for any $z = x_1 + \cdots + x_n \in \tilde{C}_i$ write

$$\tilde{D}_i(z) = p_{2_*}\big((p_1^* z) \cdot \tilde{D}_i\big)$$

as divisors on $\tilde{C}_i$, where p_1 and p_2 are the first and second projections. With the notation of Section 1.2, we have

$$\tilde{D}_i(z) = [2 + (n-2)'](z) \tag{3.1}$$

and

$$\tilde{D}_i^2(z) = \binom{n}{2} z + 2(n-2)[2' + (n-2)](z) + 6[4' + (n-4)](z),$$

which can be rewritten as

$$\tilde{D}_i^2(z) = \binom{n}{2} z + 2(n-2)\sigma\tilde{D}_i(z) + 6[4' + (n-4)](z). \tag{3.2}$$

Remark 3.1. If $n = 2$, then the correspondences $\tilde{D}_i$ are just the diagonals of $\tilde{C}_1 \times \tilde{C}_1$ and $\tilde{C}_2 \times \tilde{C}_2$. So D_1 and D_2 are the diagonals of C_1 and C_2.

3.2. Splitting of the jacobians. The involution σ splits the jacobians of $\tilde{C}_i$ into their $+1$ and -1 eigen-abelian varieties, i.e., the respective images of $\sigma+1$ and $\sigma-1$. We denote

$$P_i^\sigma := \operatorname{Im}(\sigma-1) \subset \mathrm{J}\tilde{C}_i, \quad B_i^\sigma := \operatorname{Im}(\sigma+1) \subset \mathrm{J}\tilde{C}_i.$$

Note that B_i^σ is the image of $\mathrm{J}C_i$ by the pull-back map of $\tilde{C}_i \to C_i$.

It is immediate from the definitions that the endomorphisms σ and $\tilde{D}_i$ commute on $\mathrm{J}\tilde{C}_i$. Hence $\tilde{D}_i$ induces endomorphisms on P_i^σ and B_i^σ which we denote again by $\tilde{D}_i$.

As the double cover $\tilde{C}_i \to C_i$ is étale, the map $\mathrm{J}C_i \to B_i^\sigma$ which is obtained from pull-back of line bundles from C_i to $\tilde{C}_i$ has degree 2. The endomorphism of $\mathrm{J}C_i$ obtained from D_i and that of B_i^σ obtained from $\tilde{D}_i$ fit into the commutative diagram

$$\begin{tikzcd} \mathrm{J}C_i \arrow[r, "D_i"] \arrow[d] & \mathrm{J}C_i \arrow[d] \\ B_i^\sigma \arrow[r, "\tilde{D}_i"] & B_i^\sigma. \end{tikzcd}$$

3.3. The general equation for *n* even. We proceed as in the case n odd to find the general equation for $\tilde{D}_i$, for $i=1$ or 2. In order to formulate it, we define

$$\{k\} := \prod_{i=1}^{k} \binom{2i}{2}.$$

Proposition 3.2. *For $i=1$ and 2 and any integer k, $2 \leqq k \leqq \dfrac{n-2}{4}$, there are integers b_j^k, $0 \leqq j \leqq k$ satisfying an equation*

$$\tilde{D}_i^k(z) = \sum_{j=0}^{k-1} b_j^k \sigma^{k+j} \tilde{D}_i^j(z) + \{k\}\sigma^k[(2k)' + (n-2k)](z). \tag{3.3}$$

Note that $\sigma^\ell = \mathrm{id}$ for ℓ even and $\sigma^\ell = \sigma$ for ℓ odd.

Proof. Suppose first $k=2$. Then

$$\begin{aligned} \tilde{D}_i^2(z) &= \binom{n}{2} z + 2(n-2)[2' + (n-2)](z) + 6[4' + (n-4)](z) \\ &= \binom{n}{2} z + 2(n-2)\sigma\tilde{D}_i(z) + 6[4' + (n-4)](z) \end{aligned}$$

which is of the form (3.3). For $2 \leqq k \leqq \dfrac{n-4}{4}$ we apply $\tilde{D}_i$ to (3.3) to obtain

$$\begin{aligned} \tilde{D}_i^{k+1}(z) &= b_0^k \sigma^k \tilde{D}_i(z) + b_1^k \sigma^{k+1} \tilde{D}_i^2(z) + \cdots + b_{k-1}^k \sigma^{2k-1} \tilde{D}_i^k(z) \\ &\quad + \{k\}\binom{n-2k+2}{2}\sigma^{k+1}[(2k-2)' + (n-2k+2)](z) \end{aligned} \tag{3.4}$$

$$+ \{k\} 2k(n-2k)\sigma^{k+1}[(2k)' + (n-2k)](z)$$

$$+ \{k\} \binom{2k+2}{2} \sigma^{k+1}[(2k+2)' + (n-2k-2)](z).$$

First assume $k \geqq 3$. Then, using (3.3) to substitute for $[(2k-2)' + (n-2k+2)](z)$ and $[(2k)' + (n-2k)](z)$, we can write

$$\begin{aligned}\{k\} & \binom{n-2k+2}{2} \sigma^{k+1}[(2k-2)' + (n-2k+2)](z) \\ &= \binom{2k}{2}\binom{n-2k+2}{2}\left(\tilde{D}_i^{k-1}(z) - \sum_{j=0}^{k-2} b_j^{k-1}\sigma^{k-1+j}\tilde{D}_i^j(z)\right)\end{aligned}$$

and

$$\{k\} 2k(n-2k)\sigma^{k+1}[(2k)' + (n-2k)](z) = 2k(n-2k)\left(\sigma\tilde{D}_i^k(z) - \sum_{j=0}^{k-1} b_j^k \sigma^{k+1+j}\tilde{D}_i^j(z)\right).$$

Inserting these into (3.4) we obtain

$$\begin{aligned}\tilde{D}_i^{k+1}(z) = & \left(-\binom{2k}{2}\binom{n-2k+2}{2} b_0^{k-1}\sigma^{k-1} - 2k(n-2k) b_0^k \sigma^{k+1}\right) z \\ & + \left(a_0^k \sigma^k - \binom{2k}{2}\binom{n-2k+2}{2} b_1^{k-1}\sigma^k \right. \\ & \left. - 2k(n-2k) b_1^k \sigma^{k+2}\right) \tilde{D}_i(z) + \cdots \\ & + \left(b_{k-3}^k \sigma^{2k-3} - \binom{2k}{2}\binom{n-2k+2}{2} b_{k-2}^{k-1}\sigma^{2k-3} \right. \\ & \left. - 2k(n-2k) b_{k-2}^k \sigma^{2k-1}\right) \tilde{D}_i^{k-2}(z) \\ & + \left(b_{k-2}^k \sigma^{2k-2} + \binom{2k}{2}\binom{n-2k+2}{2} \right. \\ & \left. - 2k(n-2k) b_{k-1}^k \sigma^{2k}\right) \tilde{D}_i^{k-1}(z) \\ & + \left(b_{k-1}^k \sigma^{2k-1} + 2k(n-2k)\sigma\right) \tilde{D}_i^k(z) \\ & + \{k+1\}\sigma^{k+1}[(2k+2)' + (n-2k-2)](z).\end{aligned} \tag{3.5}$$

For $k = 2$ we only need to replace $6[4 + (n-4)'](z)$ which is

$$6[4 + (n-4)'](z) = \sigma\tilde{D}_i^2 - \binom{n}{2}\sigma - 2(n-2)\tilde{D}_i$$

and we obtain the equation

$$\tilde{D}_i^3 = -4(n-4)\binom{n}{2}\sigma + \left(\binom{n}{2} + 6\binom{n-2}{2} - 4(n-4)2(n-2)\right)\tilde{D}_i$$
$$+ \big(2(n-2) + 4(n-4)\big)\sigma\tilde{D}_i^2 + 6 \cdot 15[6 + (n-6)'].$$

This proves the existence of (3.3) for all $k \leqq \dfrac{n-2}{4}$. $\square$

3.4. The recursion relations between the coefficients for *n* even. Using equations (3.2) and (3.3) we obtain the following initial values

$$b_0^2 = \binom{n}{2} \quad \text{and} \quad b_1^2 = 2(n-2).$$

Using equations (3.3) and (3.5) we obtain, for $2 \leqq k \leqq \dfrac{n-2}{4}$, the recursion relations for the integers b_j^ℓ.

