EQUIVALENCE OF SPARSE CIRCULANTS: THE BIPARTITE ÁDÁM PROBLEM

DOUG WIEDEMANN AND MICHAEL E. ZIEVE

Abstract. We consider n-by-n circulant matrices having entries 0 and 1. Such matrices can be identified with sets of residues mod n, corresponding to the columns in which the top row contains an entry 1. Let A and B be two such matrices, and suppose that the corresponding residue sets S_A, S_B have size at most 3. We prove that the following are equivalent: (1) there are integers u, v mod n, with u a unit, such that $S_A = uS_B + v$; (2) there are permutation matrices P, Q such that $A = PBQ$. Our proof relies on some new results about vanishing sums of roots of unity. We give examples showing this result is not always true for denser circulants, as well as results showing it continues to hold in some situations. We also explain how our problem relates to the Ádám problem on isomorphisms of circulant directed graphs.

1. Introduction

We define a *circulant* to be any square matrix whose rows are consecutive right circular shifts of each other. In other words, it is any n-by-n matrix $(a_{i,j})$ where $a_{i,j}$ depends only on $i - j$ mod n. Thus, a circulant is a special type of Toeplitz matrix. Circulant matrices occur in numerous applications and have been studied extensively; for instance, see [3].

Surprisingly, for many applications the interest in circulants does not directly stem from the circular symmetry just described. For example, every Desarguesian finite projective plane can be represented as a circulant, by a theorem of Singer. In other words, if m is a prime power, there is an n-by-n circulant matrix (where $n = m^2 + m + 1$) in which each row has $m+1$ entries being 1 and the rest being 0, with the further condition that the componentwise product of any two rows has exactly one 1. Here the rows represent lines and the columns points, where a line contains a point whenever the corresponding entry in the circulant is a 1.

Date: June 18, 2007.

In this paper we are primarily interested in circulants with entries 0 and 1, which we call $(0, 1)$ circulants. One can think of a $(0, 1)$ circulant as an incidence structure, or as the nonzero block of the adjacency matrix of a bipartite graph. Many interesting examples of incidence structures correspond to $(0, 1)$ circulants; for instance, these include the much-studied subject of "cyclic difference sets".

The *weight* of a $(0, 1)$ circulant is the number of 1's in each row. Often the n-by-n circulants of interest have weight quite small compared to n. In this paper we prove that, for circulants of weight at most 3, various equivalence relations are the same. We need some notation to state our result. For any n-by-n $(0, 1)$ circulant A, let S_A be the set of integers mod n corresponding to the columns in which the top row of A contains an entry 1; here the leftmost column is labeled 0, the next is 1, and so on. Also, A^T denotes the transpose of the matrix A. Recall that a permutation matrix is an n-by-n matrix in which each row and each column contains a single entry 1 and $n - 1$ entries 0.

Theorem 1.1. *Let A and B be two n-by-n $(0, 1)$ circulants of weight at most 3. Then the following are equivalent:*

1. *There exist $u, v \in \mathbb{Z}/n\mathbb{Z}$ such that $\gcd(u, n) = 1$ and $S_A = uS_B + v$.*
2. *There are n-by-n permutation matrices P, Q such that $A = PBQ$.*
3. *There is an n-by-n permutation matrix P such that $AA^T = PBB^TP^{-1}$.*
4. *The complex matrices AA^T and BB^T are similar.*

It is not difficult to prove that (1) ⇒ (2) ⇒ (3) ⇒ (4). The bulk of our effort in proving Theorem 1.1 is devoted to proving (4) ⇒ (1) in the case of weight 3 (smaller weights are easier to handle). We give counterexamples to this result for every weight larger than 3. However, for weights 4 and 5, the result can be salvaged to some extent: we show that it holds as long as every prime factor of n is sufficiently large. On the other hand, for each weight exceeding 5, we give counterexamples for every sufficiently large n.

In the context of isomorphisms of circulant graphs, many authors have studied questions of a similar flavor as Theorem 1.1. In that context, we restrict to $v = 0$ in condition (1) and to $Q = P^{-1}$ in (2), getting conditions (1') and (2'). The equivalence of (1') and (2') is known as the Ádám problem; it is not always true, but the combined efforts of several authors have shown precisely when it holds (cf. [1, 2, 9, 10] and the references therein). Likewise, the equivalence of (1') to the similarity of A and B is called the spectral Ádám problem, and is still being studied [4, 5, 6, 8]. The equivalence of (1) and (2) amounts to a bipartite analogue of the Ádám problem. From the perspective of circulant matrices, condition (2) is quite natural, and arises in various applications.

