Ann. Comb. 14 (2010) 443–456
DOI 10.1007/s00026-011-0069-6
Published online February 19, 2011

Annals of Combinatorics

A Prime Sensitive Hankel Determinant of Jacobi Symbol Enumerators

Ömer Eğecioğlu

Department of Computer Science, University of California, Santa Barbara, CA 93106, USA
omer@cs.ucsb.edu

Received July, 11, 2007

Mathematics Subject Classification: 11C20, 15A36, 11T24

Abstract. We show that the determinant of a Hankel matrix of odd dimension n whose entries are the enumerators of the Jacobi symbols which depend on the row and the column indices vanishes if and only if n is composite. If the dimension is a prime p, then the determinant evaluates to a polynomial of degree $p-1$ which is the product of a power of p and the generating polynomial of the partial sums of Legendre symbols. The sign of the determinant is determined by the quadratic character of -1 modulo p. The proof of the evaluation makes use of elementary properties of Legendre symbols, quadratic Gauss sums, and orthogonality of trigonometric functions.

Keywords: determinant, prime, Legendre symbol, Jacobi symbol, Gauss sum

1. Introduction

For an odd integer n and $k = 1, 2, \ldots, n$, define the polynomials

$$a_k(x) = \sum_{m=0}^{k} J(k-m, n)x^m,$$

in which $J(a, m)$ is the Jacobi symbol defined for odd integers m by

$$J(a, m) = \left(\frac{a}{p_1}\right)^{e_1} \left(\frac{a}{p_2}\right)^{e_2} \cdots \left(\frac{a}{p_k}\right)^{e_k},$$

where the prime factorization of m is $m = p_1^{e_1} p_2^{e_2} \cdots p_k^{e_k}$ and for a prime p, $\left(\frac{a}{p}\right)$ is the Legendre symbol defined by

$$\left(\frac{a}{p}\right) = \begin{cases} 0, & \text{if } p \mid a, \\ 1, & \text{if } a \text{ is a quadratic residue mod } p, \\ -1, & \text{if } a \text{ is a quadratic nonresidue mod } p\ . \end{cases}$$

For example, when $n = 3$, the first five polynomials are

$$a_1(x) = 1,$$
$$a_2(x) = x - 1,$$
$$a_3(x) = x^2 - x,$$
$$a_4(x) = x^3 - x^2 + 1,$$
$$a_5(x) = x^4 - x^3 + x - 1.$$

It is easy to see that $a_k(x)$ is a monic polynomial of degree $k-1$ and $a_k(0) = J(k,n)$. Consider the $n \times n$ Hankel determinant

$$H_n(x) = \det\left[a_{i+j-1}(x)\right]_{1\le i,\, j\le n}. \tag{1.1}$$

As an example,

$$H_3(x) = \det\begin{bmatrix} 1 & x-1 & x^2-x \\ x-1 & x^2-x & x^3-x^2+1 \\ x^2-x & x^3-x^2+1 & x^4-x^3+x-1 \end{bmatrix} = -x^2.$$

A few other determinant evaluations for small n are as follows:

$$H_5(x) = 5x^2(x-1)(x+1),$$
$$H_7(x) = -49x^2\left(x^4+2x^3+x^2+2x+1\right),$$
$$H_9(x) = 0,$$
$$H_{11}(x) = -14641x^2\left(x^8+x^6+2x^5+3x^4+2x^3+x^2+1\right),$$
$$H_{13}(x) = 371293x^2(x-1)(x+1)\left(x^8+2x^6+2x^5+3x^4+2x^3+2x^2+1\right),$$
$$H_{15}(x) = 0,$$
$$H_{17}(x) = 410338673x^2(x-1)(x+1)\Big(x^{12}+2x^{11}+2x^{10}+4x^9+3x^8+4x^7+2x^6$$
$$+4x^5+3x^4+4x^3+2x^2+2x+1\Big),$$
$$H_{19}(x) = -16983563041x^2\Big(x^{16}-x^{14}+x^{12}+2x^{11}+3x^{10}+2x^9+3x^8+2x^7+3x^6$$
$$+2x^5+x^4-x^2+1\Big).$$

Recently, Chapman [2] evaluated Hankel determinants of certain $\frac{p-1}{2} \times \frac{p-1}{2}$ dimensional 0–1 matrices built up from the Legendre symbol defined modulo a prime p. These evaluations give

$$\det\left[\frac{1}{2}\left(1+\left(\frac{i+j-1}{p}\right)\right)\right]_{1\le i,\, j\le \frac{p-1}{2}} = \det\left[\frac{1}{2}\left(1-\left(\frac{i+j-1}{p}\right)\right)\right]_{1\le i,\, j\le \frac{p-1}{2}} = -1,$$

for any prime $p > 3$, $p \equiv 3 \pmod 4$. [2] also includes additional conjectures related to such determinants. In this paper, we prove the following evaluation of the Hankel determinant $H_n(x)$:

