# Jacobi Sum Matrices

**Sam Vandervelde**

**Abstract.** In this article we identify several beautiful properties of Jacobi sums that become evident when these numbers are organized as a matrix and studied via the tools of linear algebra. In the process we reconsider a convention employed in computing Jacobi sum values by illustrating how these properties become less elegant or disappear entirely when the standard definition for Jacobi sums is utilized. We conclude with a conjecture regarding polynomials that factor in an unexpected manner.

**1. JACOBI SUMS.** Carl Jacobi's formidable mathematical legacy includes such contributions as the Jacobi triple product, the Jacobi symbol, the Jacobi elliptic functions with associated Jacobi amplitudes, and the Jacobian in the change of variables theorem, to but scratch the surface. Among his many discoveries, Jacobi sums stand out as one of the most brilliant gems. Very informally, a Jacobi sum adds together certain roots of unity in a manner prescribed by the arithmetic structure of the finite field on which it is based. (We will supply a precise definition momentarily.) For a given finite field a Jacobi sum depends on two parameters, so it is natural to assemble these values into a matrix. We have done so below for the Jacobi sums arising from the field with eight elements. We invite the reader to study this collection of numbers and identify as many properties as are readily apparent.

$$\begin{pmatrix} 6 & -1 & -1 & -1 & -1 & -1 & -1 \\ -1 & -1+i\sqrt{7} & \frac{5}{2}-\frac{1}{2}i\sqrt{7} & -1-i\sqrt{7} & \frac{5}{2}-\frac{1}{2}i\sqrt{7} & -1+i\sqrt{7} & -1 \\ -1 & \frac{5}{2}-\frac{1}{2}i\sqrt{7} & -1+i\sqrt{7} & -1+i\sqrt{7} & \frac{5}{2}-\frac{1}{2}i\sqrt{7} & -1 & -1-i\sqrt{7} \\ -1 & -1-i\sqrt{7} & -1+i\sqrt{7} & -1-i\sqrt{7} & -1 & \frac{5}{2}+\frac{1}{2}i\sqrt{7} & \frac{5}{2}+\frac{1}{2}i\sqrt{7} \\ -1 & \frac{5}{2}-\frac{1}{2}i\sqrt{7} & \frac{5}{2}-\frac{1}{2}i\sqrt{7} & -1 & -1+i\sqrt{7} & -1-i\sqrt{7} & -1+i\sqrt{7} \\ -1 & -1+i\sqrt{7} & -1 & \frac{5}{2}+\frac{1}{2}i\sqrt{7} & -1-i\sqrt{7} & -1-i\sqrt{7} & \frac{5}{2}+\frac{1}{2}i\sqrt{7} \\ -1 & -1 & -1-i\sqrt{7} & \frac{5}{2}+\frac{1}{2}i\sqrt{7} & -1+i\sqrt{7} & \frac{5}{2}+\frac{1}{2}i\sqrt{7} & -1-i\sqrt{7} \end{pmatrix} \quad (1)$$

Before enumerating the standard properties of Jacobi sums we offer a modest background on their development and applications. According to **[2]** Jacobi first proposed these sums as mathematical objects worthy of study in a letter mailed to Gauss in 1827. Ten years later he published his findings, with extensions of his work provided soon after by Cauchy, Gauss, and Eisenstein. It is interesting to note that while Gauss sums will suffice for a proof of quadratic reciprocity, a demonstration of cubic reciprocity along similar lines requires a foray into the realm of Jacobi sums; Eisenstein formulated a generalization of Jacobi sums (see **[3]**) in order to prove biquadratic reciprocity. As shown in **[5]**, Jacobi sums may be used to estimate the number of integral solutions

to congruences such as $x^3 + y^3 \equiv 1 \bmod p$. These estimates played an important role in the development of the Weil conjectures [**6**]. Jacobi sums were also employed by Adleman, Pomerance, and Rumely [**1**] for primality testing.

Although Jacobi sums have been around for a long time, several of the results presented below seem to have gone unnoticed. We suspect this has to do in part with the fact that the usual definition of Jacobi sums differs slightly from the one we use. Conventional wisdom would have us forego the 6 in the upper left corner of (1) in favor of an 8 and replace each $-1$ along the top row and left column by a 0. However, some of the most compelling features of Jacobi sum matrices evaporate when the standard definition is used. Therefore one of our purposes in presenting these results is to suggest that this alternative warrants serious consideration as the "primary" definition, at least in the setting of finite fields. To be fair, the version of Jacobi sums we study does appear in the literature: e.g., in [**2, Section 2.5**], which discusses the relationship between Jacobi sums and cyclotomic numbers.

**2. PRELIMINARIES.** Recall that there exists a finite field $\mathbb{F}_q$ with $q$ elements if and only if $q = p^r$ is a power of a prime, and such a field is unique up to isomorphism. We shall not require any specialized knowledge of finite fields beyond the fact that the multiplicative group $\mathbb{F}_q^*$ of nonzero elements forms a cyclic group of order $q - 1$. The quantity $q - 1$ appears throughout our discussion, so we set $m = q - 1$ from here on. Thus $\mathbb{F}_q^*$ has $m$ elements.

Fix a generator $g$ of $\mathbb{F}_q^*$ and let $\xi = e^{2\pi i/m}$. The function $\chi$ defined by $\chi(g^k) = \xi^k$ for $1 \le k \le m$ is an example of a multiplicative character on $\mathbb{F}_q^*$; that is, a function $\chi : \mathbb{F}_q^* \to \mathbb{C}$ satisfying

$$\chi(1) = 1, \qquad \chi(uv) = \chi(u)\chi(v), \quad u, v \in \mathbb{F}_q^*. \tag{2}$$

We use an $m$th root of unity since $(\chi(g))^m = \chi(g^m) = \chi(1) = 1$. As the reader may verify, there are precisely $m$ multiplicative characters on $\mathbb{F}_q^*$, namely $\chi$, $\chi^2$, $\ldots$, $\chi^m$, where $\chi^a(g^k) = (\chi(g^k))^a = \xi^{ak}$ as one would expect. Note that $\chi^m(g^k) = 1$ for all $k$, so we call $\chi^m$ the trivial character. It follows that the value of the exponent $a$ only matters mod $m$. In particular, the inverse of $\chi^a$ (which is also the complex conjugate) may be written either as $\chi^{-a}$ or as $\chi^{m-a}$. By the same token, we will usually write the trivial character as $\chi^0$.

To define a Jacobi sum it is necessary to extend each character $\chi^a$ to all of $\mathbb{F}_q$ by defining $\chi^a(0)$. The multiplicative condition forces $\chi^a(0) = 0$ whenever $1 \le a < m$. But for the trivial character a seemingly arbitrary choice[1] must be made, since taking either $\chi^0(0) = 0$ or $\chi^0(0) = 1$ satisfies (2). Convention dicates that we declare $\chi^0(0) = 1$ for the trivial character. However, we opt for setting $\chi^a(0) = 0$ for all $a$. As the opportunity arises we will point out the ramifications of this choice. Properties of roots of unity now imply that

$$\sum_{u \in \mathbb{F}_q} \chi^a(u) = 0, \quad 1 \le a < m, \qquad \sum_{u \in \mathbb{F}_q} \chi^0(u) = q - 1 = m. \tag{3}$$

(One rationale behind taking $\chi^0(0) = 1$ is presumably rooted in the fact that the latter sum would come to $q$ rather than $q - 1$, giving a more pleasing value.)

[1]Ireland and Rosen explain that Jacobi sums arise when counting solutions to equations over $\mathbb{F}_p$. In this context $\chi^0(0)$ tallies solutions to $x^e = 0$, which would seem to motivate the value $\chi^0(0) = 1$. However, one might also argue that the zero solution should not be included since the equations are homogenous, leading to $\chi^0(0) = 0$ instead.

A Jacobi sum takes as its arguments a pair of multiplicative characters on a given finite field and returns a complex number:

$$J_q(\chi^a, \chi^b) \;=\; \sum_{u \in \mathbb{F}_q} \chi^a(u)\chi^b(1-u) \;=\; \sum_{\substack{u,v \in \mathbb{F}_q \\ u+v=1}} \chi^a(u)\chi^b(v). \tag{4}$$

The middle expression is more utilitarian, while the final one highlights the symmetry in the definition. When the field $\mathbb{F}_q$ is clear we will drop the subscript $q$. We will also often omit $\chi$ and refer to a particular Jacobi sum simply as $J(a, b)$. Because the terms of the sum corresponding to $u = 0$ and $u = 1$ always vanish, we may write

$$J(a, b) \;=\; \sum_{u \neq 0,1} \chi^a(u)\chi^b(1-u), \tag{5}$$

where it is understood that the sum is over $u \in \mathbb{F}_q$. Thus a Jacobi sum adds together $q - 2$ not necessarily distinct $m$th roots of unity.

In a marvelous manner this sum plays the additive and multiplicative structures of the field off one another, yielding a collection of numbers with extraordinary properties. To illustrate how these numbers are computed we return to matrix (1), which catalogs the values $J_8(\chi^a, \chi^b)$ for $0 \leq a, b \leq 6$ for a particular generator $g$ of $\mathbb{F}_8^*$. (For aesthetic reasons we begin numbering rows and columns of this matrix at 0.) The generator $g$ of $\mathbb{F}_8^*$ chosen satisfies

$$g^1 + g^3 = 1, \qquad g^2 + g^6 = 1, \qquad g^4 + g^5 = 1, \qquad g^7 + 0 = 1. \tag{6}$$

Letting $\xi = e^{2\pi i/7}$ we may now calculate, for instance,

$$\begin{aligned} J(1,2) &= \chi(g)\chi^2(1-g) + \chi(g^2)\chi^2(1-g^2) + \cdots + \chi(g^6)\chi^2(1-g^6) \\ &= \chi(g)\chi^2(g^3) + \chi(g^2)\chi^2(g^6) + \cdots + \chi(g^6)\chi^2(g^2) \\ &= \chi(g^7) + \chi(g^{14}) + \chi(g^5) + \chi(g^{14}) + \chi(g^{13}) + \chi(g^{10}) \\ &= \xi^7 + \xi^{14} + \xi^5 + \xi^{14} + \xi^{13} + \xi^{10} \\ &= 1 + 1 + \xi^5 + 1 + \xi^6 + \xi^3 \\ &= \tfrac{5}{2} - \tfrac{1}{2}i\sqrt{7}, \end{aligned} \tag{7}$$

which explains the entry in row 1, column 2 of (1). For $1 \leq a \leq 6$ we find

$$\begin{aligned} J(a,0) &= \chi^a(g)\chi^0(1-g) + \chi^a(g^2)\chi^0(1-g^2) + \cdots + \chi^a(g^6)\chi^0(1-g^6) \\ &= \chi^a(g) + \chi^a(g^2) + \cdots + \chi^a(g^6) \\ &= -\chi^a(g^7) \\ &= -1, \end{aligned} \tag{8}$$

where the penultimate step follows from (3). If we had employed the conventional value for $\chi^0(0)$ the term $\chi^a(g^7)$ would also appear in the sum, giving a total of 0 instead. By way of further orientation the reader is encouraged to confirm that $J(5, 1) = -1 + i\sqrt{7}$ and that $J(3, 4) = -1$.

A cursory examination shows that matrix (1) is symmetric, that the top left entry equals $q-2$, and that the remaining entries along the top row, the left column, and the secondary diagonal are $-1$. Slightly less obvious is the fact that all other entries have an absolute value of $\sqrt{8}$. The sum of the entries along the top row is 0; a quick check reveals the same is true for every row and column. We summarize these properties below without proof. (One may consult **[5]** for details.)

**Proposition 1** *Fix a generator $g$ of $\mathbb{F}_q^*$, let $\chi(g^k) = \xi^k$ with $\xi = e^{2\pi i/m}$ be the corresponding character, take $\chi^a(0) = 0$ for all $a$, and abbreviate $J_q(\chi^a, \chi^b)$ to $J(a,b)$. Then for $0 \le a, b \le m-1$ we have*

*i.* $J(a,b) = J(b,a)$,

*ii.* $J(0,0) = q-2$,

*iii.* $J(a,0) = J(0,b) = -1$ *when* $a, b \neq 0$,

*iv.* $J(a, m-a) = -\chi^a(-1)$,

*v.* $|J(a,b)|^2 = q$ *when* $a, b \neq 0$ *and* $a+b \neq m$,

*vi.* $\sum_{k=0}^{m-1} J(a,k) = \sum_{k=0}^{m-1} J(k,b) = 0$.

Observe that $|J(a,b)+1|^2$ and $|J(a,b)+8|^2$ are either 0 or of the form $2^r 7^s$ with $r, s \in \mathbb{N}$ for every entry of (1). In general the quantities $J_q(a,b)+1$ and $J_q(a,b)+q$ satisfy interesting congruences. We also remark that all the results presented here continue to be valid regardless of the generator $g$ of $\mathbb{F}_q^*$ used to define $\chi$. The value of $J_q(\chi^{as}, \chi^{bs})$ obtained by using the generator $g^s$ is identical to that of $J_q(\chi^a, \chi^b)$ using the original generator $g$, so altering the generator only permutes the rows and columns of a Jacobi sum matrix in a symmetric fashion.

**3. EIGENVALUES.** Thus far our discussion has focused on properties of Jacobi sums taken individually. However, we are primarily interested in what can be said about the set of all Jacobi sum values for a particular finite field, viewed collectively as a matrix. It may have occurred to the curious individual to calculate the eigenvalues of matrix (1). We are rewarded for our efforts upon finding that its characteristic polynomial factors as

$$p(x) = -x(x-7)^2(x-7\omega)^2(x-7\overline{\omega})^2, \tag{9}$$

where $\omega = e^{2\pi i/3}$. One might speculate that cube roots of unity make an appearance since we used characters of $\mathbb{F}_8$, and $8 = 2^3$. But in fact the same phenomenon occurs for every value of $q$. This is explained by the fact that powers of these matrices (suitably scaled) cycle with period three, a property that depends on using the nonstandard value for $\chi^0(0)$.

**Theorem 1** *Defining $J(a,b)$ as in Proposition 1, let $B$ be the $m \times m$ matrix with entries $J(a,b)$ for $0 \le a, b \le m-1$. Then the powers of $B$ satisfy*

*i.* $B^2 = m\overline{B}$,

*ii.* $B^3 = m^3 I - m^2 U$,

*iii.* $B^n = m^3 B^{n-3}$ *for* $n \ge 4$,

*where $I$ is the $m \times m$ identity matrix and $U$ is the matrix all of whose entries are 1.*

*Proof.* The first claim is equivalent to the assertion that

$$\sum_{k=0}^{m-1} J(a,k)J(k,b) = m\overline{J(a,b)} \tag{10}$$

for all $a$ and $b$. Using definition (5) for $J(a,b)$ we expand the left-hand side as

$$\sum_{k=0}^{m-1}\left(\sum_{u\neq 0,1}\chi^a(u)\chi^k(1-u)\right)\left(\sum_{v\neq 0,1}\chi^k(v)\chi^b(1-v)\right). \tag{11}$$

It is a standard opening gambit in these sorts of proofs to move the summation over $k$ to the inside and then use the fact that $\sum_{k=0}^{m-1}\chi^k(u)=0$ unless $u=1$, in which case the sum equals $m$. (It is this feature of characters that make them useful for counting arguments.) Employing this strategy leads to

$$\sum_{u\neq 0,1}\sum_{v\neq 0,1}\chi^a(u)\chi^b(1-v)\sum_{k=0}^{m-1}\chi^k((1-u)v). \tag{12}$$

The final sum vanishes unless $(1-u)v=1$, or $u=1-\frac{1}{v}$. Hence our expression reduces to

$$m\sum_{v\neq 0,1}\chi^a\left(1-\frac{1}{v}\right)\chi^b(1-v)=m\sum_{v\neq 0,1}\chi^{-a}\left(\frac{v}{v-1}\right)\chi^{-b}\left(\frac{1}{1-v}\right), \tag{13}$$

where we have used $\chi^a(u)=\chi^{-a}(\frac{1}{u})$. Next observe that $\overline{J(a,b)}=J(-a,-b)$ since $\overline{\chi^a}=\chi^{-a}$; we introduced negative exponents in anticipation of this fact. And now in a beautiful stroke we realize that $\frac{v}{v-1}+\frac{1}{1-v}=1$, and as $v$ runs through all elements of $\mathbb{F}_q$ other than 0 and 1 so does $\frac{v}{v-1}$. Hence the right-hand side of (13) is precisely the sum defining $J(-a,-b)$, thus proving the first part.

With this result in hand the second part will follow once we show $B\overline{B}=m^2I-mU$. This is equivalent to demonstrating that

$$\sum_{k=0}^{m-1}J(a,k)\overline{J(k,b)}=\begin{cases} m^2-m & a=b \\ -m & a\neq b. \end{cases} \tag{14}$$

The same ingredients are needed as above (but without negative exponents at the end), so we omit the proof in favor of permitting the reader to supply the steps. There are no major surprises along the way, and the explanation is quite satisfying.

The final claim is an immediate consequence of the second part. For $n\geq 4$ we compute

$$B^n=B^{n-4}B(m^3I-m^2U)=m^3B^{n-3}, \tag{15}$$

where we have used the fact that $BU$ is the zero matrix because the entries within each row of $B$ sum to 0. This completes the proof. ■

**Corollary 1** *If $\lambda$ is an eigenvalue of a Jacobi sum matrix $B$ then $\lambda\in\{0,m,m\omega,m\overline{\omega}\}$, where $\omega=e^{2\pi i/3}$.*

*Proof.* Suppose that $Bv=\lambda v$ for some nonzero vector $v$. Then multiplying $B^4=m^3B$ on the right by $v$ yields $\lambda^4v=m^3\lambda v$. Therefore $\lambda^4=m^3\lambda$ since $v\neq 0$, which implies that $\lambda\in\{0,m,m\omega,m\overline{\omega}\}$. ■

**Corollary 2** *Every Jacobi sum matrix $B$ has an orthogonal basis of eigenvectors.*

*Proof.* Since $B$ is symmetric its conjugate transpose $B^*$ is just $\overline{B}$. But $\overline{B}$ is a scalar multiple of $B^2$, so we deduce that $B$ and $B^*$ commute, and hence $B$ is normal. The assertion now follows from well-known properties of normal matrices as furnished by [**4**], for instance. ■

The fact that the eigenspaces for $\lambda=7$, $7\omega$, and $7\overline{\omega}$ have the same dimension has probably not escaped notice. In general the eigenspaces are always as close in size as possible, a fact that depends upon ascertaining the traces of Jacobi sum matrices.

**Proposition 2** *The trace* $\mathrm{tr}(B)$ *of a Jacobi sum matrix* $B$ *is equal to* 0, $m$, *or* $2m$ *according to whether* $m-1 \equiv 0, 1,$ *or* 2 mod 3.

*Proof.* The values occurring along the main diagonal of $B$ are $J(a,a)$. Hence

$$\mathrm{tr}(B) = \sum_{a=0}^{m-1} J(a,a) = \sum_{a=0}^{m-1} \sum_{u \in \mathbb{F}_q} \chi^a(u)\chi^a(1-u) = \sum_{u \in \mathbb{F}_q} \sum_{a=0}^{m-1} \chi^a(u-u^2). \tag{16}$$

But the inner sum vanishes unless $u - u^2 = 1$, in which case its value is $m$. When $\mathbb{F}_q$ has characteristic 3 we find that $u = -1$ is a double root of the equation, while for other characteristics $u = -1$ is not a root. Since $(u^2 - u + 1)(u + 1) = u^3 + 1$, in these cases we seek values of $u$ with $u^3 = -1$ other than $u = -1$. For $m \equiv 0$ mod 3 there will be two such values, while for $m \equiv 1$ mod 3 there are no such values, because $\mathbb{F}_q^*$ is a cyclic group of order $m$. In summary, $u - u^2 = 1$ has one, two, or zero distinct roots when $m \equiv 2, 0, 1$ mod 3, as claimed. ∎

**Proposition 3** *The characteristic polynomial of a Jacobi sum matrix* $B$ *has the form*

$$p_B(x) = \pm x(x-m)^r(x-m\omega)^s(x-m\overline{\omega})^s \tag{17}$$

*for nonnegative integers* $r \geq s$ *satisfying* $r + 2s = m - 1$ *with* $r$ *as close to* $s$ *as possible.*

*Proof.* Clearly $p_B(x)$ is monic. Furthermore, the sign will be positive unless $m$ is odd; i.e., when $q = 2^r$. We will also see below that $\mathrm{rank}(B) = m-1$, giving the single factor of $x$. Now let us show that $p_B(x)$ has real coefficients, meaning that the eigenvalues $m\omega$ and $m\overline{\omega}$ occur in pairs. This follows from the relationship $J(m-a, m-b) = \overline{J(a,b)}$. In other words, swapping rows $a$ and $m-a$ as well as columns $b$ and $m-b$ for all $a$ and $b$ with $1 \leq a, b \leq \frac{m}{2}$ does not alter $p_B(x)$ but does conjugate every entry of $B$, and therefore $p_B(x)$ is real. The trace of $B$ is the sum of the eigenvalues, and each triple $m$, $m\omega$, $m\overline{\omega}$ will cancel. The result now follows from the fact that $\mathrm{tr}(B)$ is equal to 0, $m$, or $2m$. ∎

**4. RELATED MATRICES.** Observe that the list of eigenvalues for a Jacobi sum matrix constructed using the conventional definition is nearly identical to the list given by Proposition 3, the difference being that the eigenvalue $\lambda = 0$ is replaced by $\lambda = 1$ and a single occurrence of $\lambda = m$ changes to $\lambda = m + 1 = q$. This is a consequence of the close relationship in each case between the characteristic polynomial of the entire matrix and that of the lower right $(m-1) \times (m-1)$ submatrix of values they share.

**Lemma 1** *Let* $M$ *be an* $n \times n$ *matrix whose first column contains the entries* $c-1$, $-1$, $\ldots$, $-1$ *for some number* $c$, *as shown below, and such that the sum of the entries in each row of* $M$ *is 0. Let* $M'$ *be the* $(n-1) \times (n-1)$ *submatrix obtained by deleting the first row and column of* $M$. *Then the list of eigenvalues of* $M'$ *(with multiplicity) is given by removing the values* $\lambda = 0, c$ *from the list of eigenvalues for* $M$ *and including* $\lambda = 1$.

$$M = \begin{pmatrix} c-1 & \cdots & \\ -1 & & \\ \vdots & & M' \\ -1 & & \end{pmatrix} \tag{18}$$

*Proof.* Multiplying the first column of $M - xI$ by $(1-x)$ before taking the determinant yields

$$(1-x)\det(M-xI) = \begin{vmatrix} (c-1-x)(1-x) & \cdots & \\ x-1 & & \\ \vdots & & M'-xI' \\ x-1 & & \end{vmatrix}. \tag{19}$$

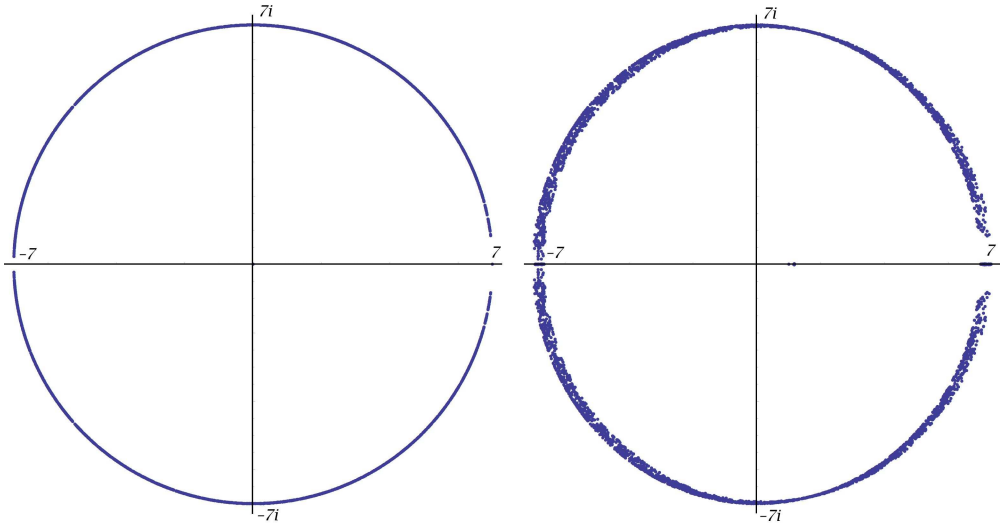


Figure 1: A plot of the roots of $\det(PB - xI)$ on the left and the roots of $\det(P\tilde{B} - xI)$ on the right for all $7 \times 7$ permutation matrices $P$.

We next add columns 2 through $n$ to the first column. Since the sum of the entries within each row of $M$ is zero this operation cancels every term in the first column below the top entry, which becomes

$$(c - 1 - x)(1 - x) + (1 - c) = x(x - c). \tag{20}$$

Therefore the value of the determinant may be rewritten as

$$(1 - x)\det(M - xI) = \begin{vmatrix} x(x-c) & \cdots \\ 0 & \\ \vdots & M' - xI' \\ 0 & \end{vmatrix} = x(x - c)\det(M' - xI'). \tag{21}$$

The assertion follows. ■

If $J_q(a, b)$ were computed in the traditional manner the top row of our Jacobi sum matrix would be $q$ followed by a row of 0's, so the list of eigenvalues would consist of those of the lower right submatrix, augmented by the value $\lambda = q$. Invoking the lemma now leads to the statement made above comparing lists of eigenvalues.

Purely to satisfy our curiosity, we now propose permuting the rows and columns of a Jacobi sum matrix $B$ before computing the eigenvalues. For example, take $B$ to equal matrix (1), let $P$ be any $7 \times 7$ permutation matrix, and consider the degree-seven polynomial $\det(PB - xI)$. Compiling the roots to all 5040 polynomials that arise in this manner produces a list with somewhat more than 3500 distinct complex numbers; locating them in the complex plane yields the scatterplot on the left in Figure 1. The roots, whose locations are marked by small solid discs, form a nearly unbroken chain along the circle of radius 7 centered at the origin, with discernible gaps located only near the real axis. By way of comparison, the related $7 \times 7$ matrix $\tilde{B}$ of conventional Jacobi sum values yields the right-hand plot in Figure 1. Put another way, matrix $B$ generates in excess of 3500 algebraic integers, each of degree 14 or less over $\mathbb{Q}$ and each having absolute value 7. As one might hope, this property is shared by all Jacobi

sum matrices. The following result was conjectured by the author and proved by Ron Evans (personal communication, Jan. 2011); we present this proof below.

**Proposition 4** *Let $B$ denote a Jacobi sum matrix for the finite field $\mathbb{F}_q$ and let $P$ be any $m \times m$ permutation matrix, where $m = q-1$. Then every nonzero eigenvalue $\lambda$ of the matrix $PB$ satisfies $|\lambda| = m$.*

*Proof.* Let $\lambda$ be a nonzero eigenvalue of $PB$, so that $PBv = \lambda v$ for some nonzero vector $v$. Letting $M^*$ denote the conjugate transpose of a matrix $M$, it follows that $(PBv)^*(PBv) = (\lambda v)^*(\lambda v)$. Expanding yields $v^*B^*P^*PBv = |\lambda|^2 v^*v$, which implies

$$v^*\left(\tfrac{1}{m}B^3\right)v = |\lambda|^2 v^*v, \tag{22}$$

since $P^*P = I$ for any permutation matrix and $B^* = \overline{B} = \frac{1}{m}B^2$ using Theorem 1 and the fact that $B$ is symmetric. Appealling once more to Theorem 1, we find that $\frac{1}{m}B^3 = m^2I - mU$, where every entry of $U$ equals 1. Next observe that $Uv = 0$, since multiplying $PBv = \lambda v$ on the left by $U$ gives $UPBv = \lambda Uv$, and $UPB = UB = 0$ while $\lambda \neq 0$. Therefore (22) becomes

$$v^*(m^2I - mU)v = m^2v^*v - mv^*Uv = m^2v^*v = |\lambda|^2 v^*v. \tag{23}$$

But $v^*v > 0$ since $v$ is a nonzero vector, and hence $|\lambda| = m$, as desired. ■

**5. DETERMINANTS.** One of the more striking properties of Jacobi sum matrices emerges once we begin to examine submatrices and their determinants, in particular. Thus the alert reader may have wondered about the determinant of (1). Since the sum of the entries in each row is zero, it is clear that $\det(B) = 0$ for any Jacobi sum matrix. Not content, the truly enterprising individual next computes $\det(B')$ for the lower right $6 \times 6$ submatrix $B'$ of matrix (1), obtaining the intriguing value $\det(B') = 16807 = 7^5$. The obvious generalization is true, and the groundwork for a proof has largely been laid. We need only one further observation, which is a nice result in its own right.

**Proposition 5** *Let $B$ denote a Jacobi sum matrix with lower right $(m-1) \times (m-1)$ submatrix $B'$. Then $(B')^{-1} = \frac{1}{m^2}(\overline{B'} + (m+1)U')$, where every entry of $U'$ is 1.*

*Proof.* The statement follows readily from the equality $B\overline{B} = m^2I - mU$ stated in Theorem 1. We omit the details. ■

**Proposition 6** *With $B$ and $B'$ as above, we have $\det(B') = m^{m-2}$.*

*Proof.* According to Corollary 1 the eigenvalues of $B$ belong to the set $\{0, m, m\omega, m\overline{\omega}\}$. We know $\det(B) = 0$, so $\operatorname{rank}(B) < m$. But by the previous lemma $B'$ is nonsingular; therefore $\operatorname{rank}(B) = m-1$, implying that exactly one eigenvalue of $B$ is 0. We next apply Lemma 1 to conclude that the eigenvalues of $B'$ are among $\{1, m, m\omega, m\overline{\omega}\}$, with the value 1 occurring precisely once. Finally, the discussion within Proposition 3 indicates that the values $m\omega$ and $m\overline{\omega}$ come in pairs. Hence the product of the $m-1$ eigenvalues, which is $\det(B')$, comes to $m^{m-2}$. ■

**Corollary 3** *Let $A$ be the submatrix of a Jacobi sum matrix $B$ obtained by deleting row $i$ and column $j$. Then we have $\det(A) = (-1)^{i+j}m^{m-2}$.*

*Proof.* The case $i = j = 0$ is handled by Proposition 6. When $j > 0$ note that adding all other columns of $B'$ to column $j$ effectively replaces that column with the negative of column 0 of $B$, since the sum of the entries within every row is 0. Moving this

column back to the far left and negating it introduces a sign of $(-1)^j$ to the value of the determinant. The same reasoning applies to the rows; therefore $B'$ is transformed into $A$ by operations that change the sign of $\det(B')$ by $(-1)^{i+j}$. ■

But why stop there? If $A$ is the lower right $5 \times 5$ submatrix of (1), we discover that $\det(A) = 343(7 - i\sqrt{7})$. The power of 7 is nice, but even more interesting is

$$7 - i\sqrt{7} = \overline{J(0,0)} - \overline{J(0,1)} - \overline{J(1,0)} + \overline{J(1,1)}. \tag{24}$$

In other words, the determinant of this submatrix appears to be related to the conjugates of the entries in the "complementary" upper left $2 \times 2$ submatrix. The same phenomenon occurs elsewhere; for instance, if $A$ is the upper left $5 \times 5$ submatrix of (1) then we find that $\det(A) = 343(-7 + 3i\sqrt{7})$, and sure enough

$$-7 + 3i\sqrt{7} = \overline{J(5,5)} - \overline{J(5,6)} - \overline{J(6,5)} + \overline{J(6,6)}. \tag{25}$$

These computations hint at a beautiful extension to Corollary 3. We first formalize a few of the above ideas.

A $k \times k$ submatrix $A$ is determined by a subset $r_1, \ldots, r_k$ of the rows of $B$, where $0 \le r_1 < \cdots < r_k \le m - 1$, and a similar subset $c_1, \ldots, c_k$ of $k$ columns. Deleting these rows and columns yields the *complementary submatrix* $A^c$, which contains exactly those entries of $B$ that are not in the same row or column as any element of $A$. The *sign of the submatrix*, denoted by $\epsilon_A$, is based on its position within $B$. It is given by

$$\epsilon_A = (-1)^{r_1 + \cdots + r_k + c_1 + \cdots + c_k}. \tag{26}$$

It is routine to verify that $\epsilon_A = \epsilon_{A^c}$. Finally, the *diminished determinant* $\operatorname{ddet}(A)$ of $A$ is an alternating sum of the determinants of all maximal submatrices of $A$. Letting $A^i_j$ represent the matrix obtained by deleting row $i$ and column $j$ of $A$ we have

$$\operatorname{ddet}(A) = \sum_{i,j=1}^{k} (-1)^{i+j} \det(A^i_j) = \sum_{A' \subset A} \epsilon_{A'} \det(A'), \tag{27}$$

where $A' \subset A$ signifies a $(k-1) \times (k-1)$ submatrix of $A$. We have chosen the term "diminished" since the degree of $\operatorname{ddet}(A)$ as a polynomial in the entries of $A$ is one less than the degree of $\det(A)$.

So that the upcoming result will apply to all possible submatrices of $B$, we adopt the convention that $\operatorname{ddet}(A) = 1$ for a $1 \times 1$ matrix $A$, while $\operatorname{ddet}(A) = 0$, $\det(A) = 1$, and $\epsilon_A = 1$ when $A$ is the $0 \times 0$ "empty" matrix. With the foregoing definitions in hand we are now prepared to state our main result.

**Theorem 2** *Given a Jacobi sum matrix $B$, let $A$ be any $k \times k$ submatrix of $B$, where $0 \le k \le m$. Denote the complementary submatrix to $A$ and its sign by $A^c$ and $\epsilon_{A^c}$, respectively. Then the following identity holds:*

$$\frac{\det(A)}{m^k} = \epsilon_{A^c} \frac{\operatorname{ddet}(\overline{A^c})}{m^{m-k}}. \tag{28}$$

Observe that the power of $m$ in each denominator corresponds to the size of the matrix in the numerator. Also, the examples outlined above illustrate the case $m = 7$, $k = 5$; in both examples the sign happened to be $\epsilon_{A^c} = 1$. We provide a proof of this result in the appendix. The reader is encouraged to peruse the argument—among other things, a number of steps would make excellent exercises for linear algebra students.

Before considering a collection of multivariable polynomials with unlikely factorizations, we pause to present a couple of elementary facts concerning the diminished determinant, which arose naturally in the preceding discussion. Early in the proof of Theorem 2 we will need an analogue to expansion by minors to handle the transition between diminished determinants for matrices of different sizes. To clarify the analogy, let $M$ be an $n \times n$ matrix with entries $m_{ij}$ and let $M_j^i$ denote the submatrix obtained by deleting row $i$ and column $j$ from $M$. Then expansion by minors implies that

$$\det(M) = \frac{1}{n} \sum_{i,j=1}^{n} (-1)^{i+j} m_{ij} \det(M_j^i). \tag{29}$$

**Lemma 2** *With $M$ and $M_j^i$ as above we have*

$$\operatorname{ddet}(M) = \frac{1}{n-1} \sum_{i,j=1}^{n} (-1)^{i+j} m_{ij} \operatorname{ddet}(M_j^i). \tag{30}$$

*Proof.* Applying (29) to the definition of $\operatorname{ddet}(M)$ yields

$$\begin{aligned} \operatorname{ddet}(M) &= \sum_{k,l=1}^{n} (-1)^{k+l} \det(M_l^k) \\ &= \sum_{k,l} (-1)^{k+l} \frac{1}{n-1} \sum_{\substack{i \neq k \\ j \neq l}} (-1)^{i'+j'} m_{ij} \det(M_{jl}^{ik}). \end{aligned} \tag{31}$$

Here $M_{jl}^{ik}$ is the submatrix of $M$ obtained by deleting rows $i$, $k$ and columns $j$, $l$. Note that if row $i$ is below row $k$ then we must use $i-1$ in the exponent when applying (29) to $\det(M_l^k)$; otherwise $i$ is the correct value. Hence we set $i' = i-1$ when $i > k$ and $i' = i$ when $i < k$, and similarly for $j'$ relative to $l$.

The key to ensuring that the signs behave is to realize that $(-1)^{i'+k} = (-1)^{i+k'+1}$, where $k' = k-1$ when $k > i$ and $k' = k$ otherwise. Defining $l'$ in the same manner relative to $j$ enables us to rewrite (31) as

$$\begin{aligned} \operatorname{ddet}(M) &= \frac{1}{n-1} \sum_{i,j} (-1)^{i+j} m_{ij} \sum_{\substack{k \neq i \\ l \neq j}} (-1)^{k'+l'} \det(M_{jl}^{ik}) \\ &= \frac{1}{n-1} \sum_{i,j=1}^{n} (-1)^{i+j} m_{ij} \operatorname{ddet}(M_j^i). \end{aligned} \tag{32}$$

This completes the proof. ∎

Diminished determinants also resemble determinants with respect to row and column transpositions.

**Lemma 3** *Interchanging a pair of adjacent rows or columns in a matrix $M$ negates the value of* $\operatorname{ddet}(M)$.

*Proof.* Every term in the sum $\sum (-1)^{i+j} \det(M_j^i)$ is negated by such an operation, for one of two reasons. If column $i$ and row $j$ stay put then a pair of rows or columns within $M_j^i$ trade places, negating $\det(M_j^i)$ without affecting $(-1)^{i+j}$. On the other hand, if column $i$ or row $j$ is involved in the exchange then $M_j^i$ still appears in the sum with entries intact, but now with an attached sign of $(-1)^{i+j\pm 1}$. ∎

**6. FURTHER INQUIRY.** To conclude we offer an observation regarding Jacobi sum matrices that suggests there is still gold left to be mined. Define the three permutation matrices

$$P_1 = \begin{pmatrix} 1&0&0&0&0&0&0\\ 0&1&0&0&0&0&0\\ 0&0&1&0&0&0&0\\ 0&0&0&1&0&0&0\\ 0&0&0&0&1&0&0\\ 0&0&0&0&0&1&0\\ 0&0&0&0&0&0&1 \end{pmatrix}, \quad P_2 = \begin{pmatrix} 1&0&0&0&0&0&0\\ 0&0&0&0&1&0&0\\ 0&1&0&0&0&0&0\\ 0&0&0&0&0&1&0\\ 0&0&1&0&0&0&0\\ 0&0&0&0&0&0&1\\ 0&0&0&1&0&0&0 \end{pmatrix}, \quad P_4 = \begin{pmatrix} 1&0&0&0&0&0&0\\ 0&0&1&0&0&0&0\\ 0&0&0&0&1&0&0\\ 0&0&0&0&0&0&1\\ 0&1&0&0&0&0&0\\ 0&0&0&1&0&0&0\\ 0&0&0&0&0&1&0 \end{pmatrix}. \tag{33}$$

In each case the 1s are situated along a "line through the origin," where the origin is the upper left entry and we reduce coordinates mod 7; the subscript indicates the slope of the line. We have already observed that the characteristic polynomial of matrix (1), which we shall denote as $B$ once again, splits completely over the field $\mathbb{Q}(\omega)$:

$$p_B(x) = \det(B - xP_1) = -x(x-7)^2(x-7\omega)^2(x-7\overline{\omega})^2. \tag{34}$$

Remarkably, much more is true:

$$\begin{aligned} \det(B - xP_1 - yP_2 - zP_4) \quad = \quad & -(x+y+z)(x+y+z-7)^2 \\ & (x+\omega y+\overline{\omega}z-7\omega)(x+\omega y+\overline{\omega}z-7\overline{\omega}) \\ & (x+\overline{\omega}y+\omega z-7\omega)(x+\overline{\omega}y+\omega z-7\overline{\omega}). \end{aligned} \tag{35}$$

Further experimentation suggests that it is not a coincidence that the slopes used for $P_1$, $P_2$, and $P_4$ are powers of 2. For instance, $\det(B - wP_1 - xP_2 - yP_4 - zP_8)$ splits into linear and quadratic factors, where $B$ is the Jacobi sum matrix for $\mathbb{F}_{16}$ and all matrices are $15 \times 15$ in size. This phenomenon persists for finite fields of odd characteristic as well. Thus when working over $\mathbb{F}_9$ we find that $\det(B - xP_1 - yP_3)$ splits completely over $\mathbb{Q}(\omega)$. We also point out the related beautiful factorization

$$\det(B - xP_5 - yP_7) = (x+y)(x+y+8)(x-y+8)(x-y-8)^2(x+y-8)^3. \tag{36}$$

Based on these observations we surmise the following.

**Conjecture 1** *Let $B$ be a Jacobi sum matrix for the finite field $\mathbb{F}_q$, where $q = p^r$ and $m = q - 1$. For $(k, m) = 1$ denote by $P_k$ the $m \times m$ permutation matrix whose entry in row $s$, column $t$ is 1 for all $0 \le s, t < m$ with $s \equiv kt \bmod m$. Then the polynomial*

$$\det(B - x_0P_1 - x_1P_p - x_2P_{p^2} - \cdots - x_{r-1}P_{p^{r-1}}) \tag{37}$$

*in the $r$ variables $x_0, x_1, \ldots, x_{r-1}$ may be written as a product of factors each of which has degree at most two in these variables.*

Other evidence that we have not included here suggests that this conjecture can be extended in scope.

In summary, we have examined an elegant tool from number theory via the lens of linear algebra and uncovered several nice results in the process. At the very least this approach demonstrates a tidy manner in which many of the elementary (though perhaps not fully mapped out) facts concerning Jacobi sums may be packaged. On an optimistic note, this avenue of inquiry may even lead to a more complete understanding of Jacobi sums.

**7. APPENDIX.** Our main result relates the determinant of a submatrix of a Jacobi sum matrix to the diminished determinant of the conjugate complementary submatrix.

**Theorem 2** *Given a Jacobi sum matrix $B$, let $A$ be any $k \times k$ submatrix of $B$, where $0 \le k \le m$. Denote the complementary submatrix to $A$ and its sign by $A^c$ and $\epsilon_{A^c}$, respectively. Then the following identity holds:*

$$\frac{\det(A)}{m^k} = \epsilon_{A^c} \frac{\mathrm{ddet}(\overline{A^c})}{m^{m-k}}. \tag{38}$$

*Proof.* For $k = 0$ and $k = m$ the statement to be proved reduces to

$$1 = \frac{\mathrm{ddet}(\overline{B})}{m^m}, \qquad \frac{\det(B)}{m^m} = 0. \tag{39}$$

The former is a consequence of Corollary 3, while the latter is clear. Furthermore, the statement for $k = m - 1$ is equivalent to Corollary 3. Hence we need only show that case $k$ follows from case $k + 1$ for $1 \le k \le m - 2$. In the interest of presenting a lucid argument, we will provide a sketch of the proof in the case $k = m - 3$, followed by a summary of the algebra for the general case, which is qualitatively no different.

Therefore suppose the result holds for $k = m-2$ and that $A$ is an $(m-3) \times (m-3)$ submatrix of $B$. For the sake of organization we permute the rows and columns of $B$ in order to situate the entries of $A^c$ in the upper left corner, but otherwise maintain the original order of the rows and columns within $A$ and $A^c$. Let us label the permuted matrix as $C$, having entries $\gamma_{ij}$ for $0 \le i, j \le m - 1$.

$$C = \left(\begin{array}{ccc|cc|c} \gamma_{00} & \gamma_{01} & \gamma_{02} & \gamma_{03} & \gamma_{04} & \\ \gamma_{10} & \gamma_{11} & \gamma_{12} & \gamma_{13} & \gamma_{14} & \cdots \\ \gamma_{20} & \gamma_{21} & \gamma_{22} & \gamma_{23} & \gamma_{24} & \\ \hline \gamma_{30} & \gamma_{31} & \gamma_{32} & & & \\ \gamma_{40} & \gamma_{41} & \gamma_{42} & & A & \\ & \vdots & & & & \end{array}\right) \tag{40}$$

We claim that the result for $k = m - 2$ continues to hold for matrix $C$, up to a sign which we now determine. For exchanging a pair of adjacent rows or columns of $B$ will negate exactly one of $\det(A)$, $\mathrm{ddet}(\overline{A^c})$ or $\epsilon_{A^c}$, according as the pair of rows or columns both intersect $A$, both intersect $A^c$ (by Lemma 3), or intersect both. If the entries of $A^c$ reside in rows $r_1$, $r_2$, $r_3$ and columns $c_1$, $c_2$, $c_3$ then it requires

$$r_1 + (r_2 - 1) + (r_3 - 2) + c_1 + (c_2 - 1) + (c_3 - 2) \tag{41}$$

swaps of adjacent rows or columns to transform $B$ into $C$; hence we must include a factor of $\epsilon_{A^c}$ when applying (28) to $C$. In other words, if $D$ is an $(m - 2) \times (m - 2)$ submatrix of $C$ then

$$\epsilon_{A^c} \frac{\det(D)}{m^{m-2}} = \epsilon_{D^c} \frac{\mathrm{ddet}(\overline{D^c})}{m^2}. \tag{42}$$

The final observation to be made before embarking upon a grand calculation is that the dot product of any row vector of $C$ with the conjugate of another row vector is $-m$, while the dot product of a row vector with its own conjugate is $m^2 - m$. This relationship holds for $B$ since $B$ is symmetric and $B\overline{B} = m^2 I - mU$, as noted in the proof of Theorem 1. Permuting rows and columns of $B$ does not destroy this property, which consequently holds for $C$ as well. Now to begin.

We wish to relate $\mathrm{ddet}(\overline{A^c})$ to $\det(A)$. By Lemma 2 we may begin

$$\begin{aligned} \mathrm{ddet}(\overline{A^c}) &= \frac{1}{2}\left(\overline{\gamma}_{00}\,\mathrm{ddet}\begin{pmatrix}\overline{\gamma}_{11} & \overline{\gamma}_{12} \\ \overline{\gamma}_{21} & \overline{\gamma}_{22}\end{pmatrix} - \overline{\gamma}_{01}\,\mathrm{ddet}\begin{pmatrix}\overline{\gamma}_{10} & \overline{\gamma}_{12} \\ \overline{\gamma}_{20} & \overline{\gamma}_{22}\end{pmatrix} + \cdots\right) \\ &= \frac{\epsilon_{A^c}}{2m^{m-4}}\Big(\overline{\gamma}_{00}\det(C_{12}^{12}) + \overline{\gamma}_{01}\det(C_{02}^{12}) + \overline{\gamma}_{02}\det(C_{01}^{12}) + \cdots\Big), \end{aligned} \tag{43}$$

since the result holds for $k = m - 2$ with a correction factor of $\epsilon_{A^c}$. As before $C^{ik}_{jl}$ denotes the submatrix of $C$ obtained by deleting rows $i$, $k$ and columns $j$, $l$. We then expand each of $\det(C^{12}_{12})$, $\det(C^{12}_{02})$, and $\det(C^{12}_{01})$ by minors along row 0, which gives $(\overline{\gamma}_{00}\gamma_{00} + \overline{\gamma}_{01}\gamma_{01} + \overline{\gamma}_{02}\gamma_{02})\det(A)$, along with a fair number of other terms. We next collect the remaining terms according to whether they involve $\gamma_{03}$, $\gamma_{04}$, $\gamma_{05}$, and so on. The reader may verify that the sum of the terms containing a factor of $\gamma_{03}$ is

$$\gamma_{03}\overline{\gamma}_{03}\det(A) + m\det(A_{\gamma_{03}\triangleright 3}), \tag{44}$$

where $A_{\gamma_{03}\triangleright 3}$ refers to $A$ with all entries in the left column replaced by $\gamma_{03}$. Combining the terms involving $\gamma_{04}$, $\gamma_{05}$, ..., we may rewrite the first three terms of (43) as

$$\begin{aligned}&(\gamma_{00}\overline{\gamma}_{00} + \gamma_{01}\overline{\gamma}_{01} + \gamma_{02}\overline{\gamma}_{02} + \gamma_{03}\overline{\gamma}_{03} + \gamma_{04}\overline{\gamma}_{04} + \gamma_{05}\overline{\gamma}_{05} + \cdots)\det(A)\\ &+ m\det(A_{\gamma_{03}\triangleright 3}) + m\det(A_{\gamma_{04}\triangleright 4}) + m\det(A_{\gamma_{05}\triangleright 5}) + \cdots.\end{aligned} \tag{45}$$

The coefficient of $\det(A)$ is the dot product of row 0 of $C$ with its own conjugate, so

$$(m^2 - m)\det(A) + m\det(A_{\gamma_{03}\triangleright 3}) + m\det(A_{\gamma_{04}\triangleright 4}) + m\det(A_{\gamma_{05}\triangleright 5}) + \cdots. \tag{46}$$

Finally, this entire sequence of steps may be performed on the second trio and third trio of terms in (43), yielding

$$\begin{aligned}3(m^2 - m)\det(A) &+ m(\det(A_{\gamma_{03}\triangleright 3}) + \det(A_{\gamma_{04}\triangleright 4}) + \det(A_{\gamma_{05}\triangleright 5}) + \cdots)\\ &+ m(\det(A_{\gamma_{13}\triangleright 3}) + \det(A_{\gamma_{14}\triangleright 4}) + \det(A_{\gamma_{15}\triangleright 5}) + \cdots)\\ &+ m(\det(A_{\gamma_{23}\triangleright 3}) + \det(A_{\gamma_{24}\triangleright 4}) + \det(A_{\gamma_{25}\triangleright 5}) + \cdots).\end{aligned} \tag{47}$$

Since the sum of the entries of any column of $C$ is 0, we have

$$\det(A_{\gamma_{03}\triangleright 3}) + \det(A_{\gamma_{13}\triangleright 3}) + \det(A_{\gamma_{23}\triangleright 3}) = -\det(\tilde{A}_3), \tag{48}$$

where $\tilde{A}_3$ represents matrix $A$ with each entry in its leftmost column replaced by the sum of all the entries in that column. Defining $\tilde{A}_j$ similarly for $j \geq 3$, (47) reduces to

$$3(m^2 - m)\det(A) - m(\det(\tilde{A}_3) + \det(\tilde{A}_4) + \det(\tilde{A}_5) + \cdots). \tag{49}$$

It is a neat exercise in linear algebra to confirm that $\sum \det(\tilde{A}_j) = (m-3)\det(A)$. Each term of $\det(A)$ appears in $\det(\tilde{A}_j)$ for every $j$ and hence appears $m - 3$ times in the sum; all other terms cancel in pairs, as the reader may verify. Hence we are left with

$$3(m^2 - m)\det(A) - m(m-3)\det(A) = 2m^2\det(A). \tag{50}$$

In summary, we have shown that

$$\mathrm{ddet}(\overline{A^c}) = \frac{\epsilon_{A^c}}{2m^{m-4}}(2m^2\det(A)) = \epsilon_{A^c}\frac{\det(A)}{m^{m-6}}. \tag{51}$$

Dividing through by $\epsilon_{A^c}m^3$ gives the desired equality.

The calculation proceeds in an identical fashion for other values of $k$. We reach

$$k(m^2 - m)\det(A) - m(m-k)\det(A) = (k-1)m^2\det(A) \tag{52}$$

in place of (50), yielding

$$\mathrm{ddet}(\overline{A^c}) = \frac{\epsilon_{A^c}}{(k-1)m^{m-2k+2}}((k-1)m^2\det(A)) = \epsilon_{A^c}\frac{\det(A)}{m^{m-2k}}. \tag{53}$$

Rearranging gives the result. ■

**Acknowledgments.** I would like to thank the referees for many helpful remarks and suggestions. In particular, the idea of generating the right-hand scatterplot in the figure as well as the insightful remarks contained in the footnote were both due to the referees. I am also grateful to Ron Evans for sharing the (quite rapidly found) proof appearing in this article.

# References

[1] Adleman, L.; Pomerance, C.; Rumely, R., On distinguishing prime numbers from composite numbers, *Ann. of Math.* **117** (1983), 173–206.

[2] Berndt, B. C.; Evans, R. J.; Williams, K. S., Gauss and Jacobi Sums. *Wiley, New York,* 1998.

[3] Eisenstein, G., Einfacher beweis und verallgemeinerung des fundamental-theorems für die biquadratischen reste, in *Mathematische Werke,* Band I, 223–245, *Chelsea, New York,* 1975.

[4] Horn, R. A.; Johnson, C. R., Matrix Analysis. *Cambridge University Press, Cambridge,* 1985.

[5] Ireland, K.; Rosen, M., A Classical Introduction to Modern Number Theory, Second edition. *Springer, New York,* 1990.

[6] Weil, A., Number of solutions of equations in a finite field, *Bull. Amer. Math. Soc.* **55** (1949), 497–508.

**Samuel K. Vandervelde** is an assistant professor of mathematics at St. Lawrence University. His mathematical interests include number theory, graph theory, and partitions. He is an enthusiastic promoter of mathematics—he conducts math circles for students of all ages, helped to found the Stanford Math Circle and the Teacher's Circle, and composes problems for the USA Math Olympiad. He also writes and coordinates the Mandelbrot Competition, a nationwide contest for high schools. He is an active member of his church and enjoys singing, hiking, and teaching his boys to program.
*Department of Math, CS and Stats, St. Lawrence University, Canton, NY 13617*
*svandervelde@stlawu.edu*