Corollary 3.3. *Setting $b_{-1}^k = b_k^{k-1} = 0$ and $b_k^k = -1$ for $1 \leqq k \leqq \dfrac{n-2}{2}$, we have for all $0 \leqq j \leqq k$*

$$b_j^{k+1} = b_{j-1}^k - \binom{2k}{2}\binom{n-2k+2}{2}b_j^{k-1} - 2k(n-2k)b_j^k.$$

3.5. The final equations for *n* even. Suppose first that $n = 4k-2$, $k \geqq 2$. Then we have

$$[(2k)' + (n-2k)] = [(2k)' + (2k-2)] = \sigma[(2k-2)' + 2k] = \sigma.[(2k-2)' + (n-2k+2)].$$

So, combining (3.3) for k and $k-1$, we obtain

Proposition 3.4. *Suppose $n = 4k-2$, $k \geqq 2$. Then $\tilde{D}^i$ satisfies the following equation*

$$X^k - \sum_{j=0}^{k-1}\left(b_j^k\sigma^{k+j} - \binom{2k}{2}b_j^{k-1}\sigma^{k+j-1}\right)X^j = 0, \tag{3.6}$$

where the b_j^ℓ are the integers of Subsection 3.4.

Now suppose $n = 4k$, $k \geqq 2$. Here we apply $\tilde{D}_i$ to (3.3) for $k = n/4$ to obtain

$$\tilde{D}_i^{k+1} = \sum_{j=0}^{k-1} b_j^k\sigma^{k+j}\tilde{D}_i^{j+1} + \{k\}\sigma^k\tilde{D}_i[(2k)' + 2k]$$
$$= \sum_{j=0}^{k-1} b_j^k\sigma^{k+j}\tilde{D}_i^{j+1}$$

$$+\{k\}\sigma^k\left(\binom{2k+2}{2}([(2k+2)'+(2k-2)]\right.$$

$$\left.+[(2k-2)'+(2k+2)])+4k^2[(2k)'+2k]\right).$$

Now we use equation (3.3) for $k-1$ and its image by σ to replace

$$[(2k+2)'+(2k-2)]+[(2k-2)'+(2k+2)]$$

and equation (3.3) for k to replace $[(2k)'+2k]$ and obtain

Proposition 3.5. *Suppose $n=4k$, $k \geqq 2$. Then $\tilde{D}_i$ satisfies the following equation*:

$$X^{k+1}+\sum_{j=0}^{k}\left(\binom{2k}{2}\binom{2k+2}{2}b_j^{k-1}-b_{j-1}^k\right)\sigma^{k+j-1}X^j$$
$$+\sum_{j=0}^{k}\left(\binom{2k}{2}\binom{2k+2}{2}b_j^{k-1}+4k^2b_j^k\right)\sigma^{k+j}X^j=0 \tag{3.7}$$

where the b_j^ℓ are the integers of Subsection 3.4.

3.6. The equations in B_i^σ and P_i^σ. According to Subsection 3.2 the correspondences $\tilde{D}_i$ induce endomorphisms on the abelian subvarieties $B_i^\sigma = \mathrm{Im}(\sigma+1) \subset \mathrm{J}\tilde{C}_i$ and $P_i^\sigma = \mathrm{Im}(\sigma-1) \subset \mathrm{J}\tilde{C}_i$ which we denote by the same letter.

On B_i^σ we have $\sigma = 1$. Inserting this into Propositions 3.4 and 3.5 we finally obtain the following result.

Theorem 3.6. *On the abelian variety B_i^σ the endomorphism $\tilde{D}_i$ satisfies the following equation*:

(1) *For $n=4k-2$, $k \geqq 2$,*

$$X^k+\sum_{j=0}^{k-1}\left(b_j^k-\binom{2k}{2}b_j^{k-1}\right)X^j=0. \tag{3.8}$$

(2) *For $n=4k$, $k \geqq 2$,*

$$X^{k+1}+\sum_{j=0}^{k}\left(2\binom{2k}{2}\binom{2k+2}{2}b_j^{k-1}+4k^2b_j^k-b_{j-1}^k\right)X^j=0. \tag{3.9}$$

On P_i^σ we have $\sigma=-1$. Here we obtain

Theorem 3.7. *On the abelian variety P_i^σ the endomorphism $\tilde{D}_i$ satisfies the following equation*:

(1) *For* $n = 4k - 2$, $k \geqq 2$,

$$X^k + \sum_{j=0}^{k-1} (-1)^{k+j} \left(b_j^k + \binom{2k}{2} b_j^{k-1} \right) X^j = 0. \tag{3.10}$$

(2) *For* $n = 4k$, $k \geqq 2$,

$$X^k - \sum_{j=0}^{k-1} b_j^k X^j = 0. \tag{3.11}$$

Note that after proving Theorem 2 we can conclude that equation (3.11) means that the eigen-abelian variety of one of the roots of equation (3.7) on P_i^σ has dimension 0.

Proof. (1) is a direct consequence of Proposition 3.4. For $n = 4k$, $n \geqq 2$ we obtain an equation of degree k by noting that $[(2k)' + 2k] = \sigma[(2k)' + 2k]$. Subtracting equation (3.3) from its own image by σ and dividing by -2 we obtain the equation (3.11) on P_i^σ after replacing σ by -1. □

4. Combinatorial preliminaries

In order to find the zeros of (2.8), (2.9), (3.8), ..., (3.11) we need some combinatorial properties relating our set up to the *Hamming* scheme from algebraic graph theory (see [MS], [G] for background information). In particular, we shall use the fact that the eigenvalues of the distance–k transform are given by values of the *Krawtchouk* polynomials. For convenience, we will keep the presentation self-contained. Note that for the proofs of Theorems 1 and 2 only the cases $k = n - 1$ and $k = n - 2$ below are relevant.

4.1. The distance–*k* transform and its eigenvalues. Consider the group

$$\mathbb{B}^n = \mathbb{Z}_2^n = (\{0,1\}^n, \oplus)$$

of bitvectors of length n with componentwise addition mod 2. For $x = (x_1, \dots, x_n) \in \mathbb{B}^n$ and $y = (y_1, \dots, y_n) \in \mathbb{B}^n$ let

$$\|x\| = \sum_{1 \leqq i \leqq n} x_i \quad \text{and} \quad d(x, y) = \|x - y\|$$

denote their Hamming weight and distance. Let $\mathbb{B}_k^n$ denote the set of bitvectors of length n and weight k where $0 \leqq k \leqq n$.

For any field F (below we assume that the characteristic of F is $\neq 2$), let

$$R_n = F[\mathbb{B}^n]$$

denote the vector space over F with $\mathbb{B}^n$ as a basis. We consider the following endomorphisms of R_n:

• The *Hadamard transform* is the endomorphism of R_n defined on basis elements $x \in \mathbb{B}^n$ by

$$x \mapsto \hat{x} = \sum_{y \in \mathbb{B}^n} (-1)^{x \cdot y} y = \sum_{y \in \mathbb{B}^n} \chi_x(y) y,$$

where $x \cdot y$ is the scalar product, i.e., $\chi_x : y \mapsto (-1)^{x \cdot y}$ denotes the character of $\mathbb{B}^n$ belonging to x.

• For $0 \leqq k \leqq n$ the *distance–k transform* $\Gamma_{n,k}$ is the endomorphism of R_n defined on basis elements $x \in \mathbb{B}^n$ by

$$x \mapsto \Gamma_{n,k}(x) = \sum_{y \in \mathbb{B}^n_k} x \oplus y.$$

In other words $\Gamma_{n,k}$ associates to $x \in \mathbb{B}^n$ the sum of all basis elements at Hamming distance k from x (changing k coordinates from 0 to 1 or vice versa).