Theorem 1.1. *$H_n(x)$ identically vanishes unless $n = p$ is a prime. For p prime,*

$$H_p(x) = (-1)^{\frac{p-1}{2}} p^{\frac{p-3}{2}} \sum_{k=0}^{p-1} b_k x^k,$$

where

$$b_k = \sum_{i=1}^{p-k} \left(\frac{i}{p}\right). \tag{1.2}$$

Furthermore, $H_p(x)$ is divisible in $\mathbb{Z}[x]$ by x^2 for $p \equiv 3 \pmod 4$ and by $x^2\left(x^2-1\right)$ for $p \equiv 1 \pmod 4$.

The properties of the Jacobi and Legendre symbols and Gauss sums that we make use of in the proof of Theorem 1.1 can readily be found in most books on number theory: We mention only [1, 5], and [6].

2. Proof of Theorem 1.1

We divide the proof of the theorem into a series of lemmas, and start with recording the following trivial property of the polynomials $a_k(x)$:

Lemma 2.1.

$$a_{k+1}(x) = J(k+1, n) + x a_k(x).$$

2.1. The Composite Case

Now we show that $H_n(x) \equiv 0$ if and only if n is composite, and then determine the structure of $H_p(x)$ for p prime.

Lemma 2.2. *$H_n(x)$ identically vanishes for n composite.*

Proof. Let $\mathbf{r}_i = (a_i, a_{i+1}, \ldots, a_{i+n-1})$ denote the i-th row of the matrix in (1.1). Let $\mathbf{e}_i$ denote the n-dimensional unit row vector with 1 in the i-th coordinate and 0 elsewhere, with $\mathbf{e}_i^t$ denoting its transpose. The proof is in two cases depending on whether or not n is a perfect square:

Case I: $n = m^2$ is a perfect square.

We claim that in this case the four rows $\mathbf{r}_1, \mathbf{r}_2, \mathbf{r}_{m+1}, \mathbf{r}_{m+2}$ are linearly dependent. More precisely,

$$\mathbf{r}_2 - x\mathbf{r}_1 = \mathbf{r}_{m+2} - x\mathbf{r}_{m+1}.$$

From Lemma 2.1,

$$\mathbf{r}_2 - x\mathbf{r}_1 = \sum_{i=1}^{m^2} J\left(i+1, m^2\right) \mathbf{e}_i \tag{2.1}$$

and

$$\mathbf{r}_{m+2} - x\mathbf{r}_{m+1} = \sum_{i=1}^{m^2} J\left(i+m+1, m^2\right)\mathbf{e}_i\,. \tag{2.2}$$

Note that

$$J\left(a, m^2\right) = J(a,m)J(a,m) = \begin{cases} 0, & \text{if } gcd(a,m) > 1, \\ 1, & \text{if } gcd(a,m) = 1. \end{cases}$$

Since

$$gcd(i+1, m) = gcd(i+m+1, m),$$

the right hand sides of (2.1) and (2.2) evaluate to the identical 0–1 vector.

Case II: $n = p^{2e+1}q$ with p prime, $p \not| q$.

Let $m = p^{2e+1}$. In this case we show that the following linear dependence among the rows holds:

$$\sum_{i=0}^{p-1} (\mathbf{r}_{iq+2} - x\mathbf{r}_{iq+1}) = \mathbf{0}.$$

By Lemma 2.1, the j-th entry of the vector on the left is

$$\begin{aligned} \sum_{i=0}^{p-1} J(iq+j+1, mq) &= J(j+1,q)\sum_{i=0}^{p-1} J(iq+j+1, m) \\ &= J(j+1,q)\sum_{i=0}^{p-1} J(iq+j+1, p) \\ &= J(j+1,q)\sum_{i=1}^{p-1} \left(\frac{i}{p}\right) \\ &= 0. \end{aligned}$$