In the next section we prove some preliminary results about the various equivalence relations under consideration. Then in Section 3 we give a quick proof of Theorem 1.1 in case the weight k is at most 2. The next three sections prove Theorem 1.1 in the much more difficult case $k = 3$: in Section 4 we reduce the problem to a question about vanishing sums of roots of unity, which we resolve in Sections 5 and 6. We discuss the cases $k = 4$ and $k = 5$ in Section 7, and the case $k \geq 6$ in Section 8. In Section 9 we explain how our problem relates to the Ádám problem. Finally, in Section 10 we suggest some directions for future research.

2. Equivalence Classes of Circulants

In almost any application of circulants, the first row can be replaced with any circular shift of itself. For example, both circulants below represent the projective plane of order 2 (also known as the Fano plane):

$$\begin{pmatrix} 0&1&1&0&1&0&0\\ 0&0&1&1&0&1&0\\ 0&0&0&1&1&0&1\\ 1&0&0&0&1&1&0\\ 0&1&0&0&0&1&1\\ 1&0&1&0&0&0&1\\ 1&1&0&1&0&0&0 \end{pmatrix} \quad \text{and} \quad \begin{pmatrix} 1&1&0&1&0&0&0\\ 0&1&1&0&1&0&0\\ 0&0&1&1&0&1&0\\ 0&0&0&1&1&0&1\\ 1&0&0&0&1&1&0\\ 0&1&0&0&0&1&1\\ 1&0&1&0&0&0&1 \end{pmatrix}.$$

Applying a circular shift to every row of a circulant has the effect of applying a circular shift to the order of the rows, which is equivalent to applying a circular shift to the columns. The top row of a circulant can be identified with a set of residues mod n, by listing the positions containing an entry of 1; here the leftmost position is labeled 0, the next is labeled 1, and so on. Thus, the circulants above are identified with the sets $\{1, 2, 4\}$ and $\{0, 1, 3\}$ mod 7, which we will denote as $\{1, 2, 4\}_7$ and $\{0, 1, 3\}_7$.

We now establish some notation that will be used throughout the paper. Let S be the unit circular shift on n-dimensional vectors over $\mathbb{C}$ (the complex numbers). Thus, if e_i is a column unit vector with a 1 in position i and a 0 elsewhere, then S is defined by $Se_i = e_{i-1}$ for $i = 0, 1, ..., n - 1$, where the indices are computed mod n. In other words, S is the matrix

$$\begin{pmatrix} 0 & 1 & 0 & 0 & \cdots & 0 \\ 0 & 0 & 1 & 0 & \cdots & 0 \\ \vdots & \vdots & & \ddots & & \vdots \\ 0 & 0 & \cdots & 0 & 1 & 0 \\ 0 & 0 & \cdots & 0 & 0 & 1 \\ 1 & 0 & 0 & \cdots & 0 & 0 \end{pmatrix}.$$

Note that the transpose of S equals the inverse of S, and also the powers of S are precisely the circular shifts by various amounts. The circulant corresponding to the residue set $\{a_1, ..., a_k\}_n$ is

$$A = S^{a_1} + ... + S^{a_k}.$$

For the applications we have in mind, we want to consider two circulants equivalent if one can be obtained from the other by row and column permutations. This motivates the following definition:

Definition 2.1. Two circulants A and B are said to be *P-Q equivalent* if there exist permutation matrices P and Q such that $B = PAQ$.

This clearly defines an equivalence relation. However, note that for most choices of n-by-n matrices A, P, Q, where A is a $(0,1)$ circulant and P and Q are permutation matrices, the matrix PAQ will not be circulant. In order that PAQ be circulant, P and Q must be quite special.

Applying a circular shift to a circulant has the effect of adding a constant to its set of residues, i.e., applying an element of the additive group of residues mod n. This operation leads to a P-Q equivalent matrix, since, we can take P to be the shift and Q to be the identity. It is also true, but less obvious, that multiplication by a unit u mod n produces a P-Q equivalent circulant: here we choose $P : e_i \mapsto e_{ui}$ and $Q := P^{-1}$, so if the residue set of A is $\{a_1, ..., a_k\}_n$ then the residue set of PAQ is $\{ua_1, ..., ua_k\}_n$.

We restate this as the following definition and proposition.