Proposition 4.1. *For $0 \leqq k \leqq n$, and for $x \in \mathbb{B}^n_\ell$ ($0 \leqq \ell \leqq n$), the Hadamard transform $\hat{x}$ is an eigenvector of $\Gamma_{n,k}$ with eigenvalue*

$$\lambda_{n,k,\ell} = \chi_x(\mathbb{B}^n_k) = \sum_i (-1)^i \binom{\ell}{i} \binom{n-\ell}{k-i}.$$

Proof. First note that all the operators $\Gamma_{n,k}$ ($0 \leqq k \leqq n$) commute, hence they have a common system of eigenvectors. Write

$$\begin{aligned}
\Gamma_{n,k}(\hat{x}) &= \sum_{y \in \mathbb{B}^n} (-1)^{x \cdot y} \Gamma_{n,k}(y) = \sum_{y \in \mathbb{B}^n} (-1)^{x \cdot y} \sum_{z \in \mathbb{B}^n_k} y \oplus z \\
&= \sum_{y \in \mathbb{B}^n} \sum_{z \in \mathbb{B}^n_k} (-1)^{x \cdot (y \oplus z)} y = \sum_{y \in \mathbb{B}^n} (-1)^{x \cdot y} \Bigg(\sum_{z \in \mathbb{B}^n_k} (-1)^{x \cdot z} \Bigg) y \\
&= \chi_x(\mathbb{B}^n_k) \cdot \hat{x},
\end{aligned}$$

where we have used $(-1)^{x \cdot (y \oplus z)} = (-1)^{x \cdot y} (-1)^{x \cdot z}$.

It is clear that the eigenvalue

$$\lambda_{n,k}(x) = \sum_{z \in \mathbb{B}^n_k} (-1)^{x \cdot z} = \chi_x(\mathbb{B}^n_k)$$

corresponding to x depends only on the weight $\|x\| = \ell$ of x, so that one can write $\lambda_{n,k,\ell}$ for it. Now for $x \in \mathbb{B}^n_\ell$:

$$\sum_{k=0}^{n} \lambda_{n,k,\ell} t^k = \sum_{z \in \mathbb{B}^n} (-1)^{x \cdot z} t^{\|z\|} = (1-t)^\ell (1+t)^{n-\ell},$$

from which the above expression for $\lambda_{n,k,\ell}$ follows by comparison of coefficients of t^k. $\square$

Remark 4.2. For $n \in \mathbb{N}$ the *Krawtchouk* polynomials $P_k(x;n)$ $(0 \leqq k \leqq n)$ are defined by

$$\sum_{0 \leqq k \leqq n} P_k(i;n) z^k = (1-z)^i (1+z)^{n-i},$$

or equivalently,

$$P_k(x;n) = \sum_{j=0}^{k} (-1)^j \binom{x}{j} \binom{n-x}{k-j},$$

so that $\lambda_{n,k,\ell} = P_k(\ell;n)$. We note the following well known and easily proved properties of these eigenvalues:

$$\lambda_{n,k,\ell} = (-1)^k \cdot \lambda_{n,k,n-\ell},$$
$$\lambda_{n,k,\ell} = (-1)^\ell \cdot \lambda_{n,n-k,\ell},$$
$$\binom{n}{\ell} \cdot \lambda_{n,k,\ell} = \binom{n}{k} \cdot \lambda_{n,\ell,k}.$$

4.2. $\mathscr{S}_n$-symmetry. Since the Hadamard transform and the distance–k transforms are compatible with the natural action of the symmetric group $\mathscr{S}_n$ on $\mathbb{B}_n$ and on R_n, one can take quotients and consider the vector space

$$\tilde{R}_n = R_n / \mathscr{S}_n.$$

It is convenient to take a polynomial model for this space, i.e., let

$$\mathscr{H}_n = \mathscr{H}_n(X, Y)$$

denote the vector space of homogeneous polynomials in variables X, Y of degree n. Take the monomials

$$\xi_\ell = X^\ell Y^{n-\ell}, \quad 0 \leqq \ell \leqq n,$$

as a basis, where ξ_ℓ is taken as the image of the elements of $\mathbb{B}_k^n$. Then the quotient action of the distance–k transform has the matrix representation $G_{n,k} = [g_{\ell,i}]_{0 \leqq \ell, i \leqq n}$, where

$$g_{\ell,i} = \begin{cases} \binom{\ell}{j} \binom{n-\ell}{k-j} & \text{if } i = k + \ell - 2j, \\ 0 & \text{otherwise.} \end{cases}$$

The quotient action of the distance–k transform may also be represented as a differential operator

$$\Delta_k = \frac{1}{k!} \sum_{j=0}^{k} \binom{k}{j} X^j Y^{k-j} D_X^{k-j} D_Y^j$$

on $\mathscr{H}_n$. Then the eigenvectors take the convenient form

$$v_{n,\ell} = v_{n,\ell}(X, Y) = (X - Y)^{\ell}(X + Y)^{n-\ell} \quad (0 \leqq \ell \leqq n).$$

These polynomials $v_{n,\ell}$ form a basis of $\mathscr{H}_n$ adapted to the operators Δ_k, with eigenvalues $\lambda_{n,k,\ell}$ $(0 \leqq k, \ell \leqq n)$.

Remark 4.3. In terms of the *Krawtchouk* polynomials

$$v_{n,\ell} = \sum_{k=0}^{\ell} P_k(\ell; n) X^k Y^{n-k} = \sum_{k=0}^{n} \lambda_{n,k,\ell} X^k Y^{n-k}.$$

The remarkable fact that the $\lambda_{n,k,\ell}$ appear both as coefficients of the eigenpolynomials $v_{n,\ell}$ and as their eigenvalues corresponding to Δ_k:

$$\Delta_k v_{n,\ell} = \lambda_{n,k,\ell} \cdot v_{n,\ell} \quad (0 \leqq k, \ell \leqq n),$$

can be written equivalently as

$$\sum_{\ell=0}^{n} \binom{n}{\ell} \lambda_{n,k,\ell} \lambda_{n,j,\ell} = 2^n \binom{n}{k} \delta_{k,j},$$

which is the orthogonality relation for the polynomials $P_k(x; n)$ $(0 \leqq k \leqq n)$.

4.3. More symmetry. Let $\mathscr{H}_n^+$, respectively $\mathscr{H}_n^-$, denote the subspace of symmetric, respectively antisymmetric, polynomials in $\mathscr{H}_n$, i.e.

$$\mathscr{H}_n^{\pm} = \{p \in \mathscr{H}_n \mid p(X, Y) = \pm p(Y, X)\}.$$

Then obviously $\{v_{n,2\ell} \mid 0 \leqq 2\ell \leqq n\}$ is a basis of $\mathscr{H}_n^+$, and $\{v_{n,2\ell+1} \mid 0 \leqq 2\ell + 1 \leqq n\}$ is a basis of $\mathscr{H}_n^-$. Since the operators Δ_k are symmetric with respect to X, Y, the subspaces $\mathscr{H}_n^+$ and $\mathscr{H}_n^-$ are Δ_k-invariant.

Let $\mathscr{H}_n^{\mathrm{e}}$, respectively $\mathscr{H}_n^{\mathrm{o}}$, denote the subspace of polynomials in $\mathscr{H}_n$ where the variable Y appears only with even, respectively odd, powers, i.e.

$$\mathscr{H}_n^{\mathrm{e}} = \{p \in \mathscr{H}_n \mid p(X, Y) = p(X, -Y)\}, \quad \mathscr{H}_n^{\mathrm{o}} = \{p \in \mathscr{H}_n \mid p(X, Y) = -p(X, -Y)\}.$$

Let

$$p^{\mathrm{e}}(X, Y) = \big(p(X, Y) + p(X, -Y)\big)/2 \quad \text{and} \quad p^{\mathrm{o}}(X, Y) = \big(p(X, Y) - p(X, -Y)\big)/2$$

denote the even and odd part of $p(X, Y)$. We have $v_{n,\ell}(X, -Y) = v_{n,n-\ell}(X, Y)$, hence

$$v_{n,\ell}^{\mathrm{e}} = (v_{n,\ell} + v_{n,n-\ell})/2,$$

$$v_{n,\ell}^{\mathrm{o}} = (v_{n,\ell} - v_{n,n-\ell})/2,$$

so that the 2-dimensional subspace spanned by $\{v_{n,\ell}, v_{n,n-\ell}\}$ has also $\{v^{\mathrm{e}}_{n,\ell}, v^{\mathrm{o}}_{n,\ell}\}$ as a basis. A degenerate situation occurs for n even and $\ell = n/2$, where $v_{n,n/2}$ itself is an even polynomial, hence $v^{\mathrm{e}}_{n,n/2} = v_{n,n/2}$ and $v^{\mathrm{o}}_{n,n/2} = 0$, and we only have a one-dimensional subspace.