∎

2.2. The Prime Case

Let now $n = p$ be prime. Using Lemma 2.1 and replacing $\mathbf{r}_{i+1}$ by $\mathbf{r}_{i+1} - x\mathbf{r}_i$ for $i = 1, 2, \ldots, p$, we obtain

$$H_p(x) = \det \begin{bmatrix} a_1(x) & a_2(x) & \cdots & a_{p-1}(x) & a_p(x) \\ \left(\frac{2}{p}\right) & \left(\frac{3}{p}\right) & \cdots & \left(\frac{p}{p}\right) & \left(\frac{p+1}{p}\right) \\ \left(\frac{3}{p}\right) & \left(\frac{4}{p}\right) & \cdots & \left(\frac{p+1}{p}\right) & \left(\frac{p+2}{p}\right) \\ \vdots & \vdots & \cdots & \vdots & \vdots \\ \left(\frac{p}{p}\right) & \left(\frac{p+1}{p}\right) & \cdots & \left(\frac{2p-2}{p}\right) & \left(\frac{2p-1}{p}\right) \end{bmatrix}. \tag{2.3}$$

Since $a_k(x)$ is of degree $k-1$, $H_p(x)$ is a polynomial of degree $p-1$.

Consider the $p \times p$ matrix

$$\mathbf{A}_p = \begin{bmatrix} \left(\frac{1}{p}\right) & \left(\frac{2}{p}\right) & \cdots & \left(\frac{p}{p}\right) \\ \left(\frac{2}{p}\right) & \left(\frac{3}{p}\right) & \cdots & \left(\frac{p+1}{p}\right) \\ \vdots & \vdots & \cdots & \vdots \\ \left(\frac{p}{p}\right) & \left(\frac{p+1}{p}\right) & \cdots & \left(\frac{2p-1}{p}\right) \end{bmatrix} = \left[\left(\frac{i+j-1}{p}\right)\right]_{1\le i,\, j\le p}. \tag{2.4}$$

Let $c_{i,\,j}$ denote the cofactor of the entry $(i,\, j)$ of $\mathbf{A}_p$. Expanding the determinant in (2.3) by the first row, we have

$$H_p(x) = \sum_{j=1}^{p} c_{1,\,j} a_j(x),$$

and the coefficient of the leading term is the cofactor $c_{1,\,p} = \det \mathbf{C}_p$ where $\mathbf{C}_p$ is the $(p-1) \times (p-1)$ matrix

$$\mathbf{C}_p = \begin{bmatrix} \left(\frac{2}{p}\right) & \left(\frac{3}{p}\right) & \cdots & \left(\frac{p}{p}\right) \\ \left(\frac{3}{p}\right) & \left(\frac{4}{p}\right) & \cdots & \left(\frac{p+1}{p}\right) \\ \vdots & \vdots & \cdots & \vdots \\ \left(\frac{p}{p}\right) & \left(\frac{p+1}{p}\right) & \cdots & \left(\frac{2p-2}{p}\right) \end{bmatrix} = \left[\left(\frac{i+j}{p}\right)\right]_{1\le i,\, j\le p-1}. \tag{2.5}$$

First we show that the $c_{1,\,j}$'s, and in fact all cofactors of $\mathbf{A}_p$ are identical.

Lemma 2.3. *All cofactors of the matrix $\mathbf{A}_p$ are identical.*

Proof. We note that $\mathbf{A}_p$ is a symmetric matrix with the i-th row sum

$$\sum_{j=1}^{p} \left(\frac{i+j-1}{p}\right) = 0,$$

for every i. Since the row sums vanish, the cofactor $c_{i,\,j}$ is independent of j. By symmetry, $c_{i,\,j}$ is also independent of i. One way to prove Lemma 2.3 combinatorially is to use the standard weighted version of Kirchoff's matrix-tree theorems (see [7,8]). We include it here for completeness. Consider the complete graph K_p on vertices $\{1, 2, \ldots, p\}$, and introduce the indeterminates $x_{i,\,j}$ for $1 \le i,\, j \le p$. Define

$$D_i = \sum_{j=1}^{p} x_{i,\,j} - x_{i,\,i},$$

and define the weighted Laplacian matrix by setting $\mathbf{L}_p = [L_{i,\,j}]_{1\le i,\, j\le p}$, with

$$L_{i,\,j} = \begin{cases} D_i, & \text{if } i = j, \\ -x_{i,\,j}, & \text{if } i \ne j. \end{cases}$$

Let $Sp(K_p)$ denote the set of spanning trees of K_p. For any given index i, we can consider a $T \in Sp(K_p)$ as being *rooted* at vertex i. This simply gives an orientation to each edge $e = \{r, s\}$ of T by orienting it from r to s if and only if s is closer to the root than r in T. Define the weight of $e \in T$ by $w_i(e) = x_{r,s}$ and the weight of T itself by

$$w_i(T) = \prod_{e \in T} w_i(e).$$

Then any cofactor $c_{i,j}$ of an element in the i-th row of $\mathbf{L}_p$ is identical and evaluates to

$$c_{i,j} = \sum_{T \in Sp(K_p)} w_i(T). \tag{2.6}$$

This is the content of the weighted generalization of Kirchoff's matrix-tree theorem. Suppose we specialize each $x_{r,s}$, $r \neq s$ to a numerical value such that the resulting matrix is symmetric (i.e, $x_{r,s}$ and $x_{s,r}$ are assigned the same value). Given a $T \in Sp(K_p)$, $w_i(T)$ then specializes to a fixed value independent of i since the symmetry of the matrix implies that either edge orientation results in the same numerical weight for the edge. Therefore, the sum in (2.6) evaluates to the same quantity independently of i, j. ∎

