A Determinantal Identity for the Permanent of a Rank 2 Matrix

Adam W. Marcus

Abstract. We prove an identity relating the permanent of a rank 2 matrix and the determinants of its Hadamard powers. When viewed in the right way, the resulting formula looks strikingly similar to an identity of Carlitz and Levine, suggesting the possibility that these are actually special cases of some more general identity (or class of identities) connecting permanents and determinants. The proof combines some basic facts from the theory of symmetric functions with an application of a famous theorem of Binet and Cauchy in linear algebra.

1. INTRODUCTION. The relationship between the determinant function, which maps a square matrix $A$ to

$$\det [A] = \sum_{\sigma \in S_n} (-1)^{\sigma} \prod_{i=1}^{n} A(i, \sigma(i)),$$

and the permanent function, which maps a square matrix $B$ to

$$\text{per} [B] = \sum_{\sigma \in S_n} \prod_{i=1}^{n} B(i, \sigma(i)),$$

is an important open problem in complexity theory. Despite having similar forms, the computation of the determinant can be done efficiently (due to, among other things, its predictable behavior with respect to Gaussian elimination) while the computation of the permanent is thought to be significantly harder. One of the more successful approaches to relating these two functions, known as geometric complexity theory, is to look for formulas of the type

$$\text{per} [M] = \det [M'],$$

where $M$ is a square matrix and $M'$ is a (typically much larger) square matrix formed from affine combinations of the entries of $M$. (The size of the matrix $M'$ that is needed for (1) to hold can then be related to other measures of complexity—we refer the reader to [3] for more details.)

For matrices of a specific form, however, it is sometimes possible to find a formula that expresses the permanent of a matrix as the determinant of other matrices of the same size. One notable example of this is a result of Borchardt [2] that was later generalized by Cayley [5] and then further generalized by Carlitz and Levine [4]. For a matrix $M \in \mathbb{R}^{n \times n}$ with entries $m(i, j)$ and integer $p$, let $M_p$ be the matrix with

$$M_p(i, j) = m(i, j)^p.$$

In this notation, the main result of [4] is the following theorem:

\[\text{doi.org/10.1080/00029890.2022.2115803}\]

MSC: Primary 15A15, Secondary 05E05
Theorem 1 (Carlitz–Levine). For a rank 2 matrix $M$ with no zero entries,
\[
\det [M_{-2}] = \det [M_{-1}] \per [M_{-1}]. \tag{2}
\]

The proof in [4] is elementary, using little more than the definitions and some facts concerning the cycle structure of permutations. The goal of this article is to prove a formula that has an intriguingly similar form to (2) but for seemingly quite different reasons. Our main result, Theorem 9, states that for matrices $M$ with rank at most 2,
\[
(n!)^2 \det [M_n] = (n^n) \det [M_{n-1}] \per [M_1]. \tag{3}
\]

The proof will use a combination of tools from the theory of polynomials and a theorem of Binet and Cauchy on the minors of a product of matrices.

Motivation. While the restriction to matrices of rank at most 2 may seem overly simplistic, it should be noted that the permanents of such matrices appear naturally in the context of binary operations that are symmetric in both arguments (or BOSBAs). The author came across them, for example, during an investigation of the characteristic polynomials of random matrices. More specifically, let $A, B \in \mathbb{R}^{n \times n}$ be Hermitian matrices, and consider the (random) polynomial
\[
r(x) = \det \left[ xI - A - Q^T B Q \right],
\]
where $Q$ is an orthogonal matrix drawn uniformly from $O_n$ (the group of $n \times n$ orthogonal matrices) with respect to the Haar measure.

It is not hard to see that the value of $r(x)$ is independent of the eigenvectors of $B$ and therefore must be a symmetric function of the eigenvalues of $B$. Conjugating by $Q$, one can see that the same is true for $A$ as well. That is, when viewed as a function of the eigenvalues of $A$ (as the first argument) and the eigenvalues of $B$ (as the second argument), $r(x)$ is a BOSBA. Furthermore, it can be shown that the expected value of this polynomial is the permanent of a rank 2 matrix:
\[
\mathbb{E}_Q \left\{ \det \left[ xI - A - Q^T B Q \right] \right\} = \frac{1}{n!} \per \left[ \left\{ x - \lambda_i(A) - \lambda_j(B) \right\}_{i,j=1}^n \right],
\]
where $\lambda_i(A)$ denotes the eigenvalues of $A$ (and similarly for $B$).

