hexagon:2611.01151v1

ARITHMETIC ASPECTS OF COMPLEX HADAMARD MATRICES

CLAUDE F AND TEO B

ABSTRACT. The eigenvalues of a complex Hadamard matrix having roots of unity as entries are Weil numbers. In prime order p this produces an abelian variety over $\mathbb{F}_p$, whose Frobenius map and Verschiebung are given by the matrix and by its adjoint. In order 2 we recover the abelian varieties over $\mathbb{F}_2$ having a single point. For the matrices which are equivalent to the Fourier matrix F_p we compute the Hodge polygon, we bound the Newton polygons, we study the finite order case, where exotic examples appear, and we estimate the traces of the powers, by using the Deligne bounds. We also show that the McNulty-Weigert matrices of order $2q$ are isolated precisely when a certain cross-ratio is not a square modulo q, and we discuss spin models and Ising arrays.

CONTENTS

Introduction 1
1. Hadamard matrices, Weil numbers 4
2. Abelian varieties, Frobenius maps 6
3. Order 2 and single points 7
4. Hodge and Newton polygons 9
5. Fourier matrices, Smith forms 11
6. Gauss and Kloosterman sums 13
7. Power maps, Fermat criterion 14
8. Newton strata, finite order 16
9. Polynomial maps, trace bounds 18
10. Product bases, isolation questions 20
11. Spin models and Ising arrays 24
References 26

INTRODUCTION

A complex Hadamard matrix is a square matrix $H \in M_N(\mathbb{C})$ whose entries are on the unit circle, and whose rows are pairwise orthogonal. The basic example is the Fourier matrix $F_N = (w^{ij})$, with $w = e^{2\pi i/N}$, and the theory of such matrices, which is closely related to questions in combinatorics, operator algebras and quantum physics, is usually developed up to equivalence, $H \sim M_1 H M_2$, with M_1, M_2 being monomial matrices. See [8], [19], [52].

The starting point of the present paper is the following classical formula, relating the Fourier matrix to the quadratic Gauss sum:

$$Tr(F_N) = \sum_k w^{k^2}$$

2010 *Mathematics Subject Classification.* 05B20 (11L05).
Key words and phrases. Hadamard matrix, Weil number, Gauss sum, Newton polygon, defect.

This formula is the key to Schur's computation of the sign of the Gauss sum [46], via the eigenvalue multiplicities of F_N, see for instance [3]. Now observe that the trace is not invariant under the above equivalence relation. It is invariant only under conjugation, $H \to MHM^{-1}$, with M being monomial. Thus, the right framework for the study of the trace, and more generally of the spectrum, is that of the conjugation classes of complex Hadamard matrices, with each equivalence class splitting into many such classes. Some work on the subject, mostly of combinatorial nature, was done in [14], [15], [16].

We will be interested here in the case where the entries of H are roots of unity, of a given order l. These are the Butson matrices [8], forming a set $H_N(l)$. Our first observation is that the eigenvalues of such matrices are Weil numbers, and that at $N = p$ prime, the matrix itself gives the Frobenius map of an abelian variety, in the following sense:

Theorem A. *Let $H \in H_N(l)$, and set $w = e^{2\pi i/l}$ and $K = \mathbb{Q}(w)$.*

(1) *The eigenvalues of H are Weil N-numbers, that is, algebraic integers all of whose conjugates have absolute value $\sqrt{N}$.*
(2) *When $N = p$ is prime, $l \geq 3$ and $\pm\sqrt{p}$ are not eigenvalues of H, there is an abelian variety A_H over $\mathbb{F}_p$, of dimension $p\varphi(l)/2$, whose lattice in the sense of Centeleghe-Stix is $\mathbb{Z}[w]^p$, with Frobenius map H and Verschiebung H^*, and which is unique up to isomorphism, once the functor of Centeleghe-Stix is fixed.*
(3) *The variety A_H depends only on the conjugation class of H, has multiplication by $\mathbb{Z}[w]$, and its number of points over $\mathbb{F}_{p^n}$ is the absolute value of $N_{K/\mathbb{Q}} \det(1 - H^n)$.*

Here (1) is elementary, the point being that a Galois conjugate of a Butson matrix is again a Butson matrix, and (2,3) follow from (1) and from the results of Deligne [11] and Centeleghe-Stix [9], the Verschiebung being there because of $HH^* = p$. As a first illustration, in order 2 everything can be computed, and we obtain:

Theorem B. *The matrices in $H_2(l)$ are, up to conjugation and multiplication by roots of unity, the matrices $H_z = \left(\begin{smallmatrix} 1 & z \\ 1 & -z \end{smallmatrix}\right)$, with z being a root of unity. The eigenvalues of H_z are the Weil 2-numbers λ satisfying $\lambda - 1 = z(\bar{\lambda} - 1)$, the abelian variety of H_z has exactly one point over $\mathbb{F}_2$, and we obtain in this way, up to isogeny, and as simple factors, all the simple abelian varieties over $\mathbb{F}_2$ having a single rational point, as classified by Madan-Pal and Robinson.*

In general, the main arithmetic invariants of H are its Hodge polygons, coming from the Smith normal form, which are invariant under equivalence, and its Newton polygons, coming from the valuations of the eigenvalues, which are invariant only under conjugation. The Newton polygons lie above the Hodge ones, and we have:

Theorem C. *Let p be an odd prime, and normalize the valuation of $\mathbb{Q}(e^{2\pi i/p})$ by $v(p) = 1$.*

(1) *A Butson matrix $H \in H_N(l)$ has finite order, in the sense that some power of $H/\sqrt{N}$ is the identity, precisely when its Newton polygons, at the primes dividing N, are straight lines, of slope half the valuation of N.*
(2) *The Hodge slopes of the Fourier matrix F_p are $\frac{k}{p-1}$, with $k = 0, 1, \ldots, p-1$.*
(3) *For any $H \in H_p(p)$ which is equivalent to F_p, the Newton polygon lies above the polygon with slopes $\frac{1}{p-1}, \frac{1}{p-1}, \frac{2}{p-1}, \frac{3}{p-1}, \ldots, \frac{p-3}{p-1}, \frac{p-2}{p-1}, \frac{p-2}{p-1}$.*
(4) *The matrix $G_p = (w^{ij})$, which is F_p with the columns permuted by $j \to j^{-1}$, has as eigenvalues $\pm\sqrt{p}$ and the $p-2$ nontrivial Gauss sums, and its Newton slopes are $\frac{1}{2}, \frac{1}{2}$ and $\frac{k}{p-1}$ with $k = 1, \ldots, p-2$, by the Stickelberger theorem.*

In other words, the equivalence class of F_p contains the supersingular matrix F_p itself, whose trace is the quadratic Gauss sum, then the matrix G_p, whose spectrum consists of all the Gauss sums, and whose square consists of Kloosterman sums, and then the other matrices, whose Newton polygons are bounded from below as in (3). The finite order matrices can be investigated by using (1), which provides us with an exact test, and we have:

Theorem D. *Consider the matrices of type $H = F_pPD$, with P being a permutation matrix, and with D being diagonal, with p-th roots of unity as entries, and $D_{00} = 1$.*

(1) *The Clifford matrices, where P comes from an affine map of $\mathbb{Z}_p$, and D comes from a quadratic function on $\mathbb{Z}_p$, have finite order, and at $p = 3, 5$ there are no other finite order matrices.*
(2) *At $p = 7$ there are, besides the 2058 Clifford matrices, exactly 3528 exotic matrices of finite order, having projective order 7 or 15.*
(3) *The matrix $M_d = (w^{ij^d})$, with d prime to $p-1$, has finite order precisely when -1 is a power of $-d$ modulo $p-1$, and is exotic when $d \neq 1$ modulo $p-1$.*

Here the Clifford matrices are those normalizing the Heisenberg group, and we call exotic the finite order matrices which are not Clifford. The criterion in (3) is an analogue of the Shioda-Katsura criterion for the supersingularity of the Fermat varieties [48], with the converse coming, as there, from the nonvanishing at 1 of the Dirichlet L-functions of the odd characters. Exotic matrices of this type exist precisely when $\varphi(p-1)$ is not a power of 2, or -1 is a square modulo $p-1$, which happens for 219 of the 237 primes $5 \leq p \leq 1500$, starting with $p = 11$ and $d = 3$, where $M_3^4 = p^2$. As for the exotic matrices at $p = 7$, where the power maps do not help, these are given by an explicit formula, involving a Legendre symbol.

The matrices F_pPD as above are those of the form $H = (w^{i\sigma(j)+\tau(j)})$, with σ, τ being polynomials over $\mathbb{F}_p$, the corresponding functions $x\sigma(y) + \tau(y)$ being known in coding theory as Maiorana-McFarland bent functions [29], [36]. The traces of the powers of such matrices are exponential sums, which can be estimated by using the work of Deligne [12], and we have:

Theorem E. *Let $H = (w^{i\sigma(j)+\tau(j)})$, with $\sigma, \tau \in \mathbb{F}_p[x]$ of degrees d, e, where $2 \leq d \leq p-2$ and $e \leq d$.*

(1) *We have $|Tr(H^n)| \leq d^n p^{n/2}$, for any $n \geq 1$ such that $(-d)^n \neq 1$ modulo p.*
(2) *If σ is a permutation, so that H is a complex Hadamard matrix, and if H^n is a scalar multiple of the identity, then $d^n \geq p-1$.*
(3) *If σ is a permutation, with d fixed and $p \to \infty$, the eigenvalues of $H/\sqrt{p}$ become uniformly distributed on the unit circle.*

Thus, we have a contrast between the Clifford matrices, which have finite order, and the case where σ has degree $d \geq 2$, where the order, if finite, must grow with p, and where the spectrum is equidistributed.

The arithmetic is useful as well in connection with the isolation questions, where the invariants are those of the equivalence class. A complex Hadamard matrix is called isolated when it cannot be deformed, save for the multiplication of the rows and columns by scalars, and the main examples in composite order come from a construction of McNulty and Weigert [37], whose input is a complex Hadamard matrix K of order N, and a configuration

of $2N$ points of the projective line over $\mathbb{F}_q$, labeling the usual mutually unbiased bases of $\mathbb{C}^q$. We show that the defect of such a matrix, which controls the isolation, counts the occurrences of the eigenvalue N in the spectra of q^2 twisted complex Hadamard matrices of order N^2. At $N=2$ this leads to:

Theorem F. *Let q be an odd prime, and consider the McNulty-Weigert matrix H of order $2q$ associated to the Fourier matrix F_2, and to 4 distinct points of the projective line over $\mathbb{F}_q$, having cross-ratio λ.*

(1) *When λ is not a square modulo q, the matrix H has defect 0, and so is isolated.*
(2) *When λ is a square modulo q, the matrix H has defect $2(q-1)$, and is not isolated, being part of a real analytic family of dimension $q-1$.*

Here the proof uses a theorem of Chowla [10], on the linear independence of the numbers $\cot(\pi k/q)$, which relies as well on the nonvanishing at 1 of the Dirichlet L-functions. As an illustration, the simplest matrices appearing in a conjecture from [4] are isolated when $q=2$ modulo 3, and are not isolated when $q=1$ modulo 3, so that this conjecture fails for the square matrices, at $q=7,13,19,\ldots$ For $K=F_N$ with N odd we only have computer results, suggesting that the configurations of distinct points always produce isolated matrices.

Finally, we discuss the relation with statistical mechanics. A Hadamard matrix can play 2 roles there. It can be a transfer matrix, acting on a single set of spins, and this is the point of view of the present paper, with the physics depending on the conjugation class of the matrix. Or it can be a coupling matrix, between 2 sets of spins, as in the Ising arrays from [42], with the physics depending on the equivalence class of the matrix.

On the first side, we discuss the spin models of Jones [24], where the trace is N times the modulus of the model, and where the modular invariance equation of Bannai-Bannai [5] tells us that we are in the supersingular case. On the second side, we show that the 2-rank which governs the Ising arrays of order 16 is a piece of the Hodge polygon, and that the matrices F_pPD, with D having p-th roots of unity as entries, are crystalline states of the array of $F_p\otimes F_p$, in agreement with the fact that these states correspond to the bent functions.

The paper is organized as follows: Sections 1-2 contain generalities, in Section 3 we discuss the matrices of order 2, in Sections 4-5 we study the Hodge and Newton polygons, in Sections 6-7 we discuss the Gauss sums and the power maps, in Sections 8-9 we discuss the finite order matrices and the trace bounds, in Section 10 we discuss the isolation questions, and Section 11 deals with spin models and Ising arrays. The computer programs that we used are available as supplementary material, and are mentioned in the text, at the places where they are used.

1. Hadamard matrices, Weil numbers

We use the scalar product $<x,y>=\sum_i x_i\bar{y}_i$ on $\mathbb{C}^N$, and we denote by H^* the adjoint of a matrix $H\in M_N(\mathbb{C})$. Let us start with the following standard definition:

Definition 1.1. *A complex Hadamard matrix is a square matrix $H\in M_N(\mathbb{C})$ whose entries satisfy $|H_{ij}|=1$, and whose rows are pairwise orthogonal, $HH^*=N$. The Butson class $H_N(l)$ consists of such matrices, having as entries l-th roots of unity.*

The basic example is the Fourier matrix $F_N = (w^{ij})$ with $w = e^{2\pi i/N}$, and with indices $i, j \in \{0, 1, \ldots, N-1\}$, which belongs to $H_N(N)$. More generally, any finite abelian group G produces in this way a matrix $F_G \in H_N(l)$, with $N = |G|$, and with l being the exponent of G. For many other examples, we refer to [8], [19], [52].