Since $c_{1,j} = \det \mathbf{C}_p$ for all j, we have proved

Lemma 2.4.

$$H_p(x) = \det \mathbf{C}_p \sum_{j=1}^{p} a_j(x).$$

Note that

$$\sum_{j=1}^{p} a_j(x) = \sum_{k=0}^{p-1} b_k x^k,$$

where b_k is given in (1.2). Next we evaluate $\det \mathbf{C}_p$.

Lemma 2.5.

$$\det \mathbf{C}_p = (-1)^{\frac{p-1}{2}} p^{\frac{p-3}{2}}. \tag{2.7}$$

Proof. Let $\mathbf{E}_p$ denote the $p \times p$ exchange matrix which has 1's along the anti-diagonal and 0's elsewhere. Clearly,

$$\det \mathbf{E}_p = (-1)^{\frac{p(p-1)}{2}}.$$

Let $\mathbf{B}_p = \mathbf{C}_p \mathbf{E}_p$. Then

$$\mathbf{B}_p = \left[\left(\frac{i-j}{p} \right) \right]_{1 \leq i,j \leq p-1}$$

and

$$\det \mathbf{C}_p = (-1)^{\frac{p-1}{2}} \det \mathbf{B}_p. \tag{2.8}$$

Note that $\mathbf{B}_p$ is symmetric for $p \equiv 1 \pmod 4$ and skew-symmetric for $p \equiv 3 \pmod 4$.

We determine the spectrum of $\mathbf{B}_p$, and compute $\det \mathbf{B}_p$ as the product of its eigenvalues. This results in the evaluation of $\det \mathbf{C}_p$ that we need through (2.8).

Let $I = \sqrt{-1}$ and $\zeta = e^{\frac{2\pi I}{p}}$ denote a primitive p-th root of unity. For $1 \le r \le p-1$, consider the Gauss sum

$$g_r = \sum_{j=0}^{p-1} \left(\frac{j}{p}\right) \zeta^{rj}.$$

Then

$$g_r = \begin{cases} \left(\frac{r}{p}\right)\sqrt{p}, & \text{if } p \equiv 1 \pmod 4, \\ I\left(\frac{r}{p}\right)\sqrt{p}, & \text{if } p \equiv 3 \pmod 4. \end{cases} \tag{2.9}$$

A proof of Gauss's evaluation of g_r can be found in [6]. Changing the summation index, we can write

$$g_r = \sum_{j=0}^{p-1} \left(\frac{i-j}{p}\right) \zeta^{r(i-j)}. \tag{2.10}$$

We will give the details of the proof for primes of the form $p \equiv 1 \pmod 4$. The proof for primes $p \equiv 3 \pmod 4$ is similar.

For $p \equiv 1 \pmod 4$, $\frac{p-1}{2}$ is even, and $\det \mathbf{C}_p = \det \mathbf{B}_p$. Using (2.9) and (2.10), we have

$$\sum_{j=0}^{p-1} \left(\frac{i-j}{p}\right) \zeta^{-rj} = \left(\frac{r}{p}\right)\sqrt{p}\,\zeta^{-ri}$$

or

$$\left(\frac{i}{p}\right) + \sum_{j=1}^{p-1} \left(\frac{i-j}{p}\right) \zeta^{-rj} = \left(\frac{r}{p}\right)\sqrt{p}\,\zeta^{-ri}. \tag{2.11}$$

Equating the imaginary parts in identity (2.11),

$$\sum_{j=1}^{p-1} \left(\frac{i-j}{p}\right) \sin\frac{2\pi rj}{p} = \left(\frac{r}{p}\right)\sqrt{p}\,\sin\frac{2\pi ri}{p}.$$