Definition 2.2. Two subsets $\mathcal{A}, \mathcal{B} \subseteq \mathbb{Z}/n\mathbb{Z}$ are *linearly equivalent* if there is a unit u in $\mathbb{Z}/n\mathbb{Z}$ such that $\mathcal{B} = u\mathcal{A}$. The two sets are *affinely equivalent* if there exist $u, v \in \mathbb{Z}/n\mathbb{Z}$, with u a unit, such that $\mathcal{B} = u\mathcal{A} + v$.

Proposition 2.3. *If two subsets of $\mathbb{Z}/n\mathbb{Z}$ are affinely equivalent, then the associated $(0,1)$ circulants are P-Q equivalent.*

The main focus of this paper is on the converse of this result. The following example shows that the converse is not always true. It exhibits an explicit P-Q equivalence between the circulants having residue sets

$$\{0,1,4,7\}_8 \quad \text{and} \quad \{0,1,3,4\}_8.$$

These sets are affinely inequivalent since the first set has two arithmetic progressions of length 3 ($1,4,7$ and $7,0,1$) but the second set has none.

$$\begin{pmatrix} 1&1&0&0&1&0&0&1\\ 1&1&1&0&0&1&0&0\\ 0&1&1&1&0&0&1&0\\ 0&0&1&1&1&0&0&1\\ 1&0&0&1&1&1&0&0\\ 0&1&0&0&1&1&1&0\\ 0&0&1&0&0&1&1&1\\ 1&0&0&1&0&0&1&1 \end{pmatrix} = \begin{pmatrix} 1&0&0&0&0&0&0&0\\ 0&0&0&0&0&1&0&0\\ 0&0&0&0&0&0&1&0\\ 0&0&0&1&0&0&0&0\\ 0&0&0&0&1&0&0&0\\ 0&1&0&0&0&0&0&0\\ 0&0&1&0&0&0&0&0\\ 0&0&0&0&0&0&0&1 \end{pmatrix} \cdot R$$

where

$$R = \begin{pmatrix} 1&1&0&1&1&0&0&0\\ 0&1&1&0&1&1&0&0\\ 0&0&1&1&0&1&1&0\\ 0&0&0&1&1&0&1&1\\ 1&0&0&0&1&1&0&1\\ 1&1&0&0&0&1&1&0\\ 0&1&1&0&0&0&1&1\\ 1&0&1&1&0&0&0&1 \end{pmatrix} \cdot \begin{pmatrix} 1&0&0&0&0&0&0&0\\ 0&1&0&0&0&0&0&0\\ 0&0&0&0&0&0&1&0\\ 0&0&0&0&0&0&0&1\\ 0&0&0&0&1&0&0&0\\ 0&0&0&0&0&1&0&0\\ 0&0&1&0&0&0&0&0\\ 0&0&0&1&0&0&0&0 \end{pmatrix}.$$

We now derive a crucial property of P-Q equivalent circulants. If A and B are P-Q equivalent circulants, then

$$BB^T = PAQQ^TA^TP^T = PAA^TP^{-1},$$

since the the transpose of a permutation matrix is its inverse. This proves a necessary condition for P-Q equivalence:

Proposition 2.4. *If the circulants A and B are P-Q equivalent then AA^T and BB^T are similar matrices, and in fact there is a permutation matrix which conjugates one to the other.*

We call AA^T the *autocorrelation matrix* of the circulant A. In the example above, the autocorrelation matrices are actually equal, not just similar. Note that if A is a circulant then AA^T is also a circulant, although if A is a $(0,1)$ circulant then AA^T might not be $(0,1)$ -valued: if $A = S^{a_1} + ... + S^{a_k}$ then $AA^T = \sum_{i=1}^{k}\sum_{j=1}^{k} S^{a_i-a_j}$.

In order to discuss when circulant matrices are similar, we first compute their eigenvalues. We do this via the well-known method for diagonalizing circulant matrices. Let ι be the square root of -1 which lies in the upper half-plane. Let $\zeta = e^{2\pi\iota/n}$ and let V be the Vandermonde matrix $(\zeta^{ij})_{0\le i,j\le n-1}$. It turns out that V diagonalizes every n-by-n circulant. Let $A = \sum_{i=0}^{n-1} w_i S^i$ with $w_i \in \mathbb{C}$. Then $V^{-1}AV = D$ is a diagonal matrix with $D_{r,r} = \sum_i w_i \zeta^{ir}$. (One way to prove this is to verify directly that $AV = VD$, and then use the invertibility of the Vandermonde matrix V.) As a result, if $\{a_1, ..., a_k\}_n$ is the residue set for a $(0,1)$ circulant A then the multiset of eigenvalues of AA^T is

$$\left\{ \sum_{1\le i,j\le k} \zeta^{(a_i-a_j)r} : 0 \le r \le n-1 \right\}. \tag{1}$$

Proposition 2.5. *If A is the circulant with residue set $\{a_1, \dots, a_k\}_n$, then the number of times that k^2 occurs as an eigenvalue of AA^T is equal to* $\gcd(n, \{a_i - a_j : 1 \le i, j \le k\})$.