We recall that a square matrix is called monomial when it has exactly one nonzero entry on each row and each column. We will need 2 equivalence relations:

Definition 1.2. *Let $H, H' \in H_N(l)$.*

(1) *We say that H, H' are equivalent when $H' = M_1 H M_2$, with M_1, M_2 being monomial matrices, having roots of unity as nonzero entries.*
(2) *We say that H, H' are conjugate when $H' = MHM^{-1}$, with M being a monomial matrix, having roots of unity as nonzero entries.*

The first relation is the usual one, see [43], [52]. The second one is the one that we will be interested in, because the trace and the spectrum are invariant under conjugation, but not under equivalence. Observe that in both cases, the entries of H, H' being l-th roots of unity, the monomial matrices can be assumed, up to a scalar, to have l-th roots of unity as nonzero entries. Observe also that $M_1 H M_2$ is conjugate to HM_2M_1. Thus, the conjugation classes inside the equivalence class of H are represented by the matrices HM, with M monomial. The conjugation has the following interpretation:

Proposition 1.3. *Let $w = e^{2\pi i/l}$. The unitary matrices having entries in $\mathbb{Z}[w]$ are the monomial matrices having as nonzero entries roots of unity from $\mathbb{Z}[w]$. Thus, 2 matrices in $H_N(l)$ are conjugate precisely when they are conjugate by an automorphism of the standard hermitian lattice $\mathbb{Z}[w]^N$.*

Proof. Let U be unitary, with entries in $\mathbb{Z}[w]$, and let v be one of its columns. Since any $\sigma \in Gal(\mathbb{Q}(w)/\mathbb{Q})$ commutes with the complex conjugation, $\sigma(U)$ is unitary too, so:

$$\sum_i \sum_\sigma |\sigma(v_i)|^2 = \varphi(l)$$

On the other hand, for $v_i \neq 0$ the product of the numbers $|\sigma(v_i)|^2$ is a nonzero integer, so their sum is at least $\varphi(l)$, by the inequality of means. Thus v has exactly one nonzero entry, all of whose conjugates have absolute value 1, which is therefore a root of unity, by a classical theorem of Kronecker [28]. This gives the result. □

Let us discuss now the spectrum. We denote by $\chi_H(x) = \det(x - H)$ the characteristic polynomial of a matrix H. As a first, elementary result, we have:

Proposition 1.4. *For a complex Hadamard matrix $H \in M_N(\mathbb{C})$ we have*

$$\exp\left(\sum_{n\geq 1} Tr(H^n)\frac{t^n}{n}\right) = \frac{1}{\det(1 - tH)}$$

as well as the functional equation $\chi_H(x) = (-x/N)^N \det(H)\chi_{H^*}(N/x)$. Thus, the spectrum of H lies on the circle of radius $\sqrt{N}$, and is stable under $\lambda \to N/\bar{\lambda}$.

Proof. The first formula holds for any matrix. For the second one, we can use the equality $H(N/x - H^*) = -(N/x)(x - H)$, coming from $HH^* = N$. As for the last assertion, this is clear from the fact that $H/\sqrt{N}$ is unitary. □

In other words, the traces of the powers of H are encoded by a rational function, which looks like the zeta function of a curve over a field with N elements, and which satisfies the corresponding Riemann hypothesis. In the Butson matrix case, this analogy can be made precise. We recall that a Weil N-number is an algebraic integer, all of whose conjugates have absolute value $\sqrt{N}$. With this convention, we have:

Theorem 1.5. *Let $H \in H_N(l)$, and set $w = e^{2\pi i/l}$ and $K = \mathbb{Q}(w)$.*

(1) *The eigenvalues of H are Weil N-numbers.*
(2) *The polynomial $W_H = \prod_\sigma \sigma(\chi_H)$, with $\sigma \in Gal(K/\mathbb{Q})$, has integer coefficients, degree $N\varphi(l)$, and all its roots have absolute value $\sqrt{N}$.*
(3) *W_H is the characteristic polynomial of H, acting on the free $\mathbb{Z}$-module $\mathbb{Z}[w]^N$.*

Proof. (1) Let λ be an eigenvalue of H. Since χ_H is monic, with coefficients in $\mathbb{Z}[w]$, this is an algebraic integer. Consider now an embedding $\tau : K(\lambda) \to \mathbb{C}$, and let σ be its restriction to K. Then $\tau(\lambda)$ is an eigenvalue of the matrix $\sigma(H) = (\sigma(H_{ij}))$. But this matrix has roots of unity as entries, and since σ commutes with the complex conjugation, we have $\sigma(H)\sigma(H)^* = \sigma(HH^*) = N$. Thus $\sigma(H) \in H_N(l)$, and so $|\tau(\lambda)| = \sqrt{N}$.

(2) This is clear from (1), and from the Galois invariance of W_H.

(3) This is standard, the point being that $\mathbb{Z}[w]^N \otimes \mathbb{C}$ decomposes as a direct sum of copies of $\mathbb{C}^N$, indexed by the elements $\sigma \in Gal(K/\mathbb{Q})$, with H acting on them by $\sigma(H)$. □

2. Abelian varieties, Frobenius maps

We call W_H the Weil polynomial of $H \in H_N(l)$. The terminology comes from the fact that, when $N = q$ is a prime power, the Weil q-numbers are the eigenvalues of the Frobenius endomorphisms of the abelian varieties over $\mathbb{F}_q$, by a well-known theorem of Weil [60]. Conversely, by the Honda-Tate theorem [21], [54], [55], the simple abelian varieties over $\mathbb{F}_q$ are classified up to isogeny by the Weil q-numbers, up to conjugation. Thus, we can expect any matrix $H \in H_q(l)$ to correspond to an abelian variety.

In order to discuss this, we restrict the attention to the case where $N = p$ is prime. We recall that the Weil polynomial of an abelian variety A over $\mathbb{F}_p$ is the characteristic polynomial of its Frobenius endomorphism, which has degree $2\dim A$. We have:

Proposition 2.1. *Let $H \in H_p(l)$, with p prime and $l \geq 3$. Then W_H is the Weil polynomial of an abelian variety over $\mathbb{F}_p$, of dimension $p\varphi(l)/2$, which is unique up to isogeny.*

Proof. By the Honda-Tate theorem, and by the results of Waterhouse in [58], the Weil polynomials of the abelian varieties over the prime field $\mathbb{F}_p$ are the products of minimal polynomials of Weil p-numbers, with the polynomial $x^2 - p$, corresponding to the real Weil numbers $\pm\sqrt{p}$, appearing with even multiplicity. Thus, we must prove that the multiplicity m of $x^2 - p$ inside W_H is even. Let $K = \mathbb{Q}(e^{2\pi i/l})$.

(1) If $\sqrt{p} \notin K$ then $x^2 - p$ is irreducible over K, and if we denote by a its multiplicity inside χ_H, we have $m = a\varphi(l)$, which is even, due to $l \geq 3$.

(2) If $\sqrt{p} \in K$, let a, b be the multiplicities of $\sqrt{p}, -\sqrt{p}$ as eigenvalues of H. Half of the elements of $Gal(K/\mathbb{Q})$ fix $\sqrt{p}$, and half of them do not, so $m = (a + b)\varphi(l)/2$. But $\mathbb{Q}(\sqrt{p})$ is contained in the maximal real subfield of K, which has degree $\varphi(l)/2$, so this latter number is even. Thus m is even in this case too, and we are done. □

We would like to have a finer result, up to isomorphism, and with H itself being the Frobenius map. This is possible thanks to the following theorem, due to Deligne [11] in the ordinary case, over any finite field, and to Centeleghe-Stix [9] in the present setting:

Theorem 2.2 (Centeleghe-Stix)**.** *The category of abelian varieties over $\mathbb{F}_p$ whose Frobenius map has no real eigenvalue is anti-equivalent to the category of pairs (T, F), with T being a free $\mathbb{Z}$-module of finite rank, and with F being an endomorphism of T, such that:*

(1) *$F \otimes \mathbb{Q}$ is semisimple, and its eigenvalues are non-real Weil p-numbers.*
(2) *There exists an endomorphism V of T such that $FV = p$.*

If A corresponds to (T, F) then T has rank $2 \dim A$, and F corresponds to the Frobenius map of A.

Here the map V, which is unique, is called Verschiebung. The above anti-equivalence depends on some choices, explained in [9], and we fix one in what follows. Observe the similarity between the condition $FV = p$ and the Hadamard matrix condition $HH^* = p$. In fact, a pair F, V as above, acting on the lattice $\mathbb{Z}[w]^p$, with V being the adjoint of F, and with F having all its entries nonzero, is the same thing as a complex Hadamard matrix of order p whose entries are roots of unity in $\mathbb{Q}(w)$, which are of order l or $2l$. This latter fact follows from the inequality of means, as in the proof of Proposition 1.3. Based on these observations, we can now formulate our result, with the remark that the variety constructed below depends on the choice of l, a change $l \to l'$ with $l|l'$ replacing it by its power of exponent $\varphi(l')/\varphi(l)$:

Theorem 2.3. *Let $H \in H_p(l)$ with p prime and $l \geq 3$, such that $\pm\sqrt{p}$ are not eigenvalues of H, and set $w = e^{2\pi i/l}$ and $K = \mathbb{Q}(w)$.*

(1) *There is an abelian variety A_H over $\mathbb{F}_p$, of dimension $p\varphi(l)/2$, unique up to isomorphism, corresponding to the pair $(\mathbb{Z}[w]^p, H)$, with $V = H^*$.*
(2) *A_H depends only on the conjugation class of H, and we have $A_{\sigma(H)} \simeq A_H$ for any $\sigma \in Gal(K/\mathbb{Q})$. The endomorphism ring of A_H is anti-isomorphic to the ring of $\mathbb{Z}$-linear endomorphisms of $\mathbb{Z}[w]^p$ commuting with H, and so contains $\mathbb{Z}[w]$.*
(3) *The number of points of A_H over $\mathbb{F}_{p^n}$ is the absolute value of $N_{K/\mathbb{Q}} \det(1 - H^n)$.*

Proof. (1) We apply Theorem 2.2 to $T = \mathbb{Z}[w]^p$ and $F = H$. Since H is diagonalizable, so is $F \otimes \mathbb{C}$, which decomposes as a direct sum of matrices $\sigma(H)$. The eigenvalues are Weil p-numbers by Theorem 1.5, and are not real by our assumption, the only real Weil p-numbers being $\pm\sqrt{p}$. Finally, we can take $V = H^*$, which has entries in $\mathbb{Z}[w]$.

(2) If $H' = MHM^{-1}$, with M monomial, having entries in $\mathbb{Z}[w]$, then M is an isomorphism between the corresponding pairs. Regarding $\sigma(H)$, here the isomorphism is σ itself, acting on the coordinates, which is $\mathbb{Z}$-linear and satisfies $\sigma H = \sigma(H)\sigma$. The assertion about endomorphisms follows from the fact that we have an anti-equivalence of categories.

(3) The number of points over $\mathbb{F}_{p^n}$ is the value at 1 of the characteristic polynomial of the n-th power of the Frobenius map, and this gives the formula in the statement. □

3. Order 2 and single points

As a first illustration, let us discuss the case $N = 2$, where everything can be computed. We use the notation $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$ for the 2×2 matrices. The result that we need is:

Proposition 3.1. *Any matrix in $H_2(l)$ is conjugate to εH_z, where $H_z = \left(\begin{smallmatrix} 1 & z \\ 1 & -z \end{smallmatrix}\right)$, with ε, z being roots of unity. The characteristic polynomial of H_z is $x^2 - (1-z)x - 2z$, we have $\det(1-H_z) = -z$, and the eigenvalues of H_z are the complex numbers λ satisfying $|\lambda|^2 = 2$ and $\lambda - 1 = z(\bar{\lambda} - 1)$.*

Proof. A matrix $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$ with unimodular entries is Hadamard when $ad = -bc$. Dividing by a and then conjugating by $diag(1, c/a)$ gives the matrix H_z with $z = -d/a$. The formulae of the characteristic polynomial and of $\det(1 - H_z)$ are clear. Finally, for $|\lambda|^2 = 2$ we have $\bar{\lambda} = 2/\lambda$, so the equation $\lambda^2 - (1-z)\lambda - 2z = 0$ is equivalent to $\lambda - (1-z) - z\bar{\lambda} = 0$. □

Observe that $H_1 = F_2$, with eigenvalues $\pm\sqrt{2}$, and that H_{-1} has eigenvalues $1 \pm i$. In general, the above result shows that for an eigenvalue λ of H_z, the number $\lambda - 1$ is a unit, and that the quotient $(\lambda - 1)/(\bar{\lambda} - 1)$ is a root of unity. In order to exploit this, we recall that the real Weil polynomial of an abelian variety is the polynomial whose roots are the numbers $t = \lambda + \bar{\lambda}$, with λ ranging over half of the eigenvalues of the Frobenius map, one for each pair of conjugates. In the present setting, we have:

Proposition 3.2. *For an eigenvalue λ of H_z, the number $t = \lambda + \bar{\lambda}$ is a root of*

$$t^2 - (2 - 2c)t - (2 + 6c)$$

with $c = Re(z)$, and the number $x = 3 - t$ is a root of $x^2 - (4 + 2c)x + 1$. Also, H_z has a unit eigenvalue at the primes above 2 precisely when the order of z is not a power of 2, and when z has order 2^k with $k \geq 2$, its Newton slopes at 2 are 2^{1-k} and $1 - 2^{1-k}$.