Therefore, for every r which is not zero modulo p, the vector

$$u_r = \sum_{j=1}^{p-1} \left(\sin\frac{2\pi rj}{p}\right) \mathbf{e}_j^t$$

is an eigenvector of $\mathbf{B}_p$ corresponding to eigenvalue $\left(\frac{r}{p}\right)\sqrt{p}$. The vectors corresponding to r and $p-r$ differ only in sign. Therefore, if we let

$$T_1 = \left\{ u_r \;\middle|\; 1 \le r \le \frac{p-1}{2} \right\},$$

then exactly half of the $u_r \in T_1$ are eigenvectors of $\mathbf{B}_p$ corresponding to eigenvalue $\sqrt{p}$, and the other half are eigenvectors corresponding to the eigenvalue $-\sqrt{p}$. For $1 \le r \le s \le \frac{p-1}{2}$, we have the trigonometric identity

$$\sum_{j=1}^{p-1} \sin\frac{2\pi rj}{p} \sin\frac{2\pi sj}{p} = \begin{cases} 0, & \text{if } r < s, \\ \frac{p}{2}, & \text{if } r = s, \end{cases}$$

where the $r = s$ evaluation is a consequence of the general trigonometric identity

$$\sum_{j=1}^{n} \sin^2 jx = \frac{n}{2} - \frac{\cos(n+1)x \sin nx}{2 \sin x} \tag{2.12}$$

([4, p. 30]). Therefore, the $\frac{p-1}{2}$ eigenvectors in T_1 are orthogonal, and so linearly independent.

Next we obtain a set of $\frac{p-1}{2} - 2$ more eigenvectors of $\mathbf{B}_p$. Equating the real parts in identity (2.11), we obtain

$$\left(\frac{i}{p}\right) + \sum_{j=1}^{p-1} \left(\frac{i-j}{p}\right) \cos \frac{2\pi r j}{p} = \left(\frac{r}{p}\right) \sqrt{p} \cos \frac{2\pi r i}{p} \, . \tag{2.13}$$

Let

$$v_r = \sum_{j=1}^{p-1} \left(\cos \frac{2\pi r j}{p}\right) \mathbf{e}_j^t \, .$$

These are not themselves eigenvectors because of the extra term $\left(\frac{i}{p}\right)$ in identity (2.13). But the nonzero vectors of the form

$$v_r - v_s, \tag{2.14}$$

for $1 \le r < s \le p-1$, are eigenvectors of $\mathbf{B}_p$ as long as $\left(\frac{r}{p}\right) = \left(\frac{s}{p}\right)$. We will single out

$$\frac{p-1}{2} - 2$$

of these eigenvectors, half corresponding to the eigenvalue $\sqrt{p}$, and the other half to $-\sqrt{p}$. Let g be a generator of the multiplicative group $\mathbb{Z}_p^*$. Then $\left(\frac{g}{p}\right) = -1$. Put $h = g^4$. Since

$$1 = \left(\frac{1}{p}\right) = \left(\frac{h^k}{p}\right),$$

taking $r = 1$, the $\frac{p-1}{4} - 1$ vectors

$$v_1 - v_{h^k},$$

for $k = 1, 2, \ldots, \frac{p-1}{4} - 1$, are eigenvectors of $\mathbf{B}_p$ corresponding to the eigenvalue $\sqrt{p}$. Similarly,

$$-1 = \left(\frac{g}{p}\right) = \left(\frac{gh^k}{p}\right),$$

and taking $r = g$ in (2.14), the $\frac{p-1}{4} - 1$ vectors

$$v_g - v_{gh^k},$$

for $k = 1, 2, \ldots, \frac{p-1}{4} - 1$, are eigenvectors of $\mathbf{B}_p$ corresponding to the eigenvalue $-\sqrt{p}$. These eigenvectors are of the form

$$v_1 - v_{h^k} = \sum_{j=1}^{p-1} \left(\cos \frac{2\pi j}{p} - \cos \frac{2\pi h^k j}{p}\right) \mathbf{e}_j^t$$

in the first case, and

$$v_g - v_{gh^k} = \sum_{j=1}^{p-1} \left(\cos \frac{2\pi g j}{p} - \cos \frac{2\pi g h^k j}{p} \right) \mathbf{e}_j^t$$

in the second. Let

$$T_2 = \left\{ v_1 - v_{h^k} \;\middle|\; k = 1, 2, \ldots, \frac{p-1}{4} - 1 \right\} \cup \left\{ v_g - v_{gh^k} \;\middle|\; k = 1, 2, \ldots, \frac{p-1}{4} - 1 \right\}.$$

Finally, consider the two vectors

$$w_1 = \sum_{j=1}^{p-1} \frac{1}{2} \left(1 - \left(\frac{j}{p} \right) \right) \mathbf{e}_j^t,$$

$$w_2 = \sum_{j=1}^{p-1} \frac{1}{2} \left(1 + \left(\frac{j}{p} \right) \right) \mathbf{e}_j^t .$$

Thus w_1 is a 0–1 vector with a 1 for every index for which the row sum of $\mathbf{B}_p$ is 1. Similarly, w_2 is a 0–1 vector with a 1 for every index for which the row sum of $\mathbf{B}_p$ is -1.