From $\lambda_{n,k,\ell} = (-1)^k \cdot \lambda_{n,k,n-\ell}$ it follows that

$$\Delta_k v^{\mathrm{e}}_{n,\ell} = \begin{cases} \lambda_{n,k,\ell} \cdot v^{\mathrm{e}}_{n,\ell} & \text{if } k \text{ is even,} \\ \lambda_{n,k,\ell} \cdot v^{\mathrm{o}}_{n,\ell} & \text{if } k \text{ is odd,} \end{cases}$$

and similarly

$$\Delta_k v^{\mathrm{o}}_{n,\ell} = \begin{cases} \lambda_{n,k,\ell} \cdot v^{\mathrm{o}}_{n,\ell} & \text{if } k \text{ is even,} \\ \lambda_{n,k,\ell} \cdot v^{\mathrm{e}}_{n,\ell} & \text{if } k \text{ is odd.} \end{cases}$$

Hence, if k is odd, then the subspaces $\mathscr{H}^{\mathrm{e}}_n$ and $\mathscr{H}^{\mathrm{o}}_n$ are not Δ_k-invariant, they are rather Δ_k^2-invariant with

$$\Delta_k^2 v^{\mathrm{e}}_n = \lambda^2_{n,k,\ell} \cdot v^{\mathrm{e}}_n \quad \text{and} \quad \Delta_k^2 v^{\mathrm{o}}_n = \lambda^2_{n,k,\ell} \cdot v^{\mathrm{o}}_n.$$

Moreover, if k is even and n is odd, then $\{v^{\mathrm{e}}_{n,\ell} \mid 0 \leqq \ell < n/2\}$ is a basis of $\mathscr{H}^{\mathrm{e}}_n$, and $\{v^{\mathrm{o}}_{n,\ell} \mid 0 \leqq \ell < n/2\}$ is a basis of $\mathscr{H}^{\mathrm{o}}_n$.

Finally, if k and n are even, then a basis of $\mathscr{H}^{\mathrm{e}}_n$ is $\{v^{\mathrm{e}}_{n,\ell} \mid 0 \leqq \ell < n/2\} \cup \{v_{n,n/2}\}$, and a basis for $\mathscr{H}^{\mathrm{o}}_n$ is the same as for n odd. Note that in this case $v^{\mathrm{e}}_{n,2\ell} \in \mathscr{H}^+_n$ and $v^{\mathrm{e}}_{n,2\ell+1} \in \mathscr{H}^-_n$, and, similarly, $v^{\mathrm{o}}_{n,2\ell} \in \mathscr{H}^+_n$ and $v^{\mathrm{o}}_{n,2\ell+1} \in \mathscr{H}^-_n$, because n and $n-\ell$ have the same parity.

As a consequence we obtain

Proposition 4.4. (1) *If n is odd and k is even, then the actions of Δ_k on the four invariant subspaces $\mathscr{H}^+_n$, $\mathscr{H}^-_n$, $\mathscr{H}^{\mathrm{e}}_n$, $\mathscr{H}^{\mathrm{o}}_n$ of dimension $(n+1)/2$ are isomorphic, as they all afford the $\lambda_{n,k,\ell}$ with $0 \leqq \ell < n/2$ as eigenvalues.*

(2) *If n and k are both even, then the invariant subspaces $\mathscr{H}^+_n$ and $\mathscr{H}^-_n$ (of dimension $n/2$) are not only different in dimension* ($\dim \mathscr{H}^+_n = n/2+1, \dim \mathscr{H}^-_n = n/2$), *but the actions of Δ_k on these subspaces have complementary subsets of eigenvalues*: $\{\lambda_{n,k,2\ell} \mid 0 \leqq 2\ell \leqq n/2\}$ *for $\mathscr{H}^+_n$ and $\{\lambda_{n,k,2\ell+1} \mid 0 \leqq 2\ell+1 \leqq n/2\}$ for $\mathscr{H}^-_n$. All of these are double eigenvalues, except $\lambda_{n,k,n/2}$, which is simple.*

In the case of Proposition 4.4 (2) one can use $\mathscr{H}^{\mathrm{e}}_n$, $\mathscr{H}^{\mathrm{o}}_n$ to separate the eigenvalues as follows. Consider the invariant subspaces

$$\mathscr{H}^{+\mathrm{e}}_n = \mathscr{H}^+_n \cap \mathscr{H}^{\mathrm{e}}_n, \quad \mathscr{H}^{+\mathrm{o}}_n = \mathscr{H}^+_n \cap \mathscr{H}^{\mathrm{o}}_n, \quad \mathscr{H}^{-\mathrm{e}}_n = \mathscr{H}^-_n \cap \mathscr{H}^{\mathrm{e}}_n, \quad \mathscr{H}^{-\mathrm{o}}_n = \mathscr{H}^-_n \cap \mathscr{H}^{\mathrm{o}}_n.$$

Then we have the following:

- If $n \equiv 0 \bmod 4$:

	dim	eigenvalues	eigenvectors	range
$\mathscr{H}_n^{+\mathrm{e}}$	$n/4+1$	$\lambda_{n,k,2\ell}$	$v_{n,k,2\ell}^{\mathrm{e}}$	$0 \leqq \ell \leqq n/4$
$\mathscr{H}_n^{+\mathrm{o}}$	$n/4$	$\lambda_{n,k,2\ell}$	$v_{n,k,2\ell}^{\mathrm{o}}$	$0 \leqq \ell < n/4$
$\mathscr{H}_n^{-\mathrm{e}}$	$n/4$	$\lambda_{n,k,2\ell+1}$	$v_{n,k,2\ell+1}^{\mathrm{e}}$	$0 \leqq \ell < n/4$
$\mathscr{H}_n^{-\mathrm{o}}$	$n/4$	$\lambda_{n,k,2\ell+1}$	$v_{n,k,2\ell+1}^{\mathrm{o}}$	$0 \leqq \ell < n/4$

- If $n \equiv 2 \bmod 4$:

	dim	eigenvalues	eigenvectors	range
$\mathscr{H}_n^{+\mathrm{e}}$	$(n+2)/4$	$\lambda_{n,k,2\ell}$	$v_{n,k,2\ell}^{\mathrm{e}}$	$0 \leqq \ell < n/4$
$\mathscr{H}_n^{+\mathrm{o}}$	$(n+2)/4$	$\lambda_{n,k,2\ell}$	$v_{n,k,2\ell}^{\mathrm{o}}$	$0 \leqq \ell < n/4$
$\mathscr{H}_n^{-\mathrm{e}}$	$(n+2)/4$	$\lambda_{n,k,2\ell+1}$	$v_{n,k,2\ell+1}^{\mathrm{e}}$	$0 \leqq \ell < n/4$
$\mathscr{H}_n^{-\mathrm{o}}$	$(n-2)/4$	$\lambda_{n,k,2\ell+1}$	$v_{n,k,2\ell+1}^{\mathrm{o}}$	$0 \leqq \ell < (n-2)/4$

5. Proofs of the main theorems

5.1. Proof of Theorem 1. Let the situation be as in Theorem 1, i.e., suppose $n = 2k+1 \geqq 3$ and consider the coverings of smooth projective curves $\tilde{X} \xrightarrow{\kappa} X \xrightarrow{\rho_n} Y$ with ρ_n of degree n and κ étale of degree 2, satisfying Hypothesis 1.4. Let $f : C \to Y$ denote the associated covering of degree 2^{n-1}. For a point $y \in Y$ let $\rho_n^{-1}(y) = \{\bar{x}_1, \dots, \bar{x}_n\}$ and $\kappa^{-1}(\bar{x}_i) = \{x_i, x_i'\}$. Then

$$f^{-1}(y) = \{x_1^{\varepsilon_1} + \cdots + x_n^{\varepsilon_n} \,|\, \varepsilon = {}' \text{ or no } {}', \text{ even number of } {}'\text{s}\}. \tag{5.1}$$

