International J.Math. Combin. Vol.3(2024), 108-109

A Counterexample to a Theorem about Orthogonal Latin Squares

Zhiguo Ding and Michael E. Zieve

(Department of Mathematics, University of Michigan, 530 Church Street, Ann Arbor, MI 48109-1043, USA)

E-mail: dingz@umich.edu, zieve@umich.edu

Abstract: We give a counterexample to a theorem of Vadiraja and Shankar about orthogonality of Latin squares induced by bivariate polynomials in $(\mathbb{Z}/n\mathbb{Z})[X, Y]$.

Key Words: Bivariate polynomials, Latin squares, orthogonal Latin squares.

AMS(2010): 08B15.

The topic of orthogonal Latin squares has a rich history dating back to Euler. The main result of a paper by Vadiraja and Shankar asserts that certain Latin squares are orthogonal to one another. In this note we give a counterexample to this result. We need some preliminaries in order to state the result.

Let n be a positive integer, write $R := \mathbb{Z}/n\mathbb{Z}$, and pick any polynomials $f(X, Y), g(X, Y) \in R[X, Y]$. Let S_f be the n-by-n matrix with rows and columns indexed by $0, 1, 2, \cdots, n-1$ and whose entry in row i and column j is $f(i, j)$. The matrix S_f is called a *Latin square* if, for each $c \in R$, each of the polynomials $f(X, c)$ and $f(c, Y)$ permutes R. If both S_f and S_g are Latin squares then these Latin squares are *orthogonal* if, for each choice of $u, v \in R$, there exist unique $i, j \in R$ for which $f(i, j) = u$ and $g(i, j) = v$. If S_f is a Latin square then we define its "mirror image" to be $S_{\widehat{f}}$ where $\widehat{f}(X, Y) := f(X, -1-Y)$. Note that $S_{\widehat{f}}$ is the matrix obtained from S_f by reversing the order of the entries in each row. It is clear that if S_f is a Latin square then also $S_{\widehat{f}}$ is a Latin square. In light of this, it is natural to ask when S_f and $S_{\widehat{f}}$ are orthogonal. It is easy to see that this never occurs when n is even [1, Theorem 2.3]. Theorem 2.9 of [1] and Theorem 6.2 of [2] each assert that it always occurs when n is odd.

Theorem A (Vadiraja–Shankar) *If n is odd and S_f is a Latin square then S_f and $S_{\widehat{f}}$ are orthogonal.*

However, Theorem A is not true in general. One counterexample to this conclusion is $f(X, Y) = -X^3Y^2 - X^2Y^3 - X^2Y + XY^2 + X + Y$ with $n = 5$. For, we have

$$\begin{aligned} f(X,0) &= X, & f(0,Y) &= Y, \\ f(X,1) &= -(X-1)^3, & f(1,Y) &= -Y^3+1, \\ f(X,2) &= X^3+2, & f(2,Y) &= (Y-2)^3, \end{aligned}$$

[1]Received August 10, 2024, Accepted September 15, 2024.

$$f(X,3) = X^3 - 2, \qquad f(3,Y) = (Y+2)^3,$$
$$f(X,4) = -(X+1)^3, \qquad f(4,Y) = -Y^3 - 1.$$

Since X^3 permutes $Z/5\mathbb{Z}$, we see that S_f is a Latin square. But $f(0,0) = 0 = f(-1,-1)$ and

$$\widehat{f}(0,0) = f(0,-1) = -1 = f(-1,0) = \widehat{f}(-1,-1),$$

so that each of the pairs $(i,j) = (0,0)$ and $(i,j) = (-1,-1)$ satisfies $f(i,j) = 0$ and $\widehat{f}(i,j) = -1$. It follows that S_f and $S_{\widehat{f}}$ are not orthogonal. This concludes the proof that Theorem A is false.

In light of this counterexample, it is natural to reexamine the published proofs of Theorem A. The proof of Theorem 2.9 in [1] consists of restating the orthogonality condition (incorrectly) as pairwise distinctness of the pairs $\big(f(i,j), f(-1-i,j)\big)$ with $i,j \in R$, and then asserting without further justification that this distinctness follows from S_f being a Latin square.

The proof of Theorem 6.2 in [2] notes that there are n^2 distinct triples $\big(i,j,f(i,j)\big)$ with $i,j \in R$, and also n^2 distinct triples $\big(-1-i,j,f(i,j)\big)$ with $i,j \in R$, and then asserts orthogonality without further justification. Thus, the mistake in the proofs of both [1] and [2] is that the conclusion of Theorem A was claimed to follow at once from the hypothesis after an immediate reformulation, when in fact the hypothesis does not imply the conclusion.

References

[1] Vadiraja Bhatta G. R. and B. R. Shankar, Variations of orthogonality of Latin squares, *International J. Math. Combin.*, 3(2015), 55–61.

[2] G. R. Vadiraja Bhatta and B. R. Shankar, A study of permutation polynomials as Latin squares, in *Nearrings, Nearfields and Related Topics*, 270–281, World Sci. Publ., Hackensack, NJ, 2017.