The fact that w_1 is an eigenvalue of $\mathbf{C}_p$ (and also of $\mathbf{B}_p$) is a consequence of the identity

$$\sum_{\substack{j=1 \\ \left(\frac{j}{p}\right)=-1}}^{p-1} \left(\frac{i+j}{p} \right) = \begin{cases} 0, & \text{if } \left(\dfrac{i}{p} \right) = 1, \\ 1, & \text{if } \left(\dfrac{i}{p} \right) = -1. \end{cases}$$

To prove this identity, write it in the form

$$\sum_{j=1}^{p-1} \left(\frac{i+j}{p} \right) \frac{1}{2} \left(1 - \left(\frac{j}{p} \right) \right) = \frac{1}{2} \left(1 - \left(\frac{i}{p} \right) \right).$$

In this latter form, the identity can be proved by expanding the left hand side and making use of

$$\sum_{j=0}^{p-1} \left(\frac{i+j}{p} \right) \left(\frac{j}{p} \right) = -1,$$

which holds for $p \nmid i$ from the general orthogonality condition

$$\sum_{k=0}^{p-1} \left(\frac{i+k}{p} \right) \left(\frac{j+k}{p} \right) = \begin{cases} p-1, & \text{if } i = j, \\ -1, & \text{if } i \neq j. \end{cases} \tag{2.15}$$

For $\mathbf{B}_p$, we obtain

$$\sum_{j=1}^{p-1} \left(\frac{i-j}{p} \right) \frac{1}{2} \left(1 - \left(\frac{j}{p} \right) \right) = \frac{1}{2} \left(1 - \left(\frac{i}{p} \right) \right),$$

so that w_1 is an eigenvector of $\mathbf{B}_p$ corresponding to eigenvalue 1. Similarly, w_2 is an eigenvector of $\mathbf{B}_p$ corresponding to eigenvalue -1. Putting

$$T_3 = \{w_1, w_2\},$$

we have $p-1$ eigenvectors in

$$T_1 \cup T_2 \cup T_3$$

with $\frac{p-2}{2}$ corresponding to eigenvalue $\sqrt{p}$, $\frac{p-2}{2}$ corresponding to eigenvalue $-\sqrt{p}$, and one each for the eigenvalues ± 1. To show that there is no linear dependence among these vectors, we proceed to show that any two vectors $u, v \in T_1 \cup T_2 \cup T_3$ are orthogonal. We have already done this for $u, v \in T_1$. For $u, v \in T_2$, we need to show

$$\sum_{j=1}^{p-1} \left(\cos\frac{2\pi j}{p} - \cos\frac{2\pi h^r j}{p} \right) \left(\cos\frac{2\pi j}{p} - \cos\frac{2\pi h^s j}{p} \right) = 0,$$

$$\sum_{j=1}^{p-1} \left(\cos\frac{2\pi g j}{p} - \cos\frac{2\pi g h^r j}{p} \right) \left(\cos\frac{2\pi g j}{p} - \cos\frac{2\pi g h^s j}{p} \right) = 0,$$

$$\sum_{j=1}^{p-1} \left(\cos\frac{2\pi j}{p} - \cos\frac{2\pi h^r j}{p} \right) \left(\cos\frac{2\pi g j}{p} - \cos\frac{2\pi g h^s j}{p} \right) = 0,$$

for $r \not\equiv s \pmod{p}$.

These identities follow from

$$\sum_{j=1}^{n-1} \cos\frac{2\pi r j}{n} \cos\frac{2\pi s j}{n} = \begin{cases} -1, & \text{if } s \neq r, n-r, \\ n-1, & \text{if } s = r = \frac{n}{2}, \\ \frac{n-2}{2}, & \text{if } s = 1, n-r, \end{cases}$$

which holds for $1 \leq r \leq s \leq n-1$, and generalizes the twin identity to (2.12)

$$\sum_{j=1}^{n} \cos^2 jx = \frac{n-1}{2} + \frac{1}{2} \cos nx \sin(n+1)x \csc x$$

([4, p. 31]).

To prove that the vectors in T_1 are orthogonal to the vectors in T_2, we use the orthogonality relations

$$\sum_{j=1}^{n-1} \cos\frac{2\pi r j}{n} \sin\frac{2\pi s j}{n} = 0,$$

valid for all integral r, s, n.