Since the correspondence D is independent of the point $y \in Y$, we can identify $f^{-1}(y)$ with the set of bitvectors of length n with an even number of components different from 0:

$$f^{-1}(y) = \mathbb{B}^{n,\mathrm{e}} := \{(e_1, \dots, e_n) \,|\, e_i = 0 \text{ or } 1, \textstyle\sum e_i \text{ even}\}. \tag{5.2}$$

This gives us two additional structures on $f^{-1}(y)$, namely the addition $\oplus$ and the Hamming distance on $\mathbb{B}^{n.\mathrm{e}}$. Denote by R_n^{e} the corresponding subspace of R_n:

$$R_n^{\mathrm{e}} := F[\mathbb{B}^{n,\mathrm{e}}],$$

and define $\mathscr{H}_n^{\mathrm{e}}$ as in Section 4. Using these identifications the correspondence D on C induces the distance–$(n-1)$ transform $\Gamma_{n,n-1}$ on the vector spaces R_n^{e} as well as the differential operator Δ_{n-1} on the vector space $\mathscr{H}_n^{\mathrm{e}}$. Now, according to Theorem 2.4, the correspondence D satisfies an equation of degree k. Hence to complete the proof of Theorem 1 it suffices to show that Δ_{n-1} admits the k eigenvalues $(-1)^{k+j}(2j+1)$, $0 \leqq j \leqq k$. This follows immediately from Proposition 4.4, since the only nonzero terms of

$$\lambda_{n,n-1,\ell} = \sum_j (-1)^j \binom{\ell}{j} \binom{n-\ell}{n-1-j}$$

are those where $j = \ell - 1$ and $j = \ell$ as nonzero summands, so that

$$\begin{aligned}\lambda_{n,n-1,\ell} &= (-1)^{\ell}\left(\binom{\ell}{0}\binom{n-\ell}{1} - \binom{\ell}{1}\binom{n-\ell}{0}\right)\\ &= (-1)^{\ell}(n-2\ell)\\ &= (-1)^{k+\ell}\bigl(2(k-\ell)+1\bigr) \quad \text{for } 0 \leqq \ell \leqq n.\end{aligned}$$

Setting $i = k - l$, this finishes the proof. □

5.2. Proof of Theorem 2. Let the situation be as in Theorem 2, i.e., suppose $n = 2k \geqq 4$ and consider the coverings of smooth projective curves $\tilde{X} \xrightarrow{\kappa} X \xrightarrow{\rho_n} Y$ with ρ_n of degree n and κ étale of degree 2, satisfying Hypothesis 1.4. For $i = 1, 2$ let $f_i : \tilde{C}_i \to Y$ denote the associated covering of degree 2^{n-1}. For a point $y \in Y$ the fibre $f_i^{-1}(y)$ is given as in (5.1) and will be identified with $\mathbb{B}^{n,\mathrm{e}}$ as in (5.2). Defining R_n^{e} and $\mathscr{H}_n^{\mathrm{e}}$ as in Section 5.1 and using these identifications, the correpondence $\tilde{D}_i$ on $\tilde{C}_i$ induces the distance–$(n-2)$ transform $\Gamma_{n,n-2}$ on the vector space R_n^{e} as well as the differential operator Δ_{n-2} on the vector space $\mathscr{H}_n^{\mathrm{e}}$. Since $\sigma = 1$ on the abelian subvariety B_i^{σ} and $\sigma = -1$ on P_i^{σ}, this implies that under the assumption $\sigma = 1$ the correspondence $\tilde{D}_i|_{B_i^{\sigma}}$ induces the operator Δ_{n-2} on the subspace $\mathscr{H}_n^{+\mathrm{e}}$, and, similarly, under the assumption $\sigma = -1$ the correspondence $\tilde{D}_i|_{P_i^{\sigma}}$ induces the operator Δ_{n-2} on the subspace $\mathscr{H}_n^{-\mathrm{e}}$.

Suppose first that $n = 4k \geqq 4$. According to Theorems 3.6 and 3.7, $\tilde{D}_i|_{B_i^{\sigma}}$, respectively $\tilde{D}_i|_{P_i^{\sigma}}$, satisfies an equation of degree $k+1$, respectively k. Hence it suffices to show that Δ_{n-2} admits the $k+1$ distinct eigenvalues $8(k-\ell)^2 - 2k$, $0 \leqq l \leqq k$ on the vector space $\mathscr{H}_n^{+\mathrm{e}}$ and the k distinct eigenvalues $-8(k-\ell)^2 + 10k - 8\ell - 2$, $0 \leqq \ell \leqq k-1$ on the vector space $\mathscr{H}_n^{-\mathrm{e}}$.

According to the table at the end of Section 4, the eigenvalues of Δ_{n-2} are $\lambda_{n,n-2,2\ell}$, $0 \leqq \ell \leqq k$, on $\mathscr{H}_n^{+\mathrm{e}}$, and $\lambda_{n,n-2,2\ell+1}$, $0 \leqq \ell \leqq k-1$, on $\mathscr{H}_n^{-\mathrm{e}}$.

In the formula

$$\lambda_{n,n-2,\ell} = \sum_j (-1)^j \binom{\ell}{j}\binom{n-\ell}{n-2-j} \tag{5.3}$$

only the three terms for $j = \ell-2, \ell-1, \ell$ are nonzero. So, for $0 \leqq \ell \leqq n$, we obtain

$$\begin{aligned}\lambda_{n,n-2,\ell} &= (-1)^{\ell}\left(\binom{\ell}{2}\binom{n-\ell}{0} - \binom{\ell}{1}\binom{n-\ell}{1} + \binom{\ell}{0}\binom{n-\ell}{2}\right)\\ &= (-1)^{\ell}\left(\binom{n-2\ell}{2} - \ell\right).\end{aligned}$$

Hence

$$\lambda_{n,n-2,2\ell} = \binom{4k-4\ell}{2} - 2l = 8(k-\ell)^2 - 2k,$$

$$\lambda_{n,n-2,2\ell+1} = -\left(\binom{4k-4\ell-2}{2} - 2l - 1\right) = -8(k-\ell)^2 + 10k - 8\ell - 2$$

which completes the proof for $n = 4k$.

The proof for $n = 4k - 2$ is essentially the same. We have to compute the eigenvalues of Δ_{n-2} on $\mathscr{H}_n^{+\mathrm{e}}$ and $\mathscr{H}_n^{-\mathrm{e}}$. According to the last table in Section 4 and (5.3) they are

$$\lambda_{n,n-2,2\ell} = \binom{4k-2-4\ell}{2} - 2l = 8(k-\ell)^2 - 10k + 8l + 3,$$

$$\lambda_{n,n-2,2\ell+1} = -\left(\binom{4k-4\ell-4}{2} - 2l - 1\right) = -8(k-\ell)^2 + 18k - 16\ell - 9.$$

This completes the proof of Theorem 2. □

5.3. The correspondences associated to the distance–k transform for $k \leqq n-3$. For $k \leqq n-3$ the associated correspondences are:

- When n is odd,

$$\tilde{D}_{i,k} := \{(x_1 + \cdots + x_n, x_1' + \cdots + x_k' + x_{k+1} + \cdots + x_n)\} \subset \tilde{C}_i \times \tilde{C}_i$$

with image D_k in $C \times C$. Then the equations in Proposition 2.1 show that the eigenvalues of the associated endomorphism of $\mathrm{J}C$ can be computed from those of D and the eigen-abelian varieties are the same as those of D.

- When k and n are even,

$$\tilde{D}_{i,k} := \{(x_1 + \cdots + x_n, x_1' + \cdots + x_k' + x_{k+1} + \cdots + x_n)\} \subset \tilde{C}_i \times \tilde{C}_i$$

with reduced image D_i in $C_i \times C_i$. Then the equations in Proposition 3.2 show that the eigenvalues of the associated endomorphisms of $\mathrm{J}\tilde{C}_i$ can be computed from those of $\tilde{D}_i$ and the eigen-abelian varieties are the same as those of $\tilde{D}_i$.

Note that odd values of k will give us correspondences between $\tilde{C}_i$ and $\tilde{C}_{3-i}$.

So, using Propositions 2.1 and 3.2 and the calculations following them, we obtain yet more combinatorial identities.