Proof. Let λ_1, λ_2 be the eigenvalues of H_z, so that $\lambda_1 + \lambda_2 = 1 - z$ and $\lambda_1\lambda_2 = -2z$, and set $t_i = \lambda_i + 2/\lambda_i$. A direct computation gives $t_1 + t_2 = 2 - 2c$ and $t_1 t_2 = -2 - 6c$, and then the substitution $t = 3 - x$ gives the second polynomial. Regarding the last assertions, modulo a prime above 2, the characteristic polynomial becomes $x(x - (1 - z))$, and $1 - z$ is a unit there precisely when the order of z is not a power of 2. When z has order 2^k with $k \geq 2$, the number $1 - z$ has valuation $2^{1-k} \leq 1/2$, with the normalization $v(2) = 1$, and the slopes are those in the statement, by looking at the Newton polygon. □

These formulae are verified numerically by the program `ordertwo.py`. The polynomials found above are well-known, and so is the equation $\lambda^2 - (1-z)\lambda - 2z = 0$, which appears in [13]. Indeed, the abelian varieties over finite fields having a single rational point were classified in the 1970s by Madan-Pal [34] and Robinson [44], with the conclusion that, with 2 exceptions over $\mathbb{F}_3$ and $\mathbb{F}_4$, these are all defined over $\mathbb{F}_2$, and that the simple ones correspond, up to isogeny, to the irreducible factors of the following polynomials, taken at $x = 3 - t$, with $n \in \mathbb{N}$:

$$P_n(x) = \prod_{0 \leq k \leq n/2, (k,n)=1} \left(x^2 - \left(4 + 2\cos\frac{2\pi k}{n} \right) x + 1 \right)$$

To be more precise, this polynomial is irreducible, unless $n = 2, 7, 30$. We refer to [13], [34], [44] for details, and for more on these varieties. Observe also that the normalization of the matrices matters here. For instance at $l = 4$ the matrix $-H_{-1}$, which is H_{-1} multiplied by a root of unity, satisfies $\det(1 + H_{-1}) = 5$, so the corresponding abelian variety, which is of dimension 2, has 25 rational points over $\mathbb{F}_2$. Thus, the single point property is specific to the normalized matrices H_z, and is lost in general when multiplying by roots of unity. We conclude that we have:

Theorem 3.3. *Let z be a root of unity of order $n \geq 3$.*

(1) *A_{H_z} is an abelian variety over $\mathbb{F}_2$, of dimension $\varphi(n)$, having exactly one rational point, and its real Weil polynomial is $P_n(3-t)$.*
(2) *Any simple abelian variety over $\mathbb{F}_2$ having a single rational point is isogenous to a factor of a variety with Weil polynomial W_{H_z}, for a unique $n \in \mathbb{N}$, with the convention $l = 4$ at $n = 1, 2$.*
(3) *A_{H_z} is simple for $n \neq 7, 30$, with endomorphism ring $\mathbb{Z}[\lambda, \bar{\lambda}]$, and is ordinary precisely when n is not a power of 2.*

Proof. (1) The eigenvalues of H_z are not real, so Theorem 2.3 applies. The number of points is the absolute value of the norm of $\det(1 - H_z) = -z$, which is 1, and the formula of the real Weil polynomial follows from Proposition 3.2.

(2) This follows from (1) and from the above classification, with the remark that at $n = 1, 2$ the Weil polynomials of H_1, H_{-1}, regarded as elements of $H_2(4)$, are $(x^2 - 2)^2$ and $(x^2 - 2x + 2)^2$, whose real Weil polynomials are $P_1(3 - t)$ and $P_2(3 - t)$.

(3) The first assertion is clear. Regarding the endomorphisms, the lattice $\mathbb{Z}[z]^2$ is generated over $\mathbb{Z}[z]$ by the first basis vector and its image by H_z, so the pair in Theorem 2.3 is isomorphic to the ring $R = \mathbb{Z}[z][\lambda]$, with F being the multiplication by λ. Now observe that we have $\bar{\lambda} = z^{-1}(\lambda - 1 + z) \in R$, and that $z = (\lambda - 1)/(\bar{\lambda} - 1)$ belongs to $\mathbb{Z}[\lambda, \bar{\lambda}]$, because $\bar{\lambda} - 1$ is a unit. Thus $R = \mathbb{Z}[\lambda, \bar{\lambda}]$, and the endomorphisms of R commuting with λ are the multiplications by the elements of R itself. Finally, the last assertion follows from Proposition 3.2. □

4. Hodge and Newton polygons

Let us go back to the general case, $H \in H_N(l)$. With $w = e^{2\pi i/l}$, pick a prime p dividing N, and a prime ideal $\mathfrak{p}$ of $\mathbb{Z}[w]$ above p. We denote by v the corresponding valuation, normalized by $v(p) = 1$, and extended to the algebraic closure. The localization of $\mathbb{Z}[w]$ at $\mathfrak{p}$ being a discrete valuation ring, with uniformizer denoted ρ, we can write, with A, B being invertible matrices over this ring, and with $a_1 \leq \ldots \leq a_N$ being integers:

$$H = A \begin{pmatrix} \rho^{a_1} & & \\ & \ddots & \\ & & \rho^{a_N} \end{pmatrix} B$$

This is the Smith normal form of H. We have then the following notions:

Definition 4.1. *Let $H \in H_N(l)$, and $\mathfrak{p}$ be as above.*

(1) *The Hodge slopes of H are the numbers $a_i v(\rho)$, with $i = 1, \ldots, N$.*
(2) *The Newton slopes of H are the valuations of the eigenvalues of H.*

The Hodge and Newton polygons are the graphs of the piecewise linear functions on $[0, N]$ which vanish at 0 and have these slopes, arranged in increasing order.

The Smith normal form is a classical invariant of the real Hadamard matrices, under equivalence, see [39], [41], [56]. The terminology comes from the theory of the F-crystals, where the Newton polygon of the Frobenius map lies above the Hodge polygon, by a theorem of Mazur [35], see also [25]. Observe also that the polygons depend on the choice of the prime ideal above p, the complex conjugation relating the polygons at a prime ideal, and at its conjugate. The same holds in our setting, as follows:

Proposition 4.2. *Let $H \in H_N(l)$, and $\mathfrak{p}$ be as above.*

(1) *The Hodge polygon is invariant under equivalence, and the Newton polygon is invariant under conjugation.*
(2) *The Newton polygon lies above the Hodge polygon, with the same endpoints.*
(3) *The number of unit eigenvalues of H is at most the rank of H modulo $\mathfrak{p}$.*

Proof. (1) This is clear, the monomial matrices having l-th roots of unity as nonzero entries being invertible over the ring in question.

(2) Let us write $\chi_H(x) = \sum_k (-1)^k e_k x^{N-k}$. The Newton polygon is the lower convex hull of the points $(k, v(e_k))$. Now e_k is the sum of the principal minors of size k of H, and by the Cauchy-Binet formula, any minor of size k of H is divisible by $\rho^{a_1+\ldots+a_k}$. Thus the points $(k, v(e_k))$ lie above the Hodge polygon, which is convex, and this gives the result. At $k = N$ we have equality, both numbers being equal to $v(\det H)$.

(3) This follows from (2), because the rank of H modulo $\mathfrak{p}$ is the number of indices i satisfying $a_i = 0$, that is, the number of Hodge slopes which are equal to 0. □

Observe that when $\mathfrak{p}$ is stable under the complex conjugation, both polygons are symmetric, in the sense that the slopes are stable under $s \to v(N) - s$. This follows from Proposition 1.4 for the Newton slopes, and from $H^* = NH^{-1}$ for the Hodge ones.

In the real case, the first nontrivial piece of the Hodge polygon is a well-known invariant. We recall that a real Hadamard matrix is called dephased when its first row and column consist of 1 entries. With this convention, we have:

Proposition 4.3. *Let $H \in H_N(2)$ be dephased, and write its other entries as $H_{jk} = (-1)^{M_{jk}}$, with M being a binary matrix of size $N-1$. Then the Smith normal form of H is $1 \oplus 2S$, with S being the Smith normal form of M, and at $p = 2$ the Hodge slope 1 has multiplicity r, where r is the rank of M modulo 2. In particular, at $N = 16$ the Hodge slopes are 0 and 4, taken once, 1 and 3, taken r times each, and 2, taken $14 - 2r$ times.*

Proof. By subtracting the first row from the other rows, and then the first column from the other columns, we obtain the matrix $1 \oplus (-2M)$, and this gives the first assertion. The number of invariant factors of H having valuation 1 is then the number of odd invariant factors of M, which is r. Finally, the last assertion follows by symmetry. □

The number r is the 2-rank of H, which is known to take the values $4, 5, 6, 7, 7$ for the 5 real Hadamard matrices of order 16, see [42], [56]. For the Walsh matrix of order 2^n, the Hodge slope k has multiplicity $\binom{n}{k}$, and for the Paley matrices of order 12, 20, 24 we have $r = 10, 18, 11$, as verified by the program `arrays.py`. We will be back to this in Section 11.

As a main application of these notions, we have the following result, which provides us with an exact test for the finite order problem investigated in [15], [16]:

Theorem 4.4. *For a matrix $H \in H_N(l)$, the following are equivalent:*

(1) *$H/\sqrt{N}$ has finite order, in the unitary group.*
(2) *For any prime p dividing N, and any prime ideal above it, the Newton polygon of H is a straight line, of slope $v(N)/2$.*
(3) *For any prime p dividing N, the Newton polygon of W_H with respect to p is a straight line, of slope $v_p(N)/2$.*

Proof. The equivalence between (2) and (3) is clear, the Newton slopes of W_H being the Newton slopes of H, at the various prime ideals above p. Assume now that (1) holds. Then any eigenvalue λ satisfies $\lambda^{2n} = N^n$, for some $n \geq 1$, and so $v(\lambda) = v(N)/2$.

Conversely, assume that (2) holds, let λ be an eigenvalue of H, and set $\mu = \lambda^2/N$. This number has absolute value 1 at any archimedean place, by Theorem 1.5. It is a unit at any finite place not dividing N, because λ and $N/\lambda = \bar{\lambda}$ are both algebraic integers. Finally, it is a unit at the places dividing N, by our assumption. Thus μ is an algebraic integer, all of whose conjugates have absolute value 1, so it is a root of unity, by Kronecker's theorem [28]. Since H is diagonalizable, we obtain (1). □

Observe that when $N = p$ is prime and $l \geq 3$, the above conditions are satisfied precisely when the abelian varieties having W_H as Weil polynomial are supersingular, by definition of the supersingularity. We will say in this case that H itself is supersingular.

5. Fourier matrices, Smith forms

In this section and in the next ones we fix an odd prime p, and we study the matrices which are equivalent to the Fourier matrix $F_p = (w^{ij})$, where $w = e^{2\pi i/p}$. We recall that the ring $\mathbb{Z}[w]$ has a unique prime ideal above p, generated by $w - 1$, and that we have $v(w-1) = \frac{1}{p-1}$. The Smith normal form of F_p, which can be deduced as well from the results in [32], is as follows:

Proposition 5.1. *We have a factorization $F_p = L\Delta U$, with $\Delta = diag(1, w-1, \ldots, (w-1)^{p-1})$, and with L, U being invertible over $\mathbb{Z}$ and $\mathbb{Z}[w]$ respectively, given by*

$$L_{ik} = \binom{i}{k} \quad , \quad U_{kj} = u_j^k$$

where $u_j = 1 + w + \ldots + w^{j-1}$. Thus, the Hodge slopes of any matrix which is equivalent to F_p are the numbers $\frac{k}{p-1}$, with $k = 0, 1, \ldots, p-1$.

Proof. The formula $F_p = L\Delta U$ follows by writing $w^{ij} = (1 + (w^j - 1))^i$ and expanding, with the remark that we have $w^j - 1 = (w-1)u_j$. The matrix L is lower triangular, with 1 on the diagonal. Regarding U, this has entries in $\mathbb{Z}[w]$, and by using $F_p^2 = pC$, with C being the permutation matrix of $j \to -j$, and the fact that $p/(w-1)^{p-1}$ is a unit, we obtain that $(\det U)^2$ is a unit. Thus U is invertible, and the last assertion follows from Proposition 4.2. □

The above factorization, as well as the functional equation from Section 1, are verified numerically by the program `basics.py`. Let us study now the Newton polygons. According to the observations in Section 1, the matrices to be investigated are those of the form $H = F_pPD$, with P being a permutation matrix, and with D being diagonal. In terms of the underlying permutation σ, and of the diagonal entries d_j, these matrices are given by:

$$H_{ij} = w^{i\sigma(j)}d_j$$

When the numbers d_j are p-th roots of unity, we can write $d_j = w^{\tau(j)}$, and we obtain the matrices $(w^{f(i,j)})$ with $f(x,y) = x\sigma(y) + \tau(y)$. Such functions f are known in coding theory as Maiorana-McFarland bent functions, see [29], [36].