Finally, below are the identities that are needed to prove that the vectors in T_3 are orthogonal to vectors in T_1 and T_2. If p is a prime of the form $4k+1$, then

$$\sum_{\substack{j=1 \\ (\frac{j}{p})=1}}^{p-1} \sin\frac{2\pi r j}{p} = 0, \tag{2.16}$$

for any r, and

$$\sum_{\substack{j=1 \\ \left(\frac{j}{p}\right)=1}}^{p-1} \cos\frac{2\pi rj}{p} = \frac{-1+\left(\frac{r}{p}\right)\sqrt{p}}{2} \tag{2.17}$$

and

$$\sum_{\substack{j=1 \\ \left(\frac{j}{p}\right)=-1}}^{p-1} \cos\frac{2\pi rj}{p} = \frac{-1-\left(\frac{r}{p}\right)\sqrt{p}}{2}. \tag{2.18}$$

The first one of these can be written as

$$\sum_{j=1}^{p-1} \frac{1}{2}\left(1+\left(\frac{j}{p}\right)\right)\sin\frac{2\pi rj}{p} = 0.$$

Clearly,

$$\sum_{j=1}^{p-1} \sin\frac{2\pi rj}{p} = 0$$

by looking at sin as the imaginary part of ζ and summing the geometric series in ζ. Therefore, to prove identity (2.16), it is enough to prove

$$\sum_{j=1}^{p-1} \left(\frac{j}{p}\right)\sin\frac{2\pi rj}{p} = 0,$$

which is an immediate consequence of the evaluation of the Gauss sum by equating the imaginary parts.

The Identities (2.17) and (2.18) are obtained by evaluating

$$\sum_{j=1}^{p-1} \frac{1}{2}\left(1\pm\left(\frac{j}{p}\right)\right)\cos\frac{2\pi rj}{p},$$

again by making use of the evaluation of Gauss sums. We sum the geometric series in ζ and equate the real parts.

Therefore, the spectrum of $\mathbf{B}_p$ consists of $\pm 1, \pm\sqrt{p}$ where 1 and -1 each has multiplicity one, and $\sqrt{p}$ and $-\sqrt{p}$ each has multiplicity $\frac{p-1}{2}-1$. This gives

$$\det\mathbf{B}_p = (-1)^{\frac{p-1}{2}} p^{\frac{p-3}{2}}.$$

This completes the proof of Lemma 2.5. ∎

I am grateful to the anonymous referee who suggested an alternate, and somewhat more economical proof of Lemma 2.5. I would like to sketch this approach here. Let

$$\mathbf{D}_p = \left[\left(\frac{i-j}{p}\right)\right]_{1\le i,j\le p}.$$

We can view $\mathbf{B}_p$ as a submatrix of $\mathbf{D}_p$ obtained by deleting the first row and column of $\mathbf{D}_p$. $\mathbf{D}_p$ is a circulant matrix, and therefore it has a basis of eigenvectors consisting of the $\left(1, \zeta^r, \zeta^{2r}, \ldots, \zeta^{(p-1)r}\right)$. The eigenvalues are g_r: $(p-1)/2$ of them equal g_1, $(p-1)/2$ of them equal $-g_1$ and also $g_0 = 0$ must be included. If we have an eigenvector of $\mathbf{D}_p$ with first entry zero, deleting that zero gives an eigenvector of $\mathbf{B}_p$ with the same eigenvalue. Taking differences of the above basis elements gives $(p-3)/2$ independent eigenvectors of $\mathbf{B}_p$ with eigenvalue g_1, and $(p-3)/2$ with eigenvalue $-g_1$. This accounts for all but two eigenvectors of $\mathbf{B}_p$, and these two are w_1 and w_2.

Remark 2.6. For $p \equiv 3 \pmod 4$, the spectrum of $\mathbf{B}_p$ consists of $\pm I, \pm I\sqrt{p}$ where I and $-I$ each has multiplicity one, and $I\sqrt{p}$ and $-I\sqrt{p}$ each has multiplicity $\frac{p-1}{2} - 1$. In this case $\mathbf{B}_p$ is skew-symmetric, so the determinant is non-negative.

3. Special Values

We can obtain factors of $H_p(x)$ by finding zeros of

$$\sum_{k=0}^{p-1} b_k x^k, \tag{3.1}$$

where b_k is given in (1.2).

Lemma 3.1. *For any p,* $x^2 \,|\, H_p(x)$.

Proof. It is easy to see that for any odd prime, $b_0 = b_1 = 0$. Therefore, $H_p(x)$ is divisible by x^2. ∎

Next we consider the case $p \equiv 1 \pmod 4$.