6. The dimensions of the eigen-abelian varieties

Let $n \geqq 3$ be an integer. In order to have a unified statement, we consider, for odd n, the curve C as $\tilde{C}_i$ and the correspondence D as $\tilde{D}_i$ (see diagram (1.3)). We will write systems of linear equations whose solutions are the dimensions of the eigen-abelian varieties of $\tilde{D}_i$. These equations will be obtained by computing the analytic traces of the powers of $\tilde{D}_i$ in two different ways. Finally, we use these equations to compute the dimensions for $n \leqq 10$. First we see that the eigen-abelian varieties can be parametrized explicitly.

6.1. Geometric description of eigen-abelian varieties. Choose a point y of Y where ρ_n is not branched and, let $\bar{x}_1, \dots, \bar{x}_n$ be the points of $\rho_n^{-1}(y)$ and $x_1, x_1', \dots, x_n, x_n'$ their inverse images in $\tilde{X}$. Fix $i = 1$ or 2 and assume that $x_1 + \dots + x_n \in \tilde{C}_i$. As in (5.1) we identify the fiber $\mu^{-1}(y)$ when n is odd, resp. $(\mu_i \tau_i)^{-1}(y)$ when n is even, with the set $\mathbb{B}^{n,\mathrm{e}}$ of bit-vectors of length n with an even number of components different from 0. Conversely, let $t_{(e_1,\dots,e_n)} = x_1^{e_1} + \dots + x_n^{e_n}$ denote the point of C corresponding to $(e_1, \dots, e_n) \in \mathbb{B}^{n,\mathrm{e}}$ where $x_i^{e_i} = x_i$ if $e_i = 0$ and $x_i^{e_i} = x_i'$ if $e_i = 1$.

As in Section 5, the correspondence $\tilde{D}_i$ on the curve $\tilde{C}_i$ induces the distance–k transform $\Gamma_{n,k}$ on the vector space R_n^{e} where $k = n-1$ if n is odd and $k = n-2$ if n is even.

According to Proposition 4.1, for each $\ell \in \{0, \dots, n\}$ and $x \in \mathbb{B}_\ell^n$ the Hadamard transform

$$x \mapsto \hat{x} = \sum_{y \in \mathbb{B}^n} (-1)^{x \cdot y} y,$$

is an eigenvector for $\Gamma_{n,k}$ with eigenvalue

$$\lambda_{n,k,\ell} = \chi_x(\mathbb{B}_k^n) = \sum_i (-1)^i \binom{\ell}{i} \binom{n-\ell}{k-i}.$$

Under the identification of $\mathbb{B}^{n,\mathrm{e}}$ with $\mu^{-1}(y)$, resp. $(\mu_i \tau_i)^{-1}(y)$, the Hadamard transform $\hat{x}$ corresponds to the divisor

$$\sum_{y \in \mathbb{B}^n} (-1)^{x \cdot y} t_y$$

on $\tilde{C}_i$. Recall that $k = n-1$ if n is odd and $k = n-2$ if n is even. We have proved

Proposition 6.1. *The eigen-abelian subvariety of* $\mathrm{J}\tilde{C}_i$ *for the eigenvalue* $\lambda_{n,k,\ell}$ *is generated by divisors of the form* $\sum_{y \in \mathbb{B}^n} (-1)^{x \cdot y} t_y$ *where* $x \in \mathbb{B}_\ell^n$ *is fixed, after substracting a fixed divisor of the correct degree.*

The map

$$\tilde{X} \hookrightarrow \mathrm{Div}^0 \tilde{C}_i,$$

$$p \mapsto (p + \tilde{X}^{(n-1)}) \cap \tilde{C}_i - (\sigma p + \tilde{X}^{(n-1)}) \cap \tilde{C}_i$$

induces a map from the Prym variety $\mathrm{P}(\tilde{X} \to X)$ of $\tilde{X} \to X$ to $\mathrm{J}\tilde{C}$ which is easily seen to be an isogeny to its image. For n odd, let d_λ be the dimension of the eigen-abelian variety of the eigenvalue λ of $\tilde{D}_1$. For n even, let d_λ, resp. e_λ, be the dimension of the eigen-abelian variety of the eigenvalue λ of $\tilde{D}_i$ in P_i^σ, resp. B_i^σ. For the special values $\ell = 0$ and $\ell = 1$ we obtain

Corollary 6.2. (1) *For n odd the eigen-abelian subvariety of* $\mathrm{J}\tilde{C}_i$ *for the eigenvalue n is* $\mu^* \mathrm{J}Y$. *The eigen-abelian subvariety of* $\mathrm{J}\tilde{C}_i$ *for the eigenvalue* $-n+2$ *is the image of* $\mathrm{P}(\tilde{X} \to X)$. *In particular,* $d_n = g_Y$ *and* $d_{-n+2} = g_X - 1$.

(2) *If n is even the eigen-abelian subvariety of* $\mathrm{J}\tilde{C}_i$ *for the eigenvalue* $\binom{n}{2}$ *is* $(\mu_i \tau_i)^* \mathrm{J}Y$. *The eigen-abelian subvariety of* $\mathrm{J}\tilde{C}_i$ *for the eigenvalue* $-\dfrac{(n-1)(n-4)}{2}$ *is the image of* $\mathrm{P}(\tilde{X} \to X)$. *In particular,* $e_{\binom{n}{2}} = g_Y$ *and* $d_{-\frac{(n-1)(n-4)}{2}} = g_X - 1$.

6.2. The case $n = 2k+1$ odd. Recall that d_λ is the dimension of the eigen-abelian variety of the eigenvalue λ of $\tilde{D}_1$. Our first equation is

$$\sum_{j=0}^{k} d_{(-1)^{j+k}(2j+1)} = g_{\tilde{C}_1}.$$

Since we already know d_n and d_{-n+2} from Corollary 6.2, we now need $k-2$ independent linear equations.

An endomorphism D of an abelian variety A naturally acts on the tangent space $T_0 A$ of A at the origin as well as on $H^1(A, \mathbb{Q})$. We denote by $\mathrm{tr}_a(D)$ the analytic trace of D, i.e., the trace of D as an endomorphism of $T_0 A$, and by $\mathrm{tr}_r(D)$ the rational trace of D, i.e., the trace of D as an endomorphism of $H^1(A, \mathbb{Q})$. Then, for every ℓ ($\leqq k-2$), we have

$$\mathrm{tr}_a(\tilde{D}_1^\ell) = \sum_{j=0}^{k} \big((-1)^{j+k}(2j+1)\big)^\ell d_{(-1)^{j+k}(2j+1)}.$$

Now

$$\mathrm{tr}_a(\tilde{D}_1^\ell) = \frac{1}{2}\,\mathrm{tr}_r(\tilde{D}_1^\ell) = \deg(\tilde{D}_1^\ell) - \frac{1}{2}\Delta_{\tilde{C}_1} \cdot \tilde{D}_1^\ell$$

by [BL], p. 334, Proposition 11.5.2. Since $\deg(\tilde{D}_1^\ell) = \big(\deg(\tilde{D}_1)\big)^\ell = n^\ell$, it remains to compute the intersection number $\Delta_{\tilde{C}_1} \cdot \tilde{D}_1^\ell$ in order to obtain a complete system of equations. For this we use induction on ℓ and the equations of Proposition 2.1, namely

$$\text{(6.1)} \qquad \ell \ \text{ even } \quad \tilde{D}_1^\ell(z) = a_0^\ell z + a_2^\ell \tilde{D}_1^2(z) + \cdots + a_{\ell-2}^\ell \tilde{D}_1^{\ell-2}(z) + \ell![\ell' + (n-\ell)](z),$$

$$\text{(6.2)} \qquad \ell \ \text{ odd } \quad \tilde{D}_1^\ell(z) = a_1^\ell \tilde{D}_1(z) + a_3^\ell \tilde{D}_1^3(z) + \cdots + a_{\ell-2}^\ell \tilde{D}_1^{\ell-2}(z) + \ell![\ell + (n-\ell)'](z),$$

where the coefficients $a_{\ell-2m}^\ell$ are as in Proposition 2.3.