Proof. If $k = 0$, the gcd is n so the statement is true because $A = 0$. Now assume $k > 0$. As above, the eigenvalues of AA^T are in bijection with the values $r \in \mathbb{Z}/n\mathbb{Z}$, where r corresponds to the sum in (1). This sum has k^2 terms of unit magnitude, so it equals k^2 if and only if each term is 1. This happens if and only if $rg \equiv 0 \pmod{n}$, where $g = \gcd\ (\{a_i - a_j : 1 \le i, j \le k\})$; this can be restated as $r \equiv 0 \pmod{n/\gcd(n, g)}$. Finally, the number of values $r \in \mathbb{Z}/n\mathbb{Z}$ with this property is $\gcd(n, g)$. □

3. The case $k \le 2$

In this section we show that, for $k \le 2$, two n-by-n $(0,1)$ circulants of weight k are affinely equivalent if and only if they are P-Q equivalent; in fact, we show that these properties are equivalent to similarity of the autocorrelation matrices. If $k \le 1$ this is clear, since all n-by-n $(0,1)$ circulants of weight k are affinely equivalent. For $k = 2$ the result is contained in the following theorem.

Theorem 3.1. *The number of affine classes of n-by-n weight-2 $(0,1)$ circulants is $\tau(n) - 1$, where $\tau(n)$ denotes the number of divisors of n. Furthermore, weight-2 circulants in distinct affine classes have dissimilar autocorrelation matrices.*

Proof. Let $\{a_1, a_2\}_n$ be the residue set corresponding to a weight-2 circulant. Put $g := \gcd(n, a_2 - a_1)$. Plainly $\{a_1, a_2\}_n$ is affinely equivalent to $\{0, a_2 - a_1\}_n$, which is linearly equivalent to $\{0, g\}_n$. Conversely, by Proposition 2.5, if g, g' are divisors of n with $1 \le g < g' < n$, then $\{0, g\}_n$ and $\{0, g'\}_n$ correspond to circulants with dissimilar autocorrelation matrices. The result follows. □

4. Preliminaries for larger k

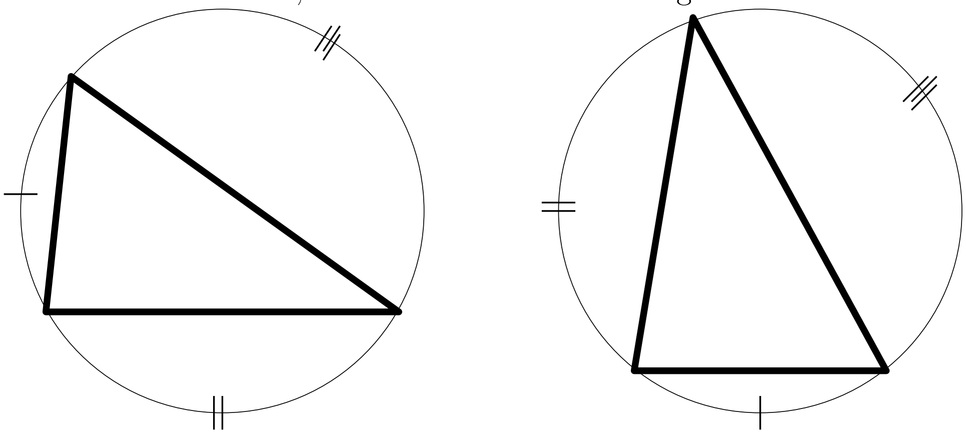
In the previous section we proved Theorem 1.1 for $k \leq 2$. The remaining case $k = 3$ is vastly more difficult. In this section we begin our attack on this case by showing that two weight-3 circulants are affinely equivalent if and only if their autocorrelation matrices are linearly equivalent. More explicitly, if $\mathcal{A} = \{a_1, ..., a_k\}$ is a set of k residues mod n, let $\Delta(\mathcal{A})$ be the multiset of k^2 residues $\{a_i - a_j \mid 1 \leq i, j \leq k\}$. If $\mathcal{A}$ is affinely equivalent to another residue set $\mathcal{B}$, then there is a unit u mod n such that $\Delta(\mathcal{A}) = u\Delta(\mathcal{B})$. We will prove the converse when $k = 3$. Since $u\Delta(\mathcal{B}) = \Delta(u\mathcal{B})$, it suffices to prove the converse in case $u = 1$.