Lemma 3.2. *If* $p \equiv 1 \pmod 4$, *then we also have* $\left(x^2 - 1\right) \,|\, H_p(x)$.

Proof. The polynomial (3.1) evaluated at $x = 1$ and $x = -1$ are

$$\sum_{k=1}^{p} \sum_{m=0}^{k} \left(\frac{k-m}{p}\right),$$

$$\sum_{k=1}^{p} \sum_{m=0}^{k} \left(\frac{k-m}{p}\right) (-1)^m, \tag{3.2}$$

respectively. We will show that both of these evaluate to 0. Rearranging the first sum,

$$\sum_{k=1}^{p} \sum_{m=0}^{k} \left(\frac{k-m}{p}\right) = \sum_{m=1}^{p-1} (p-m+1) \left(\frac{m}{p}\right).$$

Therefore, it suffices to show that

$$\sum_{m=1}^{p-1} m \left(\frac{m}{p}\right) = 0, \tag{3.3}$$

i.e., the sum of the quadratic residues minus the sum of the quadratic nonresidues mod p vanishes. Since

$$\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}} = 1,$$

the map $m \mapsto p - m$ permutes the quadratic residues among themselves, and the nonresidues among themselves. Since each of these sets has an even number of elements for $p \equiv 1 \pmod 4$, this map has no fixed points. Therefore, both the residues and the nonresidues mod p sum to

$$\frac{(p-1)}{4}p,$$

and (3.3) follows. The second sum in (3.2) can be rearranged as

$$\sum_{m=1}^{\frac{p-1}{2}} \left(\frac{2m-1}{p}\right) = -(-1)^{\frac{p^2-1}{8}} \sum_{m=1}^{\frac{p-1}{2}} \left(\frac{m}{p}\right), \tag{3.4}$$

and in this case the map $m \mapsto p - m$ shows that there are equally many residues mod p in the range $\left\{1, 2, \ldots, \frac{p-1}{2}\right\}$ as in the range $\left\{\frac{p-1}{2} + 1, \ldots, p-1\right\}$. A similar statement holds for nonresidues. Therefore, the right hand side of (3.4) is zero and $H_p(x)$ is divisible by $x^2 - 1$ for $p \equiv 1 \pmod 4$. ∎

Note that the elementary arguments we gave for the proof of the evaluations in Lemma 3.2 can directly be obtained from the following result (see [9], also [3]):

Proposition 3.3. *Let p be an odd prime and suppose F is a complex-valued function defined on the integers, which is periodic with period p. Then*

$$\sum_{j=0}^{p-1} F(j) + \sum_{j=0}^{p-1} \left(\frac{j}{p}\right) F(j) = \sum_{j=0}^{p-1} F\left(j^2\right).$$

Finally, we remark that the coefficients of the quotient polynomials

$$\frac{(-1)^{\frac{p-1}{2}} H_p(x)}{p^{\frac{p-3}{2}} x^2} \quad \text{and} \quad \frac{(-1)^{\frac{p-1}{2}} H_p(x)}{p^{\frac{p-3}{2}} x^2 \left(x^2 - 1\right)}$$

over $\mathbb{Z}[x]$ can be written in terms of the partial sums b_k. For $p \equiv 3 \pmod 4$ these coefficients are simply b_{k+2}. For $p \equiv 1 \pmod 4$ the coefficients are partial sums of odd or even indexed b_i, depending on the parity of k.

Acknowledgment. I would like to thank the anonymous referee who suggested an alternate proof of Lemma 2.5 and whose comments greatly improved the presentation of this paper.

References

1. Borevich, Z.I., Shafarevich, I.R.: Number Theory. Academic Press, New York-London (1966)
2. Chapman, R.: Determinants of Legendre symbol matrices. Acta Arith. 115(3), 231–244 (2004)

3. Davenport, H.: On certain exponential sums. J. Reine Angew. Math. 169, 158–176 (1933)
4. Gradshteyn, I.S., Ryzhik, I.M.: Table of Integrals, Series, and Products. Academic Press, Orlando (1980)
5. Hardy, G.H., Wright, E.M.: An Introduction to the Theory of Numbers. Oxford University Press, New York (1980)
6. Ireland, K., Rosen, M.: A Classical Introduction to Modern Number Theory. Springer-Verlag, New York (1990)
7. Moon, J.W.: Counting Labelled Trees. Canadian Mathematical Congress, Montreal, Que. (1970)
8. Stanley, R.P.: Enumerative Combinatorics, Volume 2. Cambridge University Press, Cambridge (1999)
9. Williams, K.S.: Finite transformation formulae involving the Legendre symbol. Pacific J. Math. 34, 559–568 (1970)