We first discuss the case where the numbers d_j are roots of unity whose orders are not powers of p. Here the situation is quite simple, as follows:

Proposition 5.2. *Let $H = F_pPD$, with D having as entries roots of unity d_j, and let $\mathfrak{p}$ be a prime ideal above p, in the corresponding cyclotomic ring. Then H has at most one unit eigenvalue, and has exactly one precisely when $\sum_j d_j \neq 0$ modulo $\mathfrak{p}$. This is the case, for instance, when the numbers d_j are signs, not all equal.*

Proof. We have $w = 1$ modulo $\mathfrak{p}$, so the reduction of H is the matrix whose rows are all equal to the vector (d_j). This matrix has rank 1, and its nonzero eigenvalue, if any, is the sum of the reductions of the numbers d_j. This gives the first assertion. As for the second one, with m signs equal to -1 the sum is $p - 2m = -2m$, which is nonzero for $0 < m < p$. □

At the level of examples, the program `strata.py` computes the Newton polygons of all the matrices F_pPD with $d_j \in \{\pm w^k\}$, at $p = 3, 5$. At $p = 3$, when the signs are not all equal, the Newton polygon equals the Hodge polygon, with slopes $0, \frac{1}{2}, 1$. At $p = 5$ the same happens for $5/6$ of such matrices, the remaining ones having slopes $0, \frac{1}{2}, \frac{1}{2}, \frac{1}{2}, 1$.

Let us discuss now the main case, where the numbers d_j are p-th roots of unity, so that $H \in H_p(p)$. By the above, there is no unit eigenvalue. In fact, we have:

Theorem 5.3. *Let $H = F_pPD$, with D having as entries p-th roots of unity, and write the characteristic polynomial as $\chi_H(x) = \sum_k (-1)^k e_k x^{p-k}$. We have then*

$$v(e_k) \geq \frac{1}{p-1}\left(\frac{k(k-1)}{2} + 1\right)$$

for any $1 \leq k \leq p-1$. Thus, the Newton polygon of H lies above the polygon with slopes $\frac{1}{p-1}, \frac{1}{p-1}, \frac{2}{p-1}, \frac{3}{p-1}, \ldots, \frac{p-3}{p-1}, \frac{p-2}{p-1}, \frac{p-2}{p-1}$, which is the Hodge polygon, with the slopes 0 and 1 replaced by $\frac{1}{p-1}$ and $\frac{p-2}{p-1}$.

Proof. With the notations of Proposition 5.1, H has the same characteristic polynomial as the matrix $L^{-1}HL = \Delta W$, where $W = UPDL$. We therefore have:

$$e_k = \sum_{|S|=k} (w-1)^{\Sigma(S)} \det(W_S)$$

Here the sum is over the subsets $S \subset \{0, 1, \ldots, p-1\}$ having k elements, $\Sigma(S)$ is the sum of the elements of S, and W_S is the corresponding principal submatrix. We have $\Sigma(S) \geq \frac{k(k-1)}{2} + 1$, unless $S = \{0, 1, \ldots, k-1\}$. Thus, it is enough to prove that the first row of W vanishes modulo $w - 1$, except for its last entry. But modulo $w - 1$ we have $D = 1$, and the first row of UP consists of 1 entries, so the entries of this first row are, with $0 \leq m \leq p-1$:

$$\sum_{j=0}^{p-1} \binom{j}{m} = \binom{p}{m+1}$$

This binomial coefficient is divisible by p for $m \leq p-2$, and we obtain the estimate in the statement. As for the last assertion, this follows from this estimate, and from the fact that the Newton polygon ends at the point $(p, \frac{p}{2})$, as the Hodge polygon does. □

6. Gauss and Kloosterman sums

We discuss now the simplest column permutation of F_p which is not affine, namely the inversion $j \to j^{-1}$ of the nonzero elements of $\mathbb{F}_p$. Consider the following matrix, with indices $i, j \in \mathbb{F}_p$, and with the convention $0^{-1} = 0$:

$$G_p = (w^{ij^{-1}})_{ij}$$

We denote by $g(\chi) = \sum_{x \neq 0} \chi(x) w^x$ the Gauss sum of a multiplicative character χ of $\mathbb{F}_p$, and by $K(a) = \sum_{x \neq 0} w^{x + a/x}$ the Kloosterman sums. With these notations, we have:

Proposition 6.1. *The eigenvalues of G_p are $\sqrt{p}, -\sqrt{p}$, and the Gauss sums $g(\chi)$ with $\chi \neq 1$. In particular, by computing the trace, we have $\sum_{\chi \neq 1} g(\chi) = 1 + (p-1)w$. Also, G_p^2 is the direct sum of the 1×1 matrix (p), and of the matrix $(1 + K(i/j))_{i,j \neq 0}$.*

Proof. Let $\chi \neq 1$, extended by $\chi(0) = 0$, and regarded as a vector in $\mathbb{C}^p$. For $i \neq 0$ the substitution $x = i/j$ gives $(G_p\chi)_i = \sum_{j \neq 0} w^{i/j} \chi(j) = g(\bar{\chi})\chi(i)$, and for $i = 0$ both sides vanish. Thus $G_p\chi = g(\bar{\chi})\chi$. On the orthogonal complement, spanned by the Dirac mass at 0 and by the indicator function of $\mathbb{F}_p^*$, the matrix of G_p is $\left(\begin{smallmatrix} 1 & p-1 \\ 1 & -1 \end{smallmatrix}\right)$, with eigenvalues $\pm\sqrt{p}$. The formula of the trace is clear, and the formula of G_p^2 follows from $(G_p^2)_{ij} = \sum_k w^{i/k + k/j}$. □

The above result, verified by the program `gauss.py`, is of course a matrix reformulation of well-known facts, the Gauss sums being the multiplicative Fourier coefficients of the additive characters, and their squares being the multiplicative Fourier coefficients of the Kloosterman sums. See [22]. The point, however, is that the matrix G_p belongs to $H_p(p)$, and is equivalent to F_p.

Observe also that the Galois conjugates of G_p are the matrices $(w^{ai/j})$, obtained from G_p by permuting the columns via $j \to a^{-1}j$, and which commute with G_p.

More generally, when the permutation σ is given by a polynomial of degree $d < p-1$, the trace of F_pP is the exponential sum $\sum_j w^{j\sigma(j)}$, which is bounded by $d\sqrt{p}$, by a well-known theorem of Weil [59]. We will come back to this in Sections 7 and 9 below, with the computation of the spectrum in the case $\sigma(j) = j^d$, and with bounds for the traces of the powers, in general.

Getting back to G_p, let us compute its Newton polygon, and its Weil polynomial. We denote by C the smooth projective curve over $\mathbb{F}_p$ given by $y^p - y = x^{p-1}$, which has genus $(p-1)(p-2)/2$, and by P_C the Weil polynomial of its Jacobian. We have:

Theorem 6.2. *The matrix $G_p \in H_p(p)$ has the following properties:*

1. *Its Newton slopes are $\frac{1}{2}, \frac{1}{2}$, and the numbers $\frac{k}{p-1}$ with $k = 1, \ldots, p-2$. Thus, they differ from the Hodge slopes only by the fact that $0, 1$ are replaced by $\frac{1}{2}, \frac{1}{2}$.*
2. *The Weil polynomial of $-G_p$ is $(x^2 - p)^{p-1} P_C(x)$.*

In particular the corresponding abelian varieties are not supersingular for $p \geq 5$, and G_p does not have finite order for $p \geq 5$, while $G_3 = F_3$.

Proof. (1) By the Stickelberger theorem [50], see also [22], at a prime above p of the field generated by the roots of unity of order $p(p-1)$, the valuations of the Gauss sums $g(\chi)$

with $\chi \neq 1$ are the numbers $\frac{k}{p-1}$ with $k = 1, \ldots, p-2$. Together with Proposition 6.1 and Proposition 5.1, this gives the result.

(2) Let us denote by $g(\chi, \psi) = \sum_{x \neq 0} \chi(x)\psi(x)$ the Gauss sum associated to a multiplicative character χ and an additive character ψ. By Proposition 6.1 and the above observation on the Galois conjugates, the roots of W_{G_p} are $\pm\sqrt{p}$, each with multiplicity $p-1$, and the numbers $g(\chi, \psi)$ with $\chi \neq 1$, $\psi \neq 1$. On the other hand, by a classical computation going back to Weil [60], the number of points of C over $\mathbb{F}_p$ is $p + 1 + \sum_{\chi \neq 1, \psi \neq 1} g(\chi, \psi)$, and similarly over the extensions of $\mathbb{F}_p$, by the Hasse-Davenport relation. Thus, the eigenvalues of the Frobenius map of C are the numbers $-g(\chi, \psi)$, and this gives the result. □

As a comment, the eigenvalues of G_p can be made fully explicit in the p-adic world, by the Gross-Koblitz formula [18], which expresses the Gauss sum whose valuation is $\frac{k}{p-1}$ as the product between $-\rho^k$, with $\rho^{p-1} = -p$, and the value at $\frac{k}{p-1}$ of the p-adic gamma function.

7. Power maps, Fermat criterion

We have seen that the inversion $j \to j^{-1}$ produces the Gauss sums. We discuss now the other power maps. Let d be an integer which is prime to $p-1$, so that $j \to j^d$ is a permutation of $\mathbb{F}_p$, and consider the following matrix, which is equivalent to F_p:

$$M_d = (w^{ij^d})_{ij}$$

This matrix depends only on d modulo $p-1$, and we have $M_1 = F_p$ and $M_{p-2} = G_p$. In order to compute its spectrum, we fix a generator ω of the group of multiplicative characters of $\mathbb{F}_p$, and we set $\chi_m = \omega^m$ and $g_m = g(\chi_m)$, for any $m \in \mathbb{Z}_{p-1}$. As before, for $m \neq 0$ we regard χ_m as a vector in $\mathbb{C}^p$, by setting $\chi_m(0) = 0$. We have:

Proposition 7.1. *Let $u = -1/d$, with the inverse taken modulo $p-1$. We have then*

$$M_d\chi_m = g_{-um}\chi_{um}$$

for any $m \neq 0$, and on the orthogonal complement of the vectors χ_m, the eigenvalues of M_d are the numbers $\pm\sqrt{p}$.

Proof. With $d' = 1/d$ modulo $p-1$, the substitution $y = j^d$ gives $\chi_m(j) = \chi_{d'm}(y)$, and so $(M_d\chi_m)_i = \sum_{y \neq 0} w^{iy}\chi_{d'm}(y) = g_{d'm}\chi_{-d'm}(i)$, for any i. As for the last assertion, this follows as in the proof of Proposition 6.1. □

Thus, M_d permutes the lines spanned by the characters, according to the permutation $m \to um$ of the set $\mathbb{Z}_{p-1} - \{0\}$. This gives the spectrum, as follows:

Proposition 7.2. *The characteristic polynomial of M_d is given by*

$$\chi_{M_d}(x) = (x^2 - p)\prod_O (x^{|O|} - \gamma_O)$$

with the product over the orbits O of $m \to um$, and with $\gamma_O = \prod_{m \in O} g_{-m}$. When ω is the Teichmüller character at a prime above p, the Newton slopes of M_d at this prime are $\frac{1}{2}, \frac{1}{2}$, and for each orbit O, the average of the numbers $\frac{m}{p-1}$ with $m \in O$, taken $|O|$ times, where the elements of $\mathbb{Z}_{p-1} - \{0\}$ are identified with the numbers $1, \ldots, p-2$.

Proof. On the span of the vectors χ_m with $m \in O$, the matrix M_d acts as a weighted cyclic permutation, the product of the weights being γ_O, by Proposition 7.1. This gives the first assertion. The second one follows from the Stickelberger theorem [50], which tells us that the valuation of g_{-m} is $\frac{m}{p-1}$, as in Section 6. □

At $d = p-2$ we have $u = 1$, the orbits are the points, and we recover the results in Section 6. As an illustration for the other cases, we have:

Example 7.3. *At $p = 11$ and $d = 3$ we have $u = 3$, the orbits being $\{5\}$, $\{1, 3, 9, 7\}$, $\{2, 6, 8, 4\}$, and*

$$\chi_{M_3}(x) = (x^2 - p)(x - i\sqrt{p})(x^4 - p^2)^2$$

so that $M_3^4 = p^2$, and M_3 has the same characteristic polynomial as F_{11}.

Here we have used the formula $g_m g_{-m} = (-1)^m p$, and the fact that g_5 is the quadratic Gauss sum. Observe that M_3 is not conjugate to F_{11}. Indeed, the matrix $(H_{ij}H_{00}/H_{i0}H_{0j})$ is symmetric for any conjugate of F_p by a monomial matrix, while for M_d this matrix is M_d itself, which is symmetric only when $d = 1$ modulo $p-1$. Thus, we have here a pair of matrices which are equivalent, have the same spectrum, and are not conjugate.