To compute the trace of $[\ell' + (n-\ell)]$, we need to count the points $z = x_1 + \cdots + x_n$ such that, after possibly renumbering the x_i, we have

$$z = x_1' + \cdots + x_\ell' + x_{\ell+1} + \cdots + x_n.$$

This happens only when $\ell = 2$ and $x_2 = x_1'$, so that $\kappa(x_1)$ is a ramification point of ρ_n. Each such ramification point gives 2^{n-3} points of $[2' + (n-2)] \cdot \Delta_{\tilde{C}_1}$. So we obtain

$$[\ell' + (n-\ell)] \cdot \Delta_{\tilde{C}_1} = 0$$

for $\ell \neq 2$ and

$$[2' + (n-2)] \cdot \Delta_{\tilde{C}_1} = 2^{n-3} \cdot \deg(R_{X/Y}) = 2^{n-3}\big(2g_X - 2 - 4(2g_Y - 2)\big).$$

6.3. The case *n* even. We will treat the case $n = 4k$, the case $n = 4k - 2$ is similar. Recall that d_λ, resp. e_λ, is the dimension of the eigen-abelian variety of the eigenvalue λ of $\tilde{D}_i$ in P_i^σ, resp. B_i^σ. Here we first have the two equations

$$\sum_{j=0}^{k-1} d_{-8(k-j)^2+10k-8j-2} = g_{C_i} - 1,$$

$$\sum_{j=0}^{k} e_{8(k-j)^2-2k} = g_{C_i}.$$

Since we already know $d_{-\frac{(n-1)(n-4)}{2}}$ and $e_{\binom{n}{2}}$ from Corollary 6.2, we now need $2k-1$ independent linear equations.

Here we compute the analytic traces of D_i and $\tilde{D}_i$ in two different ways. For every $\ell \leqq k-1$ we have

$$\operatorname{tr}_a(D_i^\ell) = \sum_{j=0}^{k} \big(8(k-j)^2 - 2k\big)^\ell e_{8(k-j)^2-2k}$$

and

$$\operatorname{tr}_a(\tilde{D}_i^\ell) = \sum_{j=0}^{k-1} \big(-8(k-1)^2 + 10k - 8j - 2\big)^\ell d_{-8(k-1)^2+10k-8j-2}$$
$$+ \sum_{j=0}^{k} \big(8(k-j)^2 - 2k\big)^\ell e_{8(k-j)^2-2k}.$$

On the other hand

$$\operatorname{tr}_a(D_i^\ell) = \frac{1}{2}\operatorname{tr}_r(D_i^\ell) = \deg(D_i^\ell) - \frac{1}{2}\Delta_{C_i} \cdot D_i^\ell$$

and

$$\operatorname{tr}_a(\tilde{D}_i^\ell) = \frac{1}{2}\operatorname{tr}_r(\tilde{D}_i^\ell) = \deg(\tilde{D}_i^\ell) - \frac{1}{2}\Delta_{\tilde{C}_i} \cdot \tilde{D}_i^\ell$$

by [BL], p. 334, Proposition 11.5.2. Since

$$\deg(D_i^\ell) = \big(\deg(D_i)\big)^\ell = \binom{n}{2}^\ell \quad \text{and} \quad \deg(\tilde{D}_i^\ell) = \big(\deg(\tilde{D}_i)\big)^\ell = \binom{n}{2}^\ell,$$

it remains to compute the intersection numbers $\Delta_{C_i} \cdot D_i^\ell$ and $\Delta_{\tilde{C}_i} \cdot \tilde{D}_i^\ell$ in order to obtain a complete system of equations. For this we use induction on ℓ and the equations of Proposition 3.2 which are in this situation

$$(6.3) \qquad \tilde{D}_i^\ell(z) = \sum_{j=0}^{\ell-1} b_j^\ell \sigma^{\ell+j} \tilde{D}_i^j(z) + \{\ell\}\sigma^\ell[2\ell' + (n-2\ell)](z).$$

On JC_i they become

$$(6.4) \qquad D_i^\ell(z) = \sum_{j=0}^{\ell-1} b_j^\ell \tilde{D}_i^j(z) + \{\ell\}[2\ell' + (n-2\ell)](z).$$

Here the coefficients b_j^ℓ are given by Corollary 3.3. The trace of $[2\ell' + (n-2\ell)]$ is the same as in the case n odd.

6.4. The case $n = 3$. For $n = 3$ the correspondence $\tilde{D}_1$ has two eigenvalues: -1 and 3. By Corollary 6.2 the eigen-abelian varieties are the images of the Prym variety of $\tilde{X} \to X$ and of JY respectively.

6.5. The case $n = 4$. For $n = 4$ the correspondence $\tilde{D}_i$ has three eigenvalues: 0 on P_i^σ, -2 and 6 on B_i^σ. By Corollary 6.2, the eigen-abelian variety for 0 is the image of the Prym $\mathrm{P}(\tilde{X} \to X)$ and the eigen-abelian variety for 6 is the image of JY. To compute e_{-2} we use the equation

$$e_{-2} + e_6 = g_{C_i} = g_X$$

from which it follows that $e_{-2} = g_X - g_Y$.

In particular, in this case the three Prym varieties P_1^σ, P_2^σ and $\mathrm{P}(\tilde{X} \to X)$ are isogeneous.

6.6. The case $n = 5$. When $n = 5$ the correspondence $\tilde{D}_1$ has the three eigenvalues $-3, 1, 5$. From Corollary 6.2 we deduce that $d_{-3} = g_X - 1$ and $d_5 = g_Y$. Now we have the equation

$$d_{-3} + d_1 + d_5 = g_{\tilde{C}_1} = 4(g_X - g_Y) + 1$$

which gives $d_1 = 3(g_X - 1) - 5(g_Y - 1)$.

6.7. The case $n = 6$. For $n = 6$ the correspondence $\tilde{D}_i$ has the eigenvalues -5, 3 on P_i^σ and the eigenvalues -1, 15 on B_i^σ. We already know that $d_{-5} = g_X - 1$ and $e_{15} = g_Y$. In addition we have the two equations

$$d_{-5} + d_3 = g_{C_i} - 1 = 4\big(g_X - 1 - 2(g_Y - 1)\big),$$
$$e_{-1} + e_{15} = g_{C_i} = 4\big(g_X - 1 - 2(g_Y - 1)\big) + 1$$

which give

$$d_3 = 3(g_X - 1) - 8(g_Y - 1), \quad e_{-1} = 4(g_X - 1) - 9(g_Y - 1).$$

6.8. The case $n = 7$. For $n = 7$ the eigenvalues of $\tilde{D}_1$ are -5, -1, 3, 7. We know $d_{-5} = g_X - 1$ and $d_7 = g_Y$. To compute d_{-1} and d_{-3} we use the equations

$$d_{-5} + d_{-1} + d_3 + d_7 = g_{\tilde{C}_1} = 16\big(g_X - 1 - 3(g_Y - 1)\big) + 1,$$
$$-5d_{-5} - d_{-1} + 3d_3 + 7d_7 = 7$$

to obtain

$$d_{-1} = 10(g_X - 1) - 35(g_Y - 1), \quad d_3 = 5(g_X - 1) - 14(g_Y - 1).$$

6.9. The case $n = 8$. For $n = 8$ the endomorphism $\tilde{D}_i$ has the eigenvalues -14, 2 on P_i^σ and -4, 4, 28 on B_i^σ. We know $d_{-14} = g_X - 1$ and $e_{28} = g_Y$. Here the additional equations are

$$\begin{aligned} d_{-16} + d_{-14} + d_2 + e_{-4} + e_4 + e_{28} &= g_{\tilde{C}_i} = 2^5\big(g_X - 1 - 4(g_Y - 1)\big) + 1, \\ e_{-4} + e_4 + e_{28} &= g_{C_i} = 2^4\big(g_X - 1 - 4(g_Y - 1)\big) + 1, \\ -16d_{-16} - 14d_{-14} + 2d_2 - 4e_{-4} + 4e_4 + 28e_{28} &= 28, \end{aligned}$$

and we obtain

$$d_2 = 15(g_X - 1) - 64(g_Y - 1), \quad e_{-4} = 10(g_X - 1) - 45(g_Y - 1),$$
$$e_4 = 6(g_X - 1) - 20(g_Y - 1).$$