Definition 4.1. For positive integers n and k, the *Same Difference Assertion*, or $\mathrm{SDA}(n, k)$, is the following assertion: for any sets $\mathcal{A}, \mathcal{B}$ of k residues mod n, we have $\Delta(\mathcal{A}) = \Delta(\mathcal{B})$ if and only if $\mathcal{A}$ is affinely equivalent to $\mathcal{B}$.

Remark. As noted above, $\mathrm{SDA}(n, k)$ is equivalent to saying that, for any two n-by-n $(0, 1)$ circulants of weight k, affine equivalence of the circulants is equivalent to linear equivalence of the autocorrelation matrices.

Proposition 4.2. $\mathrm{SDA}(n, 3)$ *is true for each* $n > 0$*.*

Proof. Suppose $\mathcal{A}$ and $\mathcal{B}$ are order-3 subsets of $\mathbb{Z}/n\mathbb{Z}$ with $\Delta(\mathcal{A}) = \Delta(\mathcal{B})$. Identify elements of $\mathbb{Z}/n\mathbb{Z}$ with points on the circle of circumference n centered at the origin, via $j \mapsto e^{2\pi\iota j/n}n/(2\pi)$. In this way we can identify $\mathcal{A}$ and $\mathcal{B}$ with sets of 3 points on this circle, where the arclength between two points equals the difference between the corresponding elements of $\mathbb{Z}/n\mathbb{Z}$. In the following diagram, $\mathcal{A}$ is recorded in the left-hand circle, and $\mathcal{B}$ is recorded in the right-hand circle.



In each diagram the circle is divided into three arcs; mark the shortest arc with a slash, the second-shortest arc with a double slash, and the longest arc with a triple slash. Note that $\Delta(\mathcal{A})$ consists of the three arclengths from the left-hand circle, together with all sums of two such arclengths, and three copies of 0. Thus the arclengths with a slash and double-slash in the left circle must equal the corresponding arclengths in the right circle. Hence the two triangles have equal angles, so they are congruent. We can make their angles occur in the same order, by replacing $\mathcal{A}$ by $-\mathcal{A}$ if necessary. Then there is a rotation which makes the triangles coincide. Thus $\mathcal{A}$ and $\mathcal{B}$ are affinely equivalent. □

Remark. This proof shows that the multiplicative coefficient can be taken to be ± 1.

We only need information about $k = 3$ for our main result, but we will say more about larger values of k later in the paper. For example, SDA$(n, 4)$ is not always true, one counterexample being the sets $\mathcal{A} := \{0, 1, 4, 7\}_8$ and $\mathcal{B} := \{0, 1, 3, 4\}_8$: one easily checks that $\Delta(\mathcal{A}) = \Delta(\mathcal{B})$, but $\mathcal{A}$ and $\mathcal{B}$ are affinely inequivalent since $\mathcal{A}$ contains arithmetic progressions of length 3 but $\mathcal{B}$ does not. However, in Section 7 we will prove SDA$(n, 4)$ for odd n, and SDA$(n, 5)$ for n coprime to 10. But in Section 8 we will give counterexamples to SDA(n, k) whenever $k > 5$ and $n > 2k + 10$.

5. Vanishing sums of roots of unity

The proof of our main result relies on some facts about vanishing sums of roots of unity, which we discuss in this section. Let $\mathfrak{A}$ be a multiset of roots of unity such that $\sum_{\alpha\in\mathfrak{A}} \alpha = 0$. If the only submultisets of $\mathfrak{A}$ with zero sum are the empty set and $\mathfrak{A}$, we say $\mathfrak{A}$ is a *minimal* vanishing sum of roots of unity. The *weight* of the sum is the size of the multiset $\mathfrak{A}$. We can multiply any vanishing sum of roots of unity by an arbitrary root of unity, without affecting minimality.

Vanishing sums of roots of unity have been studied extensively. In our situation, it turns out that we need to understand vanishing sums of twelve roots of unity. In fact, it is shown in [11] that, up to multiplying by an arbitrary root of unity, there are precisely 107 minimal vanishing sums of weight at most 12. However, complications arise in passing from minimal vanishing sums to nonminimal vanishing sums, since each minimal sum can be multiplied by an arbitrary root of unity: thus there are infinitely many vanishing sums of twelve roots of unity, so one cannot simply test them all. We give a self-contained approach which does not require the results from [11].