In general, the orbits of $m \to um$ are the orbits of the cyclic group generated by $-d$, acting on $\mathbb{Z}_{p-1}$. This is reminiscent of the Fermat varieties of degree m in characteristic p, where the eigenvalues of the Frobenius map are products of Gauss sums over the orbits of the group generated by p, acting on $\mathbb{Z}_m$, and where supersingularity is equivalent to $p^\nu = -1$ modulo m, for some ν, by a well-known result of Shioda and Katsura [48]. We have:

Theorem 7.4. *Let $p \geq 5$, let d be prime to $p-1$, and let r be the order of $-d$ in the group $\mathbb{Z}_{p-1}^*$.*

1. *M_d has finite order precisely when all the orbits O are balanced, in the sense that the average of their elements, taken in $\{1, \ldots, p-2\}$, is $\frac{p-1}{2}$.*
2. *This happens precisely when $(-d)^\nu = -1$ modulo $p-1$, for some ν, and we have then $M_d^{2r} = p^r$.*
3. *A number $d \neq 1$ modulo $p-1$ as in (2) exists precisely when $\varphi(p-1)$ is not a power of 2, or when -1 is a square modulo $p-1$.*
4. *For $d \neq 1$ modulo $p-1$, the matrix M_d is not Clifford.*

Proof. (1) This follows from Theorem 4.4 and Proposition 7.2.

(2) Assume first $(-d)^\nu = -1$. Then any orbit O is stable under $m \to -m$, and r is even. If O is not the orbit of the quadratic character, its elements come in pairs $\{m, -m\}$, and by using $g_m g_{-m} = \pm p$ we obtain $\gamma_O = \pm p^{|O|/2}$. In the remaining case γ_O is the quadratic Gauss sum, whose square is $\pm p$. Thus any eigenvalue λ satisfies $\lambda^{2r} = p^r$, the lengths of the orbits dividing r, and $2r$ being a multiple of 4.

Conversely, we follow the argument of Miyawaki for the Fermat varieties, explained in [48]. Assume that all the orbits are balanced, and that -1 is not in the group $\Gamma \subset \mathbb{Z}_{p-1}^*$ generated by $-d$. Then there is a character χ of $\mathbb{Z}_{p-1}^*$ which is trivial on Γ, and satisfies $\chi(-1) = -1$. Let f be the conductor of χ, so that χ comes from a primitive character modulo f, still denoted χ, and set $k = (p-1)/f$. For a prime to f the orbit of ka consists of the numbers kb with $b \in a\Gamma_f$, where Γ_f is the image of Γ modulo f, and the balancing condition reads $\sum_{b \in a\Gamma_f} (\frac{b}{f} - \frac{1}{2}) = 0$, with b taken in $\{1, \ldots, f-1\}$. By multiplying by

$\bar{\chi}(a)$ and summing over the cosets of Γ_f we obtain $\sum_b \bar{\chi}(b)b = 0$, with the sum over the numbers $b \in \{1, \ldots, f-1\}$ which are prime to f. But this sum is $fB_{1,\bar{\chi}}$, with $B_{1,\bar{\chi}}$ being a generalized Bernoulli number, which is nonzero, because χ is odd and primitive, and $L(1,\chi) \neq 0$ is then a multiple of $B_{1,\bar{\chi}}$. See [57]. Thus, we have a contradiction.

(3) We are looking for an element $e = -d$ of the group $\mathbb{Z}_{p-1}^*$, different from -1, having -1 among its powers, $e^k = -1$ with $k \geq 2$ minimal. If this group has an element $a \neq 1$ of odd order, we can take $e = -a$. Otherwise the order of e, which is $2k$, must be a power of 2, so $-1 = (e^{k/2})^2$ is a square, and conversely, when $-1 = b^2$ we can take $e = b$. The program `existence.py` checks this criterion for $5 \leq p \leq 1500$, where such a number d exists for 219 of the 237 primes, the exceptions starting with $5, 7, 13, 17, 31, 41$, and `fermat.py` checks (2) in the same range, by testing the balancing condition in (1) for all the numbers d. The formula of the spectrum, and the finite order criterion, are also verified numerically by the program `powermaps.py`, for $p \leq 47$.

(4) This follows from Proposition 8.1 below, the map $j \to j^d$ being not affine. □

8. Newton strata, finite order

We discuss now the finite order problem for the matrices $H = F_pPD$, with D having p-th roots of unity as entries. The question is that of deciding when some power of $H/\sqrt{p}$ is the identity. By Theorem 4.4 this is the same as asking for H to be supersingular, and so our question is part of a more general one, namely the classification of the matrices F_pPD according to their Newton polygon. By multiplying by a root of unity, which does not change the polygon, we can assume $D_{00} = 1$. There are $p!\,p^{p-1}$ such matrices.

The basic examples of finite order matrices are those coming from the Weil representation [61]. Consider the shift $X = (\delta_{i,j+1})$ and the diagonal matrix $Z = diag(w^j)$. The Clifford group is the normalizer in the unitary group of the group generated by X, Z. Its quotient by the scalars is finite, of order $p^2|SL_2(\mathbb{F}_p)|$. See [2]. We have:

Proposition 8.1. *A matrix $H = F_pPD$ as above belongs to the Clifford group, up to a scalar, precisely when the permutation σ is affine, and the numbers d_j are of the form $w^{f(j)}$, with f being a polynomial of degree at most 2. There are $p^3(p-1)$ such matrices, all of finite order.*

Proof. Since F_p belongs to the Clifford group, up to a scalar, the question is whether the monomial matrix PD does. But the monomial matrices in the Clifford group are well-known to be, up to scalars, the products of powers of X, Z, of permutation matrices coming from the maps $j \to aj$, and of diagonal matrices of type $diag(w^{cj^2})$. See [2]. This gives the first assertion, and the count, and the last assertion is clear. □

Here the finite order claim comes from the fact that the Clifford group is finite modulo scalars, and that $\det(H/\sqrt{p})$ is a root of unity. By Theorem 4.4, the Clifford matrices are supersingular, with all Newton slopes equal to $\frac{1}{2}$. The question is whether these are the only finite order matrices, and Theorem 7.4 shows that this is not the case, in general. Let us first look at the whole picture, at small values of p. At the opposite end we have the lowest possible polygon, from Theorem 5.3. The program `strata.py` computes the Newton polygons of all the above matrices at $p = 5$, by exact arithmetic in $\mathbb{Z}[w]$, implemented in the file `cyclo.py`, and the result is as follows, with the slopes multiplied by 4:

slopes $\times 4$	number of matrices	comment
$1,1,2,3,3$	50000	lowest, Theorem 5.3
$1,2,2,2,3$	22500	contains G_5
$\frac{3}{2},\frac{3}{2},2,\frac{5}{2},\frac{5}{2}$	2000	
$2,2,2,2,2$	500	supersingular, contains F_5

Thus, at $p=5$ we have 4 strata. Observe that this table is an invariant of the equivalence class of F_5, in the usual sense. At $p=7$ the number of matrices is too big for an exhaustive computation of this type. As an illustration, the program `seven.py` deals with the 7^6 matrices having as permutation the inversion, as in Section 6, and finds the following polygons, with the slopes multiplied by 6:

slopes $\times 6$	number of matrices	comment
$1,1,2,3,4,5,5$	100842	lowest, Theorem 5.3
$1,2,2,3,4,4,5$	14406	
$1,2,3,3,3,4,5$	2107	contains G_7
$1,3,3,3,3,3,5$	294	

The supersingular stratum can however be fully computed at $p=7$. Indeed, in terms of the exponents $a_j\in\mathbb{Z}_p$ of the diagonal entries of H, the supersingularity requires $Tr(H)=\sum_j w^{a_j}$ to be divisible by $(w-1)^3$, which amounts to $\sum_j a_j=\sum_j a_j^2=0$. This reduces the number of matrices to be tested by a factor of 49. In order to state the result, let us call exotic a matrix which has finite order, without being Clifford. By Theorem 7.4 such matrices exist for most primes, starting with $p=11$, but that result gives nothing at $p=5,7$. However, exotic matrices do exist at $p=7$, and are constructed as follows, with $\left(\frac{j}{p}\right)$ being the Legendre symbol, and with all the divisions being taken modulo p:

Definition 8.2. *Let $\alpha\in\mathbb{F}_7^*$, let $r\in\{2,4\}$, and let $\varepsilon_+,\varepsilon_-\in\{-1,0,1\}$ be distinct. The associated matrix of Legendre type is*

$$E_{ij}=w^{\alpha_j(ij+\varepsilon_j j^2/2)}$$

where $(\alpha_j,\varepsilon_j)=(\alpha,\varepsilon_+)$ when $\left(\frac{j}{7}\right)\neq -1$, and $(\alpha_j,\varepsilon_j)=(r\alpha,\varepsilon_-)$ when $\left(\frac{j}{7}\right)=-1$.

There are 72 such matrices. Observe that $r=2,4$ are the primitive cubic roots of unity modulo 7, and that the parameters $\varepsilon=\pm 1$ correspond to the diagonal matrices $diag(w^{\pm j^2/2})$, which will appear again in Section 11 below. Thus, the columns of E come from 2 different Clifford matrices, one for the squares, and one for the non-squares. We do not have a conceptual explanation for the result below. Also, the Newton polygons of the matrices which are equivalent to F_p, and the size of each stratum, remain to be computed in general.

Regarding the description of the exotic matrices, observe that with $H=(w^{i\sigma(j)+\tau(j)})$, the conjugation by X^aZ^b replaces the functions $\sigma(j),\tau(j)$ by the functions $\sigma(j-a)+b$ and $\tau(j-a)-a\sigma(j-a)-bj$, up to a scalar. The program `translates.py` generates in this way the $72\cdot 49$ conjugates of the matrices of Legendre type, normalized by $D_{00}=1$, and checks that these are 3528 distinct matrices, with those satisfying $\sigma(0)=0$ being precisely the 504 exotic matrices found by the exhaustive search. Our result is as follows:

Theorem 8.3. *Consider the $p!\,p^{p-1}$ matrices $H = F_pPD$ as above, with $D_{00} = 1$.*

(1) *At $p = 3, 5$ the finite order matrices are the Clifford ones.*
(2) *At $p = 7$ there are 5586 finite order matrices, namely the 2058 Clifford ones, and 3528 exotic ones. The exotic matrices are, up to scalars, the conjugates of the 72 matrices of Legendre type by the matrices X^aZ^b.*
(3) *A matrix of Legendre type has projective order 15 when $(\varepsilon_+, \varepsilon_-)$ is $(0, -1)$ or $(-1, 0)$, and 7 otherwise. Its eigenvalues are distinct, and in the order 15 case they are, up to a scalar, the cubic roots of unity, and the nontrivial roots of unity of order 5.*
(4) *At $p = 5, 11, 13$ the matrices of type $(w^{\alpha_j ij+\beta_j j^2})$, with α_j, β_j depending only on the Legendre symbol of j, are never exotic.*

Proof. All this follows from Theorem 4.4, which reduces the finite order condition to an exact computation of valuations in $\mathbb{Z}[w]$, and from computer calculations. To be more precise, (1) follows from the above table at $p = 5$, and from the fact that all the matrices are Clifford at $p = 3$. The assertion (2) is obtained by the program `exotic.py`, which performs the exhaustive search explained above, and whose output is listed in the file `exotic.txt`. Finally, (3,4) are obtained by the programs `legendre.py` and `example.py`, the latter checking the projective orders by exact arithmetic. □

9. Polynomial maps, trace bounds

We discuss now the matrices of type $H = (w^{i\sigma(j)+\tau(j)})$, with $\sigma, \tau \in \mathbb{F}_p[x]$ being polynomials. As explained in Section 5, any matrix F_pPD with D having p-th roots of unity as entries is of this form, with σ being a permutation polynomial, the point being that we are now interested in the degrees of σ, τ. Our starting point is the following observation, which holds without assuming that σ is a permutation:

Proposition 9.1. *The traces of the powers of $H = (w^{i\sigma(j)+\tau(j)})$ are given by*

$$Tr(H^n) = \sum_{x\in\mathbb{F}_p^n} w^{f_n(x)} \quad , \quad f_n(x) = \sum_{i\in\mathbb{Z}_n} (x_i\sigma(x_{i+1}) + \tau(x_i))$$

with the indices of the variables $x_1, \ldots, x_n$ being taken modulo n.

Proof. This is clear from $Tr(H^n) = \sum_x H_{x_1x_2}H_{x_2x_3}\ldots H_{x_nx_1}$. □

In the language of statistical mechanics, $Tr(H^n)$ is the partition function of a periodic chain of n spins $x_i \in \mathbb{Z}_p$, with complex Boltzmann weights $w^{x\sigma(y)+\tau(y)}$, and with H being the transfer matrix. We will be back to this in Section 11. The generating function of these partition functions is the function $1/\det(1 - tH)$ from Proposition 1.4. In order to estimate these sums, we will need:

Proposition 9.2. *Let $d, n \geq 2$, and assume that p does not divide $d(d + 1)$. The hypersurface*

$$\sum_{i\in\mathbb{Z}_n} x_ix_{i+1}^d = 0$$

in the projective space of dimension $n - 1$, over the algebraic closure of $\mathbb{F}_p$, is smooth precisely when $(-d)^n \neq 1$ modulo p.

Proof. A singular point is a nonzero solution of the equations $x_{k+1}^d + dx_{k-1}x_k^{d-1} = 0$, with $k \in \mathbb{Z}_n$. If one coordinate of such a solution vanishes, so does the next one, and so all of them. Thus the numbers $r_k = x_{k+1}/x_k$ are well-defined, their product is 1, and the equations read $r_{k-1}r_k^d = -d$. By multiplying these equations we obtain $(-d)^n = 1$.