6.10. The case $n = 9$. For $n = 9$ the eigenvalues of $\tilde{D}_1$ are -7, -3, 1, 5, 9. We have $d_{-7} = g_X - 1$ and $d_9 = g_Y$. We have the equations

$$\begin{aligned} d_{-7} + d_{-3} + d_1 + d_5 + d_9 &= 2^6\big((g_X - 1) - 5(g_Y - 1)\big) + 1, \\ -7d_{-7} - 3d_{-3} + d_1 + 5d_5 + 9d_9 &= 9, \\ 49d_{-7} + 9d_{-3} + d_1 + 25d_5 + 81d_9 &= 7 \cdot 2^6(g_X - 1) - 3 \cdot 9 \cdot 2^6(g_Y - 1) + 81 \end{aligned}$$

which give

$$d_{-3} = 21(g_X - 1) - 105(g_Y - 1), \quad d_1 = 35(g_X - 1) - 189(g_Y - 1),$$
$$d_5 = 7(g_X - 1) - 27(g_Y - 1).$$

6.11. The case $n = 10$. Here the eigenvalues of $\tilde{D}_i$ are -27, -3, 5 on P_i^σ, -3, 13, 45 on B_i^σ and $d_{-27} = g_X - 1$, $e_{45} = g_Y$. The equations are

$$\begin{aligned} d_{-27} + d_{-3} + d_5 + e_{-3} + e_{13} + e_{45} &= 2^7\big((g_X - 1) - 6(g_Y - 1)\big) + 1, \\ e_{-3} + e_{13} + e_{45} &= 2^6\big((g_X - 1) - 6(g_Y - 1)\big) + 1, \\ -27d_{-27} - 3d_{-3} + 5d_5 - 3e_{-3} + 13e_{13} + 45e_{45} &= 45, \\ -3e_{-3} + 13e_{13} + 45e_{45} &= 45 - 2^6\big((g_X - 1) - 10(g_Y - 1)\big) \end{aligned}$$

and we have

$$d_{-3} = 28(g_X - 1) - 160(g_Y - 1), \quad d_5 = 35(g_X - 1) - 224(g_Y - 1),$$
$$e_{-3} = 56(g_X - 1) - 350(g_Y - 1), \quad e_{13} = 8(g_X - 1) - 35(g_Y - 1).$$

7. A remark for the distance–$(n-1)$ transform for n odd

In this particular case the action of $\Gamma_{n,n-1}$ on $\mathscr{H}_n^+$ (or on any of $\mathscr{H}_n^-$ or $\mathscr{H}_n^{\mathrm{e}}$ or $\mathscr{H}_n^{\mathrm{o}}$) has the characteristic polynomial

$$C_n^+(X) = \prod_{\ell=1}^{m} \bigl(X - (-1)^{\ell+m}(2\ell - 1)\bigr),$$

where $m = (n+1)/2$. In terms of this action this means that,

$$C_n^+(X) = \det \begin{bmatrix} X & -1 & 0 & 0 & \cdots & 0 & 0 & 0 \\ -n & X & -2 & 0 & \cdots & 0 & 0 & 0 \\ 0 & -n+1 & X & -3 & \cdots & 0 & 0 & 0 \\ \vdots & \vdots & \vdots & \vdots & \ddots & \vdots & \vdots & \vdots \\ 0 & 0 & 0 & 0 & \cdots & X & -m+2 & 0 \\ 0 & 0 & 0 & 0 & \cdots & -m-2 & X & -m+1 \\ 0 & 0 & 0 & 0 & \cdots & 0 & -m-1 & X-m \end{bmatrix}.$$

Note that the eigenvectors $\{\lambda_{n,n-1,2\ell} \,|\, 0 \leqq \ell < m\}$ span the space under consideration. The fact that this determinant factors as mentioned before can be proved directly using elementary row and column operations with induction. On the other hand, there is a standard evaluation of the determinant of a tridiagonal matrix: let $a_1, a_2, \ldots$ and $b_1, b_2, \ldots$ be variables and define, for $m \geqq 0$, the $(m+1) \times (m+1)$ matrix $M^{(m)} = M^{(m)}(a_1, a_2, \ldots; b_1, b_2, \ldots)$ by

$$M^{(m)} = \begin{bmatrix} X & a_1 & 0 & 0 & \cdots & 0 & 0 & 0 \\ b_1 & X & a_2 & 0 & \cdots & 0 & 0 & 0 \\ 0 & b_2 & X & a_3 & \cdots & 0 & 0 & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \\ 0 & 0 & 0 & 0 & \cdots & X & a_{m-1} & 0 \\ 0 & 0 & 0 & 0 & \cdots & b_{m-1} & X & a_m \\ 0 & 0 & 0 & 0 & \cdots & 0 & b_m & X \end{bmatrix}.$$

Then

$$\det M^{(m+1)} = X \cdot \det M^{(m)} - a_m b_m \det M^{(m-1)},$$

which by induction gives

$$\det M^{(m)} = \sum_{0 \leqq 2j \leqq m} (-1)^j c_j^{(m)} X^{m-2j},$$

where

$$c_j^{(m)} = \sum_{1 \leqq i_1 \ll i_2 \ll \cdots \ll i_j \leqq m} a_{i_1} b_{i_1} a_{i_2} b_{i_2} \cdots a_{i_j} b_{i_j},$$

the notation $x \ll y$ meaning that $x + 1 < y$. We note in passing that this sum has a combinatorial interpretation in terms of "matchings", and the determinant evaluation as a second order recurrence points to a relation to orthogonal polynomials (see e.g. [G]).

Now

$$C_n^+(X) = (X - m) \cdot \det M^{(m-1)} - (m^2 - 1) \cdot \det M^{(m-2)},$$

where $(a_1, a_2, a_3, \ldots) = (-1, -2, -3, \ldots)$ and $(b_1, b_2, b_3, \ldots) = (-n, -n+1, -n+2, \ldots)$.

The fact that $C_n^+(X)$ factors into very simple linear factors leads to a surprisingly simple recurrence for the coefficients $c_j^{(m)}$ in this particular situation, which is not at all obvious from its definition, nor from its combinatorial interpretation.

References

[B] *A. Beauville*, Sous-variétés spéciales des variétés de Prym, Compos. Math. **45**, Fasc. 3 (1982), 357–383.

[BL] *Ch. Birkenhake*, *H. Lange*, Complex Abelian Varieties, Second edition, Grundl. Math. Wiss. **302**, Springer-Verlag, 2004.

[D] *R. Donagi*, The fibers of the Prym map, Curves, Jacobians, and Abelian Varieties (Amherst, MA, 1990), Contemp. Math. **136**, Amer. Math. Soc. (1992), 55–125.

[G] *C. D. Godsil*, Algebraic Combinatorics, Chapman & Hall, 1993.

[I] *E. Izadi*, The geometric structure of $\mathscr{A}_4$, the structure of the Prym map, double solids and Γ_{00}-divisors, J. reine angew. Math. **462** (1995), 93–158.

[KL] *V. Kanev* and *H. Lange*, Polarization types of isogenous Prym-Tyrin varieties, arXiv:0707.0364.

[MS] *F. J. MacWilliams*, *N. J. A. Sloane*, The Theory of Error-Correcting Codes, North Holland, 1977.

[M] *T. Matsusaka*, On a characterization of a jacobian variety, Mem. Coll. Sci. Univ. Kyoto **32** (1959), 1–19.

[R] *S. Recillas*, Jacobians of curves with a g_4^1 are Prym varieties of trigonal curves, Bol. Soc. Math. Mexicana **19** (1974), 9–13.

[W1] *G. E. Welters*, Abel-Jacobi isogenies for certain types of fano threefolds, Math. Centre Tracts, CWI Tracts **141** (1981), 1–139.

[W2] *G. E. Welters*, Curves of twice the minimal class on principally polarized abelian varieties, Nederl. Akad. Wetensch. Indag. Math. **49** (1987), no. 1, 87–109.

Department of Mathematics, University of Georgia, Athens, GA 30602-7403, USA
e-mail: izadi@math.uga.edu

Mathematisches Institut, Bismarckstr. 1 1/2, 91054 Erlangen, Germany
e-mail: lange@mi.uni-erlangen.de

Institut für Informatik, Martensstr. 1, 91098 Erlangen, Germany
e-mail: strehl@informatik.uni-erlangen.de

Eingegangen 25. März 2007, in revidierter Fassung 7. November 2007