Expected characteristic polynomials of this type play an important role in the field of finite free probability which has contributed to a number of recent theoretical [7, 9] and algorithmic [10, 12] advances. Since permanents are, by nature, often more difficult to work with than determinants (they are not multiplicative, for example), the hope is that a formula like (3) could have uses (though, admittedly, the author has not found any yet—see Section 4).

2. PRELIMINARIES. We will use the customary notation that $[n] = \{1, 2, \ldots, n\}$ and that $\binom{[n]}{k}$ denotes the collection of subsets of $[n]$ size $k$. For a permutation $\sigma$, we write $|\sigma|$ to denote the number of cycles in its cycle decomposition. For a vector $\vec{x} \in \mathbb{R}^n$, a permutation $\sigma \in S_n$, and a set $S \subseteq [n]$, we will write
\[
\vec{x}^S := \prod_{i \in S} x_i \quad \text{and} \quad \sigma(S) = \{\sigma(i) : i \in S\}.
\]

In particular, given a matrix $M$ and sets $I, J$, we will write $M(I, J)$ to denote the submatrix of $M$ formed by the rows in $I$ and columns in $J$. ©2022 Society for Industrial and Applied Mathematics.
Symmetric and alternating polynomials. A polynomial \( p \in \mathbb{R}[x_1, \ldots, x_n] \) is said to be symmetric if
\[
p(x_1, \ldots, x_i, x_{i+1}, \ldots, x_n) = p(x_1, \ldots, x_{i+1}, x_i, \ldots, x_n)
\]
and alternating if
\[
p(x_1, \ldots, x_i, x_{i+1}, \ldots, x_n) = -p(x_1, \ldots, x_{i+1}, x_i, \ldots, x_n)
\]
for all transpositions \((i, i + 1)\). Since the set of transpositions generates the symmetric group, equivalent definitions are (for symmetric polynomials)
\[
p(x_1, \ldots, x_n) = p(x_{\pi(1)}, \ldots, x_{\pi(n)})
\]
and (for alternating polynomials)
\[
p(x_1, \ldots, x_n) = (-1)^{|\pi|}p(x_{\pi(1)}, \ldots, x_{\pi(n)})\tag{4}
\]
for all \( \pi \in S_n \). In particular, (4) implies that any alternating polynomial \( p \) must be 0 whenever \( x_i = x_j \) for some \( i \neq j \).

Examples of symmetric polynomials are the elementary symmetric polynomials
\[
e_k(x_1, \ldots, x_n) = \begin{cases} 
1 & \text{for } k = 0, \\
\sum_{\mathbf{S} \in \binom{[n]}{k}} \bar{x}^\mathbf{S} & \text{for } 1 \leq k \leq n, \\
0 & \text{otherwise}
\end{cases}
\]
and the power sum polynomials
\[
p_k(x_1, \ldots, x_n) = \sum_{i=1}^{n} x_i^k.
\]
One example of an alternating polynomial is the Vandermonde polynomial
\[
\Delta(x_1, \ldots, x_n) = \prod_{i<j}(x_j - x_i)\tag{5}
\]
Furthermore, it is easy to see that the Vandermonde polynomial is an essential part of any alternating polynomial:

**Lemma 2.** For all alternating polynomials \( f(x_1, \ldots, x_n) \), there exists a symmetric polynomial \( t(x_1, \ldots, x_n) \) such that
\[
f(x_1, \ldots, x_n) = \Delta(x_1, \ldots, x_n)t(x_1, \ldots, x_n).
\]