Conversely, assume $(-d)^n = 1$. Starting with $r = r_n$, the equations give $r_{n-j} = c_j r^{(-d)^j}$, for certain nonzero constants c_j, and the last equation holds when $r^N = c$, with $N = (-d)^n - 1$, which is a nonzero integer, and with $c \neq 0$. Such a number r exists in the algebraic closure, and the product ρ of the numbers r_k satisfies $\rho^{d+1} = (-d)^n = 1$. Now replacing $r \to r\eta$ with $\eta^N = 1$ replaces $\rho \to \rho\eta^S$, with $S = -N/(d+1)$, and since η^S takes as values all the roots of unity of order $d+1$, we can arrange for having $\rho = 1$, and we obtain a singular point. □

As an illustration, at $d = n = 3$ we obtain the Klein quartic $xy^3 + yz^3 + zx^3 = 0$, which is singular precisely in characteristic 7. We can now state our main estimate:

Theorem 9.3. *Let $H = (w^{i\sigma(j)+\tau(j)})$, with $\sigma, \tau \in \mathbb{F}_p[x]$ of degrees $1 \leq d \leq p-2$ and $e \leq p-1$.*

1. *If $d \geq 2$ and $e \leq d$ then $|Tr(H^n)| \leq d^n p^{n/2}$, for any $n \geq 1$ such that $(-d)^n \neq 1$ modulo p.*
2. *If $e \geq d+2$ then $|Tr(H^n)| \leq (e-1)^n p^{n/2}$, for any $n \geq 1$.*

Proof. We use the following result of Deligne [12]: if f is a polynomial in n variables over $\mathbb{F}_p$, of degree D prime to p, whose homogeneous part of degree D defines a smooth projective hypersurface, then the corresponding exponential sum is bounded by $(D-1)^n p^{n/2}$.

(1) Here f_n has degree $d+1$, and its top homogeneous part is a multiple of the polynomial in Proposition 9.2, which applies at $n \geq 2$. At $n = 1$ this is the bound of Weil [59].

(2) Here f_n has degree e, and its top homogeneous part is a multiple of $\sum_i x_i^e$, which defines a Fermat hypersurface, which is smooth, because e is prime to p. □

The above estimates are verified numerically by the program `traces.py`. As a basic example for (2), we have the matrices $F_p diag(w^{cj^3})$ with $p \geq 5$, which are related to the cubic sequences of Alltop [1], and to the associated mutually unbiased bases [27]. For these matrices we obtain $|Tr(H^n)| \leq 2^n p^{n/2}$, for any n. As for the quadratic case, $d = 1$ and $e \leq 2$, not covered by the above result, here the matrices are Clifford, as explained in Section 8, and the situation is quite different. As a consequence, we have:

Theorem 9.4. *Let $H = (w^{i\sigma(j)+\tau(j)})$ be as above, with σ being a permutation, so that H is a complex Hadamard matrix, and let $\delta = d$ when $e \leq d$, and $\delta = e-1$ when $e \geq d+2$. Assume $\delta \geq 2$.*

1. *If H^n is a scalar multiple of the identity, for some $n \geq 1$, then $\delta^n \geq p-1$.*
2. *With δ fixed and $p \to \infty$, the eigenvalues of $H/\sqrt{p}$ become uniformly distributed on the unit circle.*

Proof. (1) Under this assumption we have $|Tr(H^n)| = p^{1+n/2}$. Thus, when Theorem 9.3 applies we obtain $p \leq \delta^n$. In the remaining case, p divides the nonzero integer $(-d)^n - 1$, and so $p \leq d^n + 1$.

(2) For $n \geq 1$ fixed and $p > \delta^n + 1$ Theorem 9.3 applies, and shows that the Fourier coefficient of order n of the spectral measure of $H/\sqrt{p}$, which is $Tr(H^n)/p^{1+n/2}$, is bounded by δ^n/p. Thus all the nontrivial Fourier coefficients converge to 0, and this gives the result. □

10. Product bases, isolation questions

We discuss now some isolation questions, where the invariants are those of the equivalence class. Given a complex Hadamard matrix $H \in M_n(\mathbb{C})$, consider the real vector space formed by the matrices $A \in M_n(\mathbb{R})$ satisfying $\sum_k H_{ik}\bar{H}_{jk}(A_{ik} - A_{jk}) = 0$, for any i, j. This is the space of first order deformations of H, and its dimension is at least $2n-1$, due to the deformations inside the equivalence class. The defect $d(H)$ is this dimension minus $2n-1$, and when $d(H) = 0$ the matrix H is isolated, in the sense that the complex Hadamard matrices which are close to it are obtained from it by multiplying the rows and columns by scalars. See [52], [53].

Throughout this section q is an odd prime, and $w = e^{2\pi i/q}$. Consider the matrices $B_c = T_c F_q/\sqrt{q}$ with $c \in \mathbb{F}_q$, where $T_c = diag(w^{cj^2})$, and set $B_\infty = 1$. The columns of these $q+1$ unitary matrices are the usual mutually unbiased bases of $\mathbb{C}^q$, from [23], [62], which are the eigenbases of the matrices XZ^{2c} and Z. We label these bases by the lines of $\mathbb{F}_q^2$, with c corresponding to the line spanned by $u_c = (1, 2c)$, and ∞ to the line spanned by $u_\infty = (0, 1)$. The following construction is due to McNulty and Weigert [37]:

Definition 10.1. *Given a complex Hadamard matrix $K \in M_N(\mathbb{C})$, and points $s_0, \ldots, s_{N-1}$ and $t_0, \ldots, t_{N-1}$ of the projective line over $\mathbb{F}_q$, with $s_i \neq t_j$ for any i, j, we set*

$$H_{ia,jb} = \sqrt{q}K_{ij}(B_{s_i}^* B_{t_j})_{ab}$$

and we denote by $H_K(s, t)$ this square matrix, of order Nq.

Since the bases B_{s_i}, B_{t_j} are unbiased, the entries of $H = H_K(s, t)$ are on the unit circle. Also, we have $H = \sqrt{Nq}U^*V$, where U, V are the unitary matrices whose columns are respectively the vectors $e_i \otimes B_{s_i}e_a$, and the vectors $\kappa_j \otimes B_{t_j}e_b$, with κ_j being the j-th column of $K/\sqrt{N}$. Thus H is a complex Hadamard matrix, coming from 2 product bases of $\mathbb{C}^N \otimes \mathbb{C}^q$. The matrices considered in [4] are those where the point ∞ is not used, the bases there being $B_{k/2}$, written as $D^k F_q$ with $D = diag(w^{j(j-1)/2})$. As a first observation, we have:

Proposition 10.2. *The equivalence class of $H_K(s, t)$ is invariant under the action of the group $PSL_2(\mathbb{F}_q)$ on the points. Also, when $K = F_N$ with N prime to q, the defect of $H_K(s, t)$ is invariant under the action of $PGL_2(\mathbb{F}_q)$ on the points.*

Proof. For any $g \in SL_2(\mathbb{F}_q)$ the Weil representation provides us with a Clifford unitary U_g, which conjugates the matrices $X^a Z^b$ according to the action of g on the vectors (a, b), up to scalars [2]. Thus U_g maps the eigenbasis labeled by a line to the eigenbasis labeled by the image of that line, so $U_g B_c = B_{gc}M_c$ with M_c monomial, and we obtain $B_{gs_i}^* B_{gt_j} = M_{s_i} B_{s_i}^* B_{t_j} M_{t_j}^*$, which gives the first assertion. As for the second assertion, the automorphism $w \to w^a$ fixing the entries of K maps B_c to B_{ac}, up to a permutation of the columns, and $\sqrt{q}$ to $\pm\sqrt{q}$, hence $H_K(s, t)$ to a matrix which is equivalent to $H_K(as, at)$. Since the defect is the corank of a linear system with coefficients in our cyclotomic field, it is invariant under such automorphisms, and since $PGL_2(\mathbb{F}_q)$ is generated by $PSL_2(\mathbb{F}_q)$ and by the maps $c \to ac$, we are done. □

In order to compute now the defect, consider the matrix $\Lambda_K \in M_{N^2}(\mathbb{C})$ having as entries the numbers $(\Lambda_K)_{ij,kl} = K_{ij}\bar{K}_{il}\bar{K}_{kj}K_{kl}/N$, which is unitary. This is the matrix of the Berezin transform of Karabegov, the defect of K being $2N-1$ less than the multiplicity of its eigenvalue 1, see [51]. Also, given $x \in \mathbb{F}_q^2$, we write $x = nu_{s_i} + mu_{t_j}$, we set $c_{ij}(x) = nm\det(u_{s_i}, u_{t_j})$, and we consider the diagonal matrix $\Theta_x = diag(w^{c_{ij}(x)})$, of order N^2. With these conventions, we have:

Theorem 10.3. *The defect of the matrix $H = H_K(s,t)$ is given by*

$$d(H) = \sum_x \dim\ker(\Lambda_K - \Theta_x) - (2Nq-1)$$

with the sum being over the q^2 points $x \in \mathbb{F}_q^2$.

Proof. Let u_α, v_β be the columns of U, V, and Q_α, P_β be the projections on these vectors. Given a first order deformation A, the matrix $R = (H_{\alpha\beta}A_{\alpha\beta})$ is such that RH^* is self-adjoint, and so is $Y = URV^*$, because $HV^* = \sqrt{Nq}U^*$. Conversely, a self-adjoint matrix Y comes from a deformation when the numbers $u_\alpha^*Yv_\beta/u_\alpha^*v_\beta$ are real, which means $Tr(Y[Q_\alpha, P_\beta]) = 0$, for any α, β. Since these equations are stable under $Y \to Y^*$, we conclude that $d(H) + 2Nq - 1$ is the dimension of the space of matrices $Y \in M_{Nq}(\mathbb{C})$ satisfying them.

In our case we have $Q_{ia} = E_i \otimes \pi_a^{s_i}$ and $P_{jb} = G_j \otimes \pi_b^{t_j}$, with E_i, G_j being the projections on e_i, κ_j, and with π_a^c being the projection on the a-th column of B_c. Consider the matrices $D_{(a,b)} = \tau^{ab}X^aZ^b$ with $\tau = w^{(q+1)/2}$, which form a basis of $M_q(\mathbb{C})$, and satisfy $D_xD_y = \tau^{-\det(x,y)}D_{x+y}$. The span of the projections π_a^c being the span of the matrices D_{nu_c} with $n \in \mathbb{Z}_q$, we can replace in our equations $\pi_a^{s_i}, \pi_b^{t_j}$ by $D_{nu_{s_i}}, D_{mu_{t_j}}$. Now with $x = nu_{s_i} + mu_{t_j}$ we have:

$$[E_i \otimes D_{nu_{s_i}}, G_j \otimes D_{mu_{t_j}}] = (\tau^{-c_{ij}(x)}E_iG_j - \tau^{c_{ij}(x)}G_jE_i) \otimes D_x$$

Thus, by writing $Y = \sum_x Y_x \otimes D_x^*$, the equations split over the points x, and $d(H) + 2Nq - 1$ is the sum over x of the dimensions of the spaces of matrices $Y_x \in M_N(\mathbb{C})$ satisfying $Tr(Y_xE_iG_j) = w^{c_{ij}(x)}Tr(Y_xG_jE_i)$, for any i, j. Finally, in terms of the numbers $v_{ij} = \bar{K}_{ij}e_i^*Y_x\kappa_j$, which determine Y_x, these latter equations read $\Lambda_K v = \Theta_x v$, and we are done. □

Observe that $N\Lambda_K$ is a complex Hadamard matrix of order N^2, which for $K = F_N$ is equivalent to $F_N \otimes F_N$. Thus, for $K = F_N$ the matrices $N\bar{\Theta}_x\Lambda_K$ are twisted Fourier matrices, of Butson type, as those studied in the previous sections, and Theorem 10.3 tells us that the defect counts the occurrences of the real Weil number N in their spectra. The point $x = 0$ contributes with $d(K) + 2N - 1$, and each nonzero point of the line s_i or t_j contributes with at least the multiplicity of that line, so when $d(K) = 0$ and the $2N$ points are distinct we have $d(H) = 0$ precisely when there are no other contributions. The program `twisted.py` checks the above formula against direct computations, `symmetry.py` checks Proposition 10.2, and `samples.py` computes the defects of random configurations for $K = F_N$ with $N = 3, 5, 7$ and $q \leq 17$. All the configurations of distinct points that we tested have defect 0, whereas for the configurations with repeated points, as those in [37] with $q < 2N - 1$, most of the defects are 0, but not all.

Question 10.4. Is the matrix $H_K(s,t)$ isolated, whenever $K = F_N$ with N being an odd prime, and the $2N$ points are distinct?