Lemma 5.1. *Let $\mathfrak{A}$ be a weight-d minimal vanishing sum of roots of unity, and suppose $1 \in \mathfrak{A}$. Let n be the least common multiple of the orders of the roots of unity in $\mathfrak{A}$. Then n divides the product of the primes not exceeding d. If d is prime and $d \mid n$ then $\mathfrak{A}$ consists of all the d^{th} roots of unity (so $n = d$). If $d-1$ is prime and $(d-1) \mid n$ then $n \mid 6(d-1)$.*

Proof. First we show n is squarefree. If not then $n = rp^{\ell}$ where p is prime, $\ell > 1$, and r is coprime to p. Let ζ be a primitive n^{th} root of unity. For any i with $0 \le i < n$, we can write $i = pa + b$ where $0 \le b < p$, so $\zeta^i = \zeta^b(\zeta^p)^a$. Rewriting our sum of roots of unity in this manner, we get a vanishing linear combination of $\zeta^0, \zeta^1, \dots, \zeta^{p-1}$ with coefficients in $\mathbb{Q}(\zeta^p)$. The field extension $\mathbb{Q}(\zeta)/\mathbb{Q}(\zeta^p)$ has degree $[\mathbb{Q}(\zeta) : \mathbb{Q}]/[\mathbb{Q}(\zeta^p) : \mathbb{Q}] = \phi(n)/\phi(n/p) = p$. Hence our vanishing linear combination must have all coefficients being zero. By minimality, only one coefficient can be a nontrivial sum of roots of unity. Since the sum includes 1, it follows that every root of unity in the sum has order dividing n/p, a contradiction. Thus n is squarefree.

Now let p be a prime dividing n, and rewrite the sum as $\sum_{\zeta^p=1} \zeta s_\zeta$ where each s_ζ is a sum of $(n/p)^{\text{th}}$ roots of unity. Since the sum includes 1, the term s_1 is a nontrivial sum of roots of unity. By the definition of n, some other s_ζ must also be a nontrivial sum of roots of unity. By minimality, any s_ζ which is nontrivial must be nonzero. Letting μ_j be the set of j^{th} roots of unity, we know that $\mathbb{Q}(\mu_p, \mu_{n/p}) = \mathbb{Q}(\mu_n)$ is an extension of $\mathbb{Q}(\mu_{n/p})$ of degree $[\mathbb{Q}(\mu_n) : \mathbb{Q}]/[\mathbb{Q}(\mu_{n/p}) : \mathbb{Q}] = \phi(n)/\phi(n/p) = p-1$. Thus the polynomial $x^{p-1} + x^{p-2} + \cdots + 1$ (whose roots are the primitive p^{th} roots of unity) is irreducible over $\mathbb{Q}(\mu_{n/p})$, so every s_ζ takes the same value. In particular, each s_ζ is nonzero, so our sum has weight at least p, whence n divides the product of the primes not exceeding d. If $d = p$ then every s_ζ is a single root of unity, and $s_1 = 1$, so every $s_\zeta = 1$ and thus our sum consists of all the p^{th} roots of unity (and $n = p$). Finally, suppose $d - 1 = p$. Then all but one s_ζ consists of a single root of unity α, and one s_ζ is the sum of two roots of unity $\beta + \gamma$. Since all s_ζ have the same value, we have $-\alpha + \beta + \gamma = 0$, which is a weight-three vanishing sum of roots of unity, and thus (from what we proved so far) must be a scalar times the sum of the cube roots of unity. Hence both β and γ are sixth roots of unity times α. Since our original sum includes 1, one of α, β, γ equals 1, so they all are sixth roots of unity and thus n divides $6p$. This concludes the proof. □

Remark. All but the last sentence of the lemma was proved by Mann [7].

Corollary 5.2. *Every minimal vanishing sum of roots of unity of weight $d < 6$ has d being prime and moreover has the form $\alpha\zeta_1 + \alpha\zeta_2 + \cdots + \alpha\zeta_d$ where α is a fixed root of unity and the ζ_i are all the distinct d^{th} roots of unity.*

Proof. Lemma 5.1 proves this unless the sum is a scalar times a sum involving only sixth roots of unity. So consider a minimal vanishing sum of sixth roots of