**Proof.** For distinct \( y_2, \ldots, y_n \in \mathbb{R} \), (4) implies that the univariate polynomial
\[
g(x) = f(x, y_2, \ldots, y_n) \in \mathbb{R}[x]
\]
satisfies \( g(y_k) = 0 \) for each \( k = 2, \ldots, n \). Hence \((x - y_k)\) must be a factor of \( g \) and so \((x_1 - x_k)\) must be a factor of \( f \). Since this is true for all \( k \) and all \( i \) (not just \( i = 1 \)), every polynomial of the form \((x_i - x_k)\) must be a factor of \( f \), and so
\[
f(x_1, \ldots, x_n) = \Delta(x_1, \ldots, x_n)t(x_1, \ldots, x_n)\tag{6}
\]
for some polynomial $t$. It remains to show that $t$ is symmetric. To do so, for each $\sigma \in S_n$, we can apply (6) to (4) to get

$$\Delta(x_1, \ldots, x_n)t(x_1, \ldots, x_n) = (-1)^{|\sigma|}\Delta(x_{\sigma(1)}, \ldots, x_{\sigma(n)})t(x_{\sigma(1)}, \ldots, x_{\sigma(n)}).$$

Since $\Delta$ is, itself, an alternating polynomial, we have

$$\Delta(x_1, \ldots, x_n) = (-1)^{|\sigma|}\Delta(x_{\sigma(1)}, \ldots, x_{\sigma(n)})$$

and so canceling both sides results in

$$t(x_1, \ldots, x_n) = t(x_{\sigma(1)}, \ldots, x_{\sigma(n)})$$

as needed.

**Linear algebra.** The only tool we will need from linear algebra is a famous theorem of Binet and Cauchy regarding the minors of products of matrices. The $(I, J)$-minor of a matrix $M$ is defined as

$$|M|_{I,J} = \det \{ M(I,J) \}.$$

The following theorem is attributed to Binet and Cauchy (independently) [11].

**Theorem 3 (Cauchy–Binet).** Let $m, n, p$, and $k$ be positive integers for which $k \leq \min\{m, n, p\}$. Then for all $m \times n$ matrices $A$ and $n \times p$ matrices $B$ and all sets $I, J$ with $|I| = |J| = k$, we have

$$|AB|_{I,J} = \sum_{K \in \binom{[n]}{k}} |A|_{I,K} |B|_{K,J} \quad (7)$$

For those unfamiliar with Theorem 3, we hope to convey some appreciation for it by pointing out that (7) simultaneously generalizes two fundamental formulas from linear algebra that (a priori) have no obvious relation to each other: the formula for matrix multiplication (the case when $k = 1$), and the product formula for determinants (the case when $m = n = p = k$).

3. **THE MAIN THEOREM.** Our approach will be to first prove (3) in a special case (Corollary 8) and to then extend that result to the full theorem. We start by finding an expansion for the permanent of certain matrices in terms of the elementary symmetric polynomials:

**Lemma 4.** For vectors $\tilde{u}, \tilde{v} \in \mathbb{R}^n$, if $A$ is the $n \times n$ matrix with

$$A(i, j) = 1 + u_i v_j,$$

then

$$\text{per}[A] = \sum_{k=0}^{n} k!(n-k)!e_k(\tilde{u})e_k(\tilde{v}).$$
Proof. By definition, we have

\[ \text{per} [A] = \sum_{\sigma \in S_n} \prod_{i=1}^{n} (1 + u_i v_{\sigma(i)}) , \]

where, for each \( \sigma \), we have

\[ \prod_{i=1}^{n} (1 + u_i v_{\sigma(i)}) = \sum_{S \subseteq [n]} \vec{u}^S \vec{v}^{\sigma(S)} . \]

For fixed \( S \) with \( |S| = k \), as \( \sigma \) ranges over all permutations, \( \sigma(S) \) will range over all sets \( T \in \binom{[n]}{k} \) and any \( \sigma' \) for which \( \sigma'(S) = \sigma(S) \) will give the same term. As there are a total of \( k!(n-k)! \) such permutations, we have

\[ \text{per} [A] = \sum_{k=0}^{n} k!(n-k)! \sum_{S \subseteq \binom{[n]}{k}} \sum_{T \in \binom{[n]}{k}} \vec{u}^S \vec{v}^T = \sum_{k=0}^{n} k!(n-k)! e_k(\vec{u}) e_k(\vec{v}) \]

as claimed. \( \blacksquare \)

For a vector \( \vec{x} \in \mathbb{R}^n \), let \( \{ Q^k_{\vec{x}} \}_{k=0}^{n} \) be the collection of \( n \times n \) matrices with entries

\[ Q^k_{\vec{x}}(i, j) = \begin{cases} x^j_i & \text{if } i > k, \\ x^{i-1}_j & \text{otherwise.} \end{cases} \]  

(8)

For example, when \( \vec{x} = (a, b, c) \), we have

\[ Q^0_{\vec{x}} = \begin{bmatrix} a & b & c \\ a^2 & b^2 & c^2 \\ a^3 & b^3 & c^3 \end{bmatrix} , \quad Q^1_{\vec{x}} = \begin{bmatrix} 1 & 1 & 1 \\ a & b & c \\ a^2 & b^2 & c^2 \end{bmatrix} , \quad \ldots , \quad Q^n_{\vec{x}} = \begin{bmatrix} 1 & 1 & 1 \\ a & b & c \\ a^2 & b^2 & c^2 \end{bmatrix} . \]

Lemma 5. For any vector \( \vec{x} \in \mathbb{R}^n \), we have

\[ \det [Q^k_{\vec{x}}] = e_{n-k}(\vec{x}) \Delta(\vec{x}) . \]

Proof. It should be clear from the properties of determinants that each function

\[ f_k(\vec{x}) := \det [Q^k_{\vec{x}}] \]

is an alternating polynomial. Hence, by Lemma 2, we have that

\[ f_k(\vec{x}) = t_k(\vec{x}) \Delta(\vec{x}) \]

for some symmetric function \( t_k \), so it remains to show that \( t_k = e_k \).

We start by considering degrees. Note that each \( f_k(\vec{x}) \) is a homogeneous polynomial of degree \( \binom{n+1}{2} - k \) and that \( \Delta(\vec{x}) \) is a homogeneous polynomial of degree \( \binom{n}{2} \). Hence \( t_k(\vec{x}) \) must be a homogeneous polynomial of degree \( n - k \). Now note that the degree of each \( x_i \) in \( f_k(\vec{x}) \) is at most \( n \), whereas the degree of each \( x_i \) in \( \Delta(\vec{x}) \) is \( n - 1 \). Hence the degree of each \( x_i \) in \( t_k(\vec{x}) \) is at most \( 1 \).
The only symmetric polynomials that satisfy these constraints are multiples of the elementary symmetric polynomials, and so we must have

$$f_k(\vec{x}) = w_k e_{n-k}(\vec{x}) \Delta(\vec{x})$$

for some constant $w_k$. However, one can check that we must have $w_k = 1$ by looking at the monomial formed by the product of the diagonal entries in $Q_\vec{x}$ and seeing that it is positive.

We will now use Lemma 5 to prove two corollaries. The first corollary appears in the solution to Problem 293(a) in [6] (and we suspect the authors were aware of Lemma 5 though they did not explicitly state it).

**Corollary 6.** For vectors $\vec{u}, \vec{v} \in \mathbb{R}^n$, if $B$ is the $n \times n$ matrix with entries

$$B(i, j) = (1 + u_i v_j)^{n-1},$$

then

$$\det [B] = \Delta(\vec{u}) \Delta(\vec{v}) \left( \prod_{j=0}^{n-1} \binom{n-1}{j} \right).$$

**Proof.** Let $Y$ be the $n \times n$ diagonal matrix with entries $Y(i, i) = \binom{n-1}{i-1}$. It is easy to check that

$$B = Q_\vec{u}^\top Y Q_\vec{v}$$

and so by the product rule for the determinant, we have

$$\det [B] = \det [Q_\vec{u}^\top] \det [Y] \det [Q_\vec{v}].$$

Lemma 5 then completes the proof.

The second corollary is similar in spirit to the first one, but requires the added machinery of Theorem 3.

**Corollary 7.** For vectors $\vec{u}, \vec{v} \in \mathbb{R}^n$, if $C$ is the $n \times n$ matrix with entries

$$C(i, j) = (1 + u_i v_j)^n,$$

then

$$\det [C] = \Delta(\vec{u}) \Delta(\vec{v}) \left( \prod_{j=0}^{n} \binom{n}{j} \right) \sum_{k=0}^{n} e_k(\vec{u}) e_k(\vec{v}) \frac{1}{\binom{n}{k}}.$$
\[
\sum_{K,L \in \binom{[n+1]}{n}} |\hat{Q}_{\hat{\mathbf{x}}}|_{[n],K} |Z|_{K,L} |\hat{Q}_x|_{L,[n]}. \tag{9}
\]

To simplify (9), we note that since \(Z\) is diagonal, \(|Z|_{K,L} = 0\) unless \(K = L\). Furthermore, note that the complement of each set \(K\) contains a single element. When that element is \(p \in [n+1]\), we have
\[
|\hat{Q}_x|_{[n],K} = |Q_p^x| \quad \text{and} \quad |Z|_{K,K} = \det [Z] \left(\frac{n}{p-1}\right).
\]

The result then follows from Lemma 5.

Putting the three corollaries together gives us the following:

**Corollary 8.** For vectors \(\mathbf{u}, \mathbf{v} \in \mathbb{R}^n\), if \(A, B, C\) are \(n \times n\) matrices with entries
\[
A(i, j) = 1 + u_i v_j, \quad B(i, j) = (1 + u_i v_j)^{n-1}, \quad \text{and} \quad C(i, j) = (1 + u_i v_j)^n,
\]
then
\[
(n!)^2 \det [C] = (n^n) \det [B] \per [A].
\]

**Proof.** Combining Lemma 4 and Corollary 7 gives
\[
n! \det [C] = \Delta(\mathbf{u}) \Delta(\mathbf{v}) \left(\prod_{j=0}^{n} \binom{n}{j}\right) \per [A],
\]
where we have
\[
\prod_{j=0}^{n} \binom{n}{j} = \prod_{j=1}^{n} \frac{n!}{j! (n-j)!} = \frac{n^n}{n!} \prod_{j=1}^{n} \frac{(n-1)!}{(j-1)!} = \frac{n^n}{n!} \prod_{j=0}^{n-1} \binom{n-1}{j}.
\]

Plugging in Corollary 6 gives the result.

Finally, we extend Corollary 8 to the case of any rank 2 matrix.

**Theorem 9.** Let \(X \in \mathbb{R}^{n \times n}\) be any rank 2 matrix and let \(X_{n-1}, X_n \in \mathbb{R}^{n \times n}\) be the matrices with
\[
X_{n-1}(i, j) = X(i, j)^{n-1} \quad \text{and} \quad X_n(i, j) = X(i, j)^n.
\]

Then
\[
(n!)^2 \det [X_n] = (n^n) \det [X_{n-1}] \per [X].
\]

**Proof.** First note that if we let \(\mathbf{1} \in \mathbb{R}^n\) denote the vector with \(\mathbf{1}(k) = 1\) for all \(k\), then Corollary 8 proves the theorem in the case that
\[
X = \mathbf{u} \otimes \mathbf{v} + \mathbf{1} \otimes \mathbf{1}.
\]
Now let \( Y = \vec{u} \otimes \vec{v} + \vec{w} \otimes \vec{x} \) for general \( \vec{w}, \vec{x} \). The expansion of \( \det [Y_n] \) in terms of monomials has the form

\[
\det [Y_n] = \sum_{i_1, \ldots, i_n, j_1, \ldots, j_n} c_{i_1, \ldots, i_n, j_1, \ldots, j_n} \prod_k u_k^{i_k} w_k^{n-i_k} v_k^{j_k} x_k^{n-j_k}, \tag{10}
\]

where the \( c_{i_1, \ldots, i_n, j_1, \ldots, j_n} \) are constants. Similarly, \( \det [Y_{n-1}] \) per \( [Y] \) has an expansion

\[
\det [Y_{n-1}] \text{ per } [Y] = \sum_{i_1, \ldots, i_n, j_1, \ldots, j_n} \hat{c}_{i_1, \ldots, i_n, j_1, \ldots, j_n} \prod_k u_k^{i_k} w_k^{n-i_k} v_k^{j_k} x_k^{n-j_k}
\tag{11}
\]

for some constants \( \hat{c}_{i_1, \ldots, i_n, j_1, \ldots, j_n} \). Plugging in \( \vec{x} = \vec{1} \) and \( \vec{w} = \vec{1} \), however, does not cause any of the coefficients to combine. That is,

\[
\det [X_n] = \sum_{i_1, \ldots, i_n, j_1, \ldots, j_n} c_{i_1, \ldots, i_n, j_1, \ldots, j_n} \prod_k u_k^{i_k} v_k^{j_k}
\]

and

\[
\det [X_{n-1}] \text{ per } [X] = \sum_{i_1, \ldots, i_n, j_1, \ldots, j_n} \hat{c}_{i_1, \ldots, i_n, j_1, \ldots, j_n} \prod_k u_k^{i_k} v_k^{j_k},
\]

and so by Corollary 8, we have

\[
(n1)^2 c_{i_1, \ldots, i_n, j_1, \ldots, j_n} = (n^n) \hat{c}_{i_1, \ldots, i_n, j_1, \ldots, j_n}
\]

for all indices \( i_1, \ldots, i_n \) and \( j_1, \ldots, j_n \). Plugging this into (10) and (11) implies equality for \( Y \).

**4. CONCLUSION.** It is worth noting that Theorem 9 does not seem to be useful algorithmically. For the purpose of computing permanents, it tends to be slower than the algorithm of Barvinok [1] and also runs into stability issues whenever the two determinants approach 0 (in particular, when the original matrix \( X \) is actually rank 1).

Returning to the motivation discussed in Section 1, the author discovered Theorem 9 in a (failed) attempt to prove the following conjecture, which would have useful implications in the field of finite free probability:

**Conjecture 10.** For any matrix \( T \) with rank at most 2,

\[
\text{per } \begin{bmatrix} T & T \\ T & T \end{bmatrix} \leq \binom{2n}{n} \text{ per } [T]^2.
\]

A proof is known in the case that the entries of \( T \) are all positive, but the general case seems harder.

**Further research.** There are two obvious directions for extending Theorem 9, both of which would be quite interesting. First, the structural similarity between (2) and (3) suggests that a larger class of formulas of the type

\[
c(n) \det[M_i] = \det[M_j] \text{ per } [M_k]
\]

December 2022}
could exist for matrices $M \in \mathbb{R}^{n \times n}$ of a certain type (in our case, rank 2). Second, one can ask if there is a determinantal formula similar to (3) that is capable of computing the permanent of a rank 3 matrix. In this regard, it is worth mentioning that the author’s original proof of Theorem 9 used a formula of Jacobi that relates the determinants of the $Q_k^{\mathbf{x}}$ matrices defined in (8) to Schur polynomials [8]. The author opted for the current presentation, which was suggested by an anonymous referee, due to its elegance. For the purposes of extension, however, we mention the connection to Schur polynomials as a possible approach.

A final (but far more speculative) research direction lies in the fundamental relationship between the permanent and determinant functions. In particular, one can ask whether different models for geometric complexity theory could lead to new and interesting results. Equations (2) and (3) suggest two possible generalizations. First, one could attempt to satisfy (1) with a matrix $M'$ whose entries are polynomials in the entries of $M$ (instead of just affine combinations). Second, one could try to replace (1) with an equation of the form

$$\det [M''] \per [M] = \det [M'],$$

where both $M''$ and $M'$ are affine (or polynomial) combinations of the entries of $M$. It is unclear what the immediate implications of either generalization would be, but given the central importance of complexity theory in computer science, one would expect that any new results of this type would be quite interesting.

ACKNOWLEDGMENTS. The author wishes to recognize the support of the National Science Foundation (NSF CAREER grant DMS-1552520) as well as the input of two anonymous referees.

REFERENCES

[1] Barvinok, A. (1996). Two algorithmic results for the traveling salesman problem. Math. Oper. Res. 21(1): 65–84.
[2] Borchardt, C. W. (1855). Bestimmung der symmetrischen Verbindungen vermittelst ihrererzeugenden Funktion. J. Reine Angew. Math. 53: 193–198.
[3] Bürgisser, P. (2016). Permanent versus determinant, obstructions and Kronecker coefficients. Séminaire Lotharingien de Combinatoire. B75a: 1–19. www.emis.de/journals/SLC/wpapers/s75buerg.html
[4] Carlitz, L., Levine, J. (1960). An identity of Cayley. Amer. Math. Monthly. 67(6): 571–573.
[5] Cayley, A. (1859). Note sur les normales dune conique. J. Reine Angew. Math. 56: 182–185.
[6] Faddeev, D., Sominsky, L. (1978). Problems in Higher Algebra. (Yankovsky, G., trans.). Moscow: Mir Publishers.
[7] Gorin, V., Marcus, A. W., (2020). Crystallization of random matrix orbits. Int. Math. Res. Not. 2020(3): 883–913.
[8] Jacobi, C. G. J. (1841). De functionibus alternantibus earumque divisione per productum e differentiis elementorum conflatum. J. Reine Angew. Math. 22: 360–371.
[9] Marcus, A. W., Spielman, D. A., Srivastava, N. (2018). Interlacing families III: sharper restricted invertibility estimates. To appear, Israel J. Math. arxiv.org/abs/1712.07766
[10] Marcus, A. W., Spielman, D. A., Srivastava, N. (2018). Interlacing families IV: Bipartite Ramanujan graphs of all sizes. SIAM J. Comput. 47(6): 2488–2509.
[11] Shafarevich, I. R., Remizov, A. O. (2012). Linear Algebra and Geometry. Berlin-Heidelberg: Springer-Verlag. doi.org/10.1007/978-3-642-30994-6
[12] Xie, J., Xu, Z. (2020). Subset selection for matrices with fixed blocks. Israel J. Math (to appear). arxiv.org/abs/1903.06350

ADAM W. MARCUS received his Ph.D. in the ACO program at the Georgia Institute of Technology. He held positions at Yale and Princeton and spent three years as Chief Scientist at a startup before joining EPFL as
Least Primitive Root of any Safe Prime is Prime

A prime $p$ is said to be a Sophie Germain prime \[ \text{[1]} \] if $2p + 1$ is also a prime and, in this case, $2p + 1$ is called a safe prime. For any $a \in (\mathbb{Z}/n\mathbb{Z})^*$, the order of $a$ is denoted by $ord_n(a)$ and is defined to be the least positive integer $k$ such that $a^k \equiv 1 \pmod{n}$. In particular, $a$ is said to be a primitive root of $n$ if $ord_n(a) = \phi(n)$. In this article, we prove the following theorem.

Theorem. Let $p$ be a Sophie Germain prime. Then the least primitive root of $2p + 1$ is prime.

Proof. Let $a$ be the least primitive root of $2p + 1$. We claim that $a$ is prime and we prove the same by method of contradiction. Suppose that there exists an $m$ such that $1 < m < a$ and $m|a$. If so, then $ord_{2p+1}(m) = 1, 2, p, or 2p$. It is to be noted that $ord_{2p+1}(m) \neq 1$ since $m > 1$ and $ord_{2p+1}(m) \neq 2$ since $m < a < 2p$. Furthermore, since $a$ is the least primitive root of $2p + 1$, it follows that $ord_{2p+1}(m) \neq 2p$.

Now, to finish the proof, we shall prove that if $ord_{2p+1}(m) = p$, then $\frac{a}{m}$ will be a primitive root of $2p + 1$, which contradicts the assumption that $a$ is the least primitive root of $2p + 1$.

Suppose $ord_{2p+1}(m) = p$. Then

$$
\left(\frac{a}{m}\right)^{mp} = a^p \equiv \left(\frac{a}{m}\right)^p \pmod{2p + 1} \implies \left(\frac{a}{m}\right)^p \equiv -1 \pmod{2p + 1}
$$

since $a$ is a primitive root of $2p + 1$. Now, since $1 < \frac{a}{m} < a < 2p$, it follows that $ord_{2p+1}(\frac{a}{m}) = 2p$, which is a contradiction.

REFERENCE

[1] Burton, D. M. (2012). Elementary Number Theory. New York: McGraw-Hill.

—Submitted by V. P. Ramesh and M. Makeshwari, Central University of Tamil Nadu, India

doi.org/10.1080/00029890.2022.2115816
MSC: Primary 11A41, Secondary 11A07