At $N = 2$ the situation is different, and can be fully understood, with the answer depending on the cross-ratio λ of the 4 points. The program `crossratio.py` checks the result below for $q \leq 23$, the defects 8 and 12 at $q = 5, 7$ having been found in [37], and finds that the entries are roots of unity of order q when λ is not a square, and of order $2q$ when λ is a square, up to equivalence. Also, `classes.py` finds by an exact test that at $q = 5, 7, 11$ the matrices associated to λ, λ' are equivalent, up to a Galois conjugation, precisely when $\lambda' = \lambda^{\pm 1}$, so that we obtain $1, 2, 3$ isolated matrices, up to equivalence and Galois conjugation. As an illustration, for the configuration $S = \{1, 3\}$, $T = \{0, 2\}$ from [4] we have $\lambda = -1/3$, which is a square precisely when $q = 1$ modulo 3. Thus, the corresponding matrix has defect 0 at $q = 5, 11, 17, 23$, and defect $2(q-1)$ at $q = 7, 13, 19$. In general, we have:

Theorem 10.5. *Let $K = F_2$, and let s_0, s_1, t_0, t_1 be distinct points of the projective line over $\mathbb{F}_q$, with cross-ratio $\lambda = \frac{(s_0-t_0)(s_1-t_1)}{(s_0-t_1)(s_1-t_0)}$. Consider the matrix $H = H_K(s,t)$, of order $2q$.*

1. *If λ is not a square in $\mathbb{F}_q$ then $d(H) = 0$, and so H is isolated.*
2. *If λ is a square in $\mathbb{F}_q$ then $d(H) = 2(q-1)$.*

Proof. We have $\Lambda_K = 1 - 2\xi\xi^t$ with $\xi = \frac{1}{2}(1, -1, -1, 1)$, the indices being $00, 01, 10, 11$. Thus, with $\theta_a = w^{c_a(x)}$, the equation $\Lambda_K v = \Theta_x v$ reads $(1-\theta_a)v_a = 2r\xi_a$ for any a, where $r =< v, \xi >$. The solutions with $r = 0$ are the vectors orthogonal to ξ, supported by the indices where $c_a(x) = 0$. Since we have $c_{ij}(x) = 0$ precisely when x is on the line s_i or t_j, these solutions form a space of dimension 3 at $x = 0$, of dimension 1 at the $4(q-1)$ nonzero points of our 4 lines, and of dimension 0 elsewhere. Thus $d(H)$ is the number of points x having solutions with $r \neq 0$. Such points must be outside the 4 lines, the solution is then unique up to a scalar, $v_a = \xi_a/(1-\theta_a)$, and it exists when $\sum_a (1-\theta_a)^{-1} = 2$. Now since $(1-e^{i\varphi})^{-1} = \frac{1}{2} + \frac{i}{2}\cot\frac{\varphi}{2}$, this latter condition reads:

$$\sum_a \cot\left(\frac{\pi c_a(x)}{q}\right) = 0$$

By a theorem of Chowla [10], the numbers $\cot(\pi k/q)$ with $1 \leq k \leq \frac{q-1}{2}$ are linearly independent over $\mathbb{Q}$. Thus, the above condition is satisfied precisely when the 4 numbers $c_a(x) \in \mathbb{F}_q^*$ cancel in pairs. In order to see when this happens, pick y with $\det(x, y) = 1$, and for a point c not on the line of x, set $\zeta(c) = \alpha/\beta$, where $u_c = \alpha x + \beta y$. This is an affine coordinate on the projective line, with the line of x at infinity, and by solving $x = nu_{s_i} + mu_{t_j}$ we obtain:

$$\frac{1}{c_{ij}(x)} = \zeta(t_j) - \zeta(s_i)$$

With this formula in hand, the conditions $c_{00} = -c_{01}$, $c_{10} = -c_{11}$ give $\zeta(s_0) = \zeta(s_1)$, which is impossible, and the same happens with $c_{00} = -c_{10}$, $c_{01} = -c_{11}$. As for the remaining conditions, $c_{00} = -c_{11}$, $c_{01} = -c_{10}$, these are both equivalent to $\zeta(s_0) + \zeta(s_1) = \zeta(t_0) + \zeta(t_1)$, which means that the involution of the projective line which exchanges $s_0 \leftrightarrow s_1$ and $t_0 \leftrightarrow t_1$ is of the form $\zeta \to 2\mu - \zeta$, that is, has the line of x as fixed point. Thus $d(H)$ is $q-1$ times the number of fixed points of this involution. But in a coordinate

where $s_0 = 0$ and $s_1 = \infty$ the involution is $\zeta \to t_0 t_1/\zeta$, having 2 fixed points when $t_0 t_1$ is a square, and none otherwise, and since $\lambda = t_0/t_1$ there, this gives the result. □

In the case where λ is a square, the matrices can be deformed. The program `deform.py` finds numerically nearby complex Hadamard matrices at $q = 5, 7$, and in fact, we have:

Theorem 10.6. *In the context of Theorem 10.5, when λ is a square in $\mathbb{F}_q$, the matrix H belongs to a real analytic family of complex Hadamard matrices, which has dimension $q - 1$ modulo the multiplication of the rows and columns by scalars. Thus, H is isolated precisely when λ is not a square.*

Proof. By the proof of Theorem 10.5, the involution which exchanges $s_0 \leftrightarrow s_1$ and $t_0 \leftrightarrow t_1$ has a fixed point. Since $PSL_2(\mathbb{F}_q)$ acts transitively on the projective line, by Proposition 10.2 we can assume that this fixed point is ∞, so that the involution is of the form $c \to e - c$, and by using a translation, which is in $PSL_2(\mathbb{F}_q)$ too, we can assume $e = 0$. Thus, we can assume that our points are $s, -s$ and $t, -t$, which are finite, and distinct.

Consider the matrices $C_h = F_q^* T_h F_q/\sqrt{q}$ with $h \neq 0$. These are circulant, with entries $(C_h)_{ij} = G(h) w^{-(j-i)^2/4h}/\sqrt{q}$, where $G(h) = \sum_x w^{hx^2}$, and satisfy $C_{-h} = C_h^*$. Since we have $\sqrt{q} B_c^* B_d = C_{d-c}$, with $A = C_{t-s}$ and $B = C_{-t-s}$ our matrix is:

$$H = \begin{pmatrix} A & B \\ B^* & -A^* \end{pmatrix}$$

Now observe that a matrix of this form, with A, B being arbitrary circulant matrices with entries on the unit circle, is a complex Hadamard matrix precisely when $AA^* + BB^* = 2q$, because the circulant matrices commute with each other, and with their adjoints. In terms of the first rows f, g of A, B, and of the quantities $R_h(f) = \sum_j f_{j+h} \bar{f}_j$, this condition reads $R_h(f) + R_h(g) = 0$ for any $h \neq 0$, and since $R_{-h} = \bar{R}_h$, we have here $q - 1$ real equations.

In our case we have $f_j = \gamma w^{kj^2}$ with $k \neq 0$ and $|\gamma| = 1$, and for a variation of the phases $f_j \to f_j e^{iuv_j}$, with $v_j \in \mathbb{R}$, the derivative of $R_h(f)$ at $u = 0$ is given by:

$$\frac{dR_h}{du} = i w^{kh^2} (w^{-2kh^2} - 1) \sum_j v_j w^{2khj}$$

Since the factor before the sum is nonzero, and $h \to 2kh$ permutes the nonzero frequencies, this derivative vanishes for all $h \neq 0$ only when v is constant. Thus, with f_0 fixed, the derivative is an isomorphism between real vector spaces of dimension $q - 1$, and by the implicit function theorem, for any phase vector g close to the initial one we can find f, depending analytically on g, such that the above block matrix is Hadamard. With g_0 fixed too, we have $q - 1$ free parameters. Finally, the quotients $g_j^2/(g_{j-1} g_{j+1})$, which are products of type $H_{ab} H_{cd}/(H_{ad} H_{cb})$, are invariant under the multiplication of the rows and columns by scalars, and their logarithmic derivatives, which are $2v_j - v_{j-1} - v_{j+1}$ up to a factor i, vanish only when v is constant. Thus our family has dimension $q - 1$ modulo such multiplications, and this gives the result, the last assertion coming from Theorem 10.5. See also [7], for related computations, for the biunimodular sequences. □

11. Spin models and Ising arrays

We end with a discussion of the relation with statistical mechanics, and more precisely with the spin models of Jones [24], which are known to produce complex Hadamard matrices, and subfactors. Let us start with the following definition, from [5], [24]:

Definition 11.1. *A unimodular spin model is a symmetric complex Hadamard matrix $W \in M_N(\mathbb{C})$ satisfying the star-triangle equation, with $D = \pm\sqrt{N}$, and for any a, b, c:*

$$\sum_x W_{ax} W_{bx} \overline{W}_{cx} = D W_{ab} \overline{W}_{ac} \overline{W}_{bc}$$

The common value of the diagonal entries of W is called modulus of the model.

Here the fact that the diagonal entries are all equal comes from the star-triangle equation at $b = c$, which reads $\sum_x W_{ax} = D\overline{W}_{bb}$, for any a, b. The modulus plays a key role in the construction of the link invariant associated to W, where it corresponds to the first Reidemeister move. See [24].

In relation with our considerations, the point is that, for a spin model, the trace is a well-defined quantity, equal to N times the modulus. Moreover, the simultaneous conjugation of rows and columns by a permutation, which preserves the notion of spin model, is a particular case of the conjugation of Hadamard matrices from Section 1.

In the case of the cyclic groups, spin models were constructed by Bannai-Bannai [5], from the solutions of a modular invariance equation, that they determined, of type $(PT)^3 = \sqrt{N}P^2$, or $(PT)^3 = N^{3/2}$, with $P = F_N$, and with T being diagonal. See also [6]. In our setting, the simplest solutions of these equations are as follows:

Proposition 11.2. *Let p be an odd prime, $c \in \mathbb{F}_p^*$, and consider the matrix $T_c = diag(w^{cj^2})$, and the quadratic Gauss sum $G(c) = \sum_x w^{cx^2}$. We have then*

$$(F_pT_c)^3 = \begin{cases} pG(c) & \text{if } 2c = 1 \\ G(c)F_p^2 & \text{if } 2c = -1 \end{cases}$$

and $(F_pT_c)^3$ is not a monomial matrix when $2c \neq \pm 1$. In all cases, F_pT_c is a Clifford matrix, having finite order.

Proof. By completing the square we have $(F_pT_cF_p)_{ik} = G(c)w^{-(i+k)^2/4c}$, and then:

$$((F_pT_c)^3)_{il} = G(c)\sum_k w^{k^2(c-1/4c)+k(l-i/2c)-i^2/4c+cl^2}$$

When $4c^2 = 1$ the sum over k vanishes unless $l = i/2c$, and we obtain the formulae in the statement. Otherwise this sum is a Gauss sum, of absolute value $\sqrt{p}$. Finally, the last assertion follows from Proposition 8.1. □

Thus, the modular invariance equation is a finite order condition, of the type studied in this paper. In the language of Section 4, it tells us that we are in the supersingular case, with the cube of the Frobenius map being a scalar, or a scalar multiple of the involution $j \to -j$.

The matrices F_pT_c are well-known in quantum physics too. Indeed, these matrices are conjugate to the matrices T_cF_p, whose columns form, together with the standard basis of

$\mathbb{C}^p$, the usual $p+1$ mutually unbiased bases, constructed by Ivanović [23] and Wootters-Fields [62]. See [38]. More generally, the Clifford matrices are known from the work of Hannay-Berry [20] and Keating [26] on the quantization of the linear maps of the torus, where the traces of their powers are given exactly by a sum over periodic orbits, and from the subsequent arithmetic work of Kurlberg-Rudnick and others [30], [31], where the Weil and Deligne bounds for exponential sums are used. It would be interesting to have a similar physical interpretation for the other Newton strata, for the exotic matrices found in Sections 7-8, and for the trace bounds in Section 9.

Regarding now the spin models themselves, in the cyclic case these are well-known as well, from the work of Goldschmidt-Jones [17]. The corresponding matrices, which appear as well as transition matrices between the above mutually unbiased bases, can be studied with our methods. The result, whose second part shows that the modulus of the model encodes the sign of the quadratic Gauss sum, which was the starting point of the present paper, and which is verified by the program `spin.py`, is as follows:

Theorem 11.3. *Let p be an odd prime, $c \in \mathbb{F}_p^*$ and $|t| = 1$, and consider the matrix $W = (tw^{c(i-j)^2})$, which is symmetric and circulant.*

(1) *W is complex Hadamard, with trace pt, and with eigenvalues $tG(c)w^{-k^2/4c}$.*

(2) *W is a unimodular spin model, with $D = \sqrt{p}$, precisely when $t^2 = \overline{G(c)}/\sqrt{p}$, that is, when $t^2 = \left(\frac{c}{p}\right)$ for $p = 1(4)$, and when $t^2 = -i\left(\frac{c}{p}\right)$ for $p = 3(4)$.*

(3) *In this case $W \in H_p(8p)$, the matrix $W/\sqrt{p}$ has finite order, with eigenvalues $\bar{t}w^{-k^2/4c}$, and the abelian varieties having W_W as Weil polynomial are supersingular.*

Proof. (1) The matrix W being circulant, its eigenvalues are the Fourier coefficients of its first row, which are the numbers in the statement, by completing the square. These numbers have absolute value $\sqrt{p}$, so W is Hadamard.

(2) With indices i, j, k, and by completing the square, the left term of the star-triangle equation is $tG(c)w^{2c(ik+jk-ij-k^2)}$, and the right term is $D\bar{t}$ times the same power of w. Thus the equation reads $t^2 = D/G(c)$, and the result follows from the classical formula of $G(c)$, namely $G(c) = \left(\frac{c}{p}\right)\sqrt{p}$ for $p = 1(4)$, and $G(c) = \left(\frac{c}{p}\right) i\sqrt{p}$ for $p = 3(4)$.

(3) This follows from (1,2), which give $tG(c) = \bar{t}\sqrt{p}$, and from Theorem 4.4. □

Let us discuss now a second relation with statistical mechanics, where the matrix plays a different role. Given a real Hadamard matrix $H \in H_N(2)$, consider $2N$ Ising spins $a_j, b_k \in \{\pm 1\}$, with energy as follows:

$$E(a,b) = -\frac{1}{\sqrt{N}} < Hb, a >$$

This is the Ising array of H, studied in [42]. Here H is a coupling matrix, between 2 different sets of spins, and the model depends only on the equivalence class of H. This is in contrast with Proposition 9.1, where H was a transfer matrix, acting on a single set of spins, with the model depending on the conjugation class of H. Thus, the 2 relations from Definition 1.2 correspond to the 2 possible physical roles of a Hadamard matrix.

The arithmetic invariants are useful for the arrays too. We have $E \geq -N$, with equality for the crystalline states, which correspond to the vectors b such that $|(Hb)_j| = \sqrt{N}$ for

any j, called bent sequences in [49]. It is shown in [42] that at $N = 16$ the density of states of the array depends only on the 2-rank r, the number of crystalline states being $2^{14-r} - 128$. By Proposition 4.3, this means that at $N = 16$ the thermodynamics of the array is determined by the Hodge polygon of H. As for the self-dual bent sequences, satisfying $Hb = \sqrt{N}b$, which were studied in [47], these are eigenvectors of H, and so depend on the conjugation class.

For the Walsh matrix of order 4^n, the crystalline states are the bent functions of Rothaus [45], whose number is known up to $n = 4$, see [33]. In relation with the present paper, consider the complex version of the array, with H being a complex Hadamard matrix, with spins a_j, b_k on the unit circle, and with energy $-Re < Hb, a > /\sqrt{N}$. As before, the crystalline states come from the vectors b such that Hb has entries of modulus $\sqrt{N}$. We have:

Theorem 11.4. *Let p be an odd prime, and to any function $f : \mathbb{Z}_p^2 \to \mathbb{Z}_p$ associate the vector $b_f = (w^{f(i,j)})$, and the matrix $B_f = (w^{f(i,j)})$, of size p.*

1. *b_f is a crystalline state of the array of $F_p \otimes F_p$ precisely when f is bent, and this happens precisely when $F_pB_fF_p$ has all its entries of modulus p.*
2. *Any matrix $H = F_pPD$, with D having p-th roots of unity as entries, is of the form B_f with f bent, and so is the transpose of F_pHF_p/p, which is of the same type.*
3. *At $p = 3$ there are 486 bent functions, all quadratic, with 270 of them corresponding to the matrices F_3PD, or to their transposes.*
4. *The vector (w^{cj^2}) is an eigenvector of F_p precisely when $4c^2 = -1$, the eigenvalue being then $\sqrt{p}$. Thus, such eigenvectors exist precisely when $p = 1(4)$.*

Proof. (1) With the vectors written as matrices, $F_p \otimes F_p$ acts by $B \to F_pBF_p$. Now the entries of $F_pB_fF_p$ are the numbers $\sum_{xy} w^{f(x,y)+ax+by}$, and by definition, see [29], f is bent when all these numbers have modulus p.

(2) We have $F_pHF_p = pCPDF_p$, where C is the permutation matrix of $j \to -j$, and this matrix has entries of modulus p. By transposing we obtain the matrix $pF_pDP^{-1}C$, which is of the form $pF_pP'D'$. This is in agreement with the well-known fact that the duals of the Maiorana-McFarland functions are of the same type.

(3) This is obtained by the program `arrays.py`.

(4) By completing the square, F_p maps (w^{cj^2}) to $G(c)(w^{-j^2/4c})$, and this gives the condition $4c^2 = -1$. Regarding the eigenvalue, this is $G(c) = \left(\frac{c}{p}\right)\sqrt{p}$, and the Legendre symbol is 1, because with $i^2 = -1$ we have $c = \pm 1/2i$, and the Legendre symbols of 2 and i are both equal to $(-1)^{(p-1)/4}$. For more on the ternary bent functions, we refer to [40]. □

References

[1] W.O. Alltop, Complex sequences with low periodic correlations, *IEEE Trans. Inform. Theory* **26** (1980), 350–354.

[2] D.M. Appleby, Symmetric informationally complete-positive operator valued measures and the extended Clifford group, *J. Math. Phys.* **46** (2005), 1–29.

[3] T. Banica, Introduction to arithmetic, hal-05224945 (2026).

[4] T. Banica, D. Özteke and L. Pittau, Isolated partial Hadamard matrices, and related topics, *Open Syst. Inf. Dyn.* **25** (2018), 1–27.
[5] E. Bannai and E. Bannai, Spin models on finite cyclic groups, *J. Algebraic Combin.* **3** (1994), 243–259.
[6] E. Bannai, E. Bannai and F. Jaeger, On spin models, modular invariance, and duality, *J. Algebraic Combin.* **6** (1997), 203–228.
[7] Y. Benoist, Fourier transform in cyclic groups, arXiv:2406.11529 (2024).
[8] A.T. Butson, Generalized Hadamard matrices, *Proc. Amer. Math. Soc.* **13** (1962), 894–898.
[9] T.G. Centeleghe and J. Stix, Categories of abelian varieties over finite fields, I: Abelian varieties over $\mathbb{F}_p$, *Algebra Number Theory* **9** (2015), 225–265.
[10] S. Chowla, The nonexistence of nontrivial linear relations between the roots of a certain irreducible equation, *J. Number Theory* **2** (1970), 120–123.
[11] P. Deligne, Variétés abéliennes ordinaires sur un corps fini, *Invent. Math.* **8** (1969), 238–243.
[12] P. Deligne, La conjecture de Weil. I, *Publ. Math. IHES* **43** (1974), 273–307.
[13] T. D'Nelly-Warady and K.S. Kedlaya, Geometric decomposition of abelian varieties of order 1, in "Research directions in number theory: Women in Numbers V", Springer (2024), 253–270.
[14] D.E. Dutkay, J. Haussermann and E. Weber, Spectral properties of small Hadamard matrices, *Linear Algebra Appl.* **506** (2016), 363–381.
[15] R. Egan and P. Ó Catháin, Morphisms of Butson classes, *Linear Algebra Appl.* **577** (2019), 78–93.
[16] R. Egan, P. Ó Catháin and E. Swartz, Spectra of Hadamard matrices, *Australas. J. Combin.* **73** (2019), 501–512.
[17] D.M. Goldschmidt and V.F.R. Jones, Metaplectic link invariants, *Geom. Dedicata* **31** (1989), 165–191.
[18] B.H. Gross and N. Koblitz, Gauss sums and the p-adic Γ-function, *Ann. of Math.* **109** (1979), 569–581.
[19] U. Haagerup, Orthogonal maximal abelian $*$-subalgebras of the $n \times n$ matrices and cyclic n-roots, in "Operator algebras and quantum field theory", International Press (1997), 296–323.
[20] J.H. Hannay and M.V. Berry, Quantization of linear maps on a torus-Fresnel diffraction by a periodic grating, *Phys. D* **1** (1980), 267–290.
[21] T. Honda, Isogeny classes of abelian varieties over finite fields, *J. Math. Soc. Japan* **20** (1968), 83–95.
[22] K. Ireland and M. Rosen, A classical introduction to modern number theory, Springer (1990).
[23] I.D. Ivanović, Geometrical description of quantal state determination, *J. Phys. A* **14** (1981), 3241–3245.
[24] V.F.R. Jones, On knot invariants related to some statistical mechanical models, *Pacific J. Math.* **137** (1989), 311–334.
[25] N.M. Katz, Slope filtration of F-crystals, *Astérisque* **63** (1979), 113–163.
[26] J.P. Keating, The cat maps: quantum mechanics and classical motion, *Nonlinearity* **4** (1991), 309–341.
[27] A. Klappenecker and M. Rötteler, Constructions of mutually unbiased bases, in "Finite fields and applications", Springer (2004), 137–144.
[28] L. Kronecker, Zwei Sätze über Gleichungen mit ganzzahligen Coefficienten, *J. Reine Angew. Math.* **53** (1857), 173–175.
[29] P.V. Kumar, R.A. Scholtz and L.R. Welch, Generalized bent functions and their properties, *J. Combin. Theory Ser. A* **40** (1985), 90–107.
[30] P. Kurlberg, L. Rosenzweig and Z. Rudnick, Matrix elements for the quantum cat map: fluctuations in short windows, *Nonlinearity* **20** (2007), 2289–2304.
[31] P. Kurlberg and Z. Rudnick, Hecke theory and equidistribution for the quantization of linear maps of the torus, *Duke Math. J.* **103** (2000), 47–77.
[32] M. Künzer and H. Weber, On the cyclotomic Dedekind embedding and the cyclic Wedderburn embedding, arXiv:math/0103125 (2004).
[33] P. Langevin and G. Leander, Counting all bent functions in dimension eight 99270589265934370305785861242880, *Des. Codes Cryptogr.* **59** (2011), 193–205.
[34] M.L. Madan and S. Pal, Abelian varieties and a conjecture of R.M. Robinson, *J. Reine Angew. Math.* **291** (1977), 78–91.
[35] B. Mazur, Frobenius and the Hodge filtration, *Bull. Amer. Math. Soc.* **78** (1972), 653–667.
[36] R.L. McFarland, A family of difference sets in non-cyclic groups, *J. Combin. Theory Ser. A* **15** (1973), 1–10.
[37] D. McNulty and S. Weigert, Isolated Hadamard matrices from mutually unbiased product bases, *J. Math. Phys.* **53** (2012), 1–21.

[38] D. McNulty and S. Weigert, Mutually unbiased bases in composite dimensions - a review, *Quantum* **10** (2026), 2051.
[39] T.S. Michael and W.D. Wallis, Skew-Hadamard matrices and the Smith normal form, *Des. Codes Cryptogr.* **13** (1998), 173–176.
[40] C. Moraga, M. Stanković, R.S. Stanković and S. Stojković, A contribution to the study of multiple-valued bent functions, in *Proc. 43rd Int. Symp. on Multiple-Valued Logic*, IEEE (2013), 340–345.
[41] M. Newman, Invariant factors of combinatorial matrices, *Israel J. Math.* **10** (1971), 126–130.
[42] Opus and Teo, Ising spins with Hadamard couplings, zenodo:24546490 (2026).
[43] P.R.J. Östergård, Equivalence of Butson-type Hadamard matrices, *J. Algebraic Combin.* **56** (2022), 271–277.
[44] R.M. Robinson, Conjugate algebraic units in a special interval, *Math. Z.* **154** (1977), 31–40.
[45] O.S. Rothaus, On "bent" functions, *J. Combin. Theory Ser. A* **20** (1976), 300–305.
[46] I. Schur, Über die Gaußschen Summen, *Nachr. Ges. Wiss. Göttingen* (1921), 147–153.
[47] M. Shi, Y. Li, W. Cheng, D. Crnković, D. Krotov and P. Solé, Self-dual Hadamard bent sequences, *J. Syst. Sci. Complex.* **36** (2023), 894–908.
[48] T. Shioda and T. Katsura, On Fermat varieties, *Tohoku Math. J.* **31** (1979), 97–115.
[49] P. Solé, W. Cheng, S. Guilley and O. Rioul, Bent sequences over Hadamard codes for physically unclonable functions, in "Proc. IEEE International Symposium on Information Theory" (2021), 801–806.
[50] L. Stickelberger, Über eine Verallgemeinerung der Kreistheilung, *Math. Ann.* **37** (1890), 321–367.
[51] W. Tadej, Defect and equivalence of unitary matrices. The Fourier case. Part I, *Open Syst. Inf. Dyn.* **25** (2018), 1850020.
[52] W. Tadej and K. Życzkowski, A concise guide to complex Hadamard matrices, *Open Syst. Inf. Dyn.* **13** (2006), 133–177.
[53] W. Tadej and K. Życzkowski, Defect of a unitary matrix, *Linear Algebra Appl.* **429** (2008), 447–481.
[54] J. Tate, Endomorphisms of abelian varieties over finite fields, *Invent. Math.* **2** (1966), 134–144.
[55] J. Tate, Classes d'isogénie des variétés abéliennes sur un corps fini (d'après T. Honda), *Sém. Bourbaki* **352** (1969), 95–110.
[56] W.D. Wallis and J. Wallis, Equivalence of Hadamard matrices, *Israel J. Math.* **7** (1969), 122–128.
[57] L.C. Washington, Introduction to cyclotomic fields, Springer (1997).
[58] W.C. Waterhouse, Abelian varieties over finite fields, *Ann. Sci. École Norm. Sup.* **2** (1969), 521–560.
[59] A. Weil, On some exponential sums, *Proc. Nat. Acad. Sci. USA* **34** (1948), 204–207.
[60] A. Weil, Numbers of solutions of equations in finite fields, *Bull. Amer. Math. Soc.* **55** (1949), 497–508.
[61] A. Weil, Sur certains groupes d'opérateurs unitaires, *Acta Math.* **111** (1964), 143–211.
[62] W.K. Wootters and B.D. Fields, Optimal state-determination by mutually unbiased measurements, *Ann. Physics* **191** (1989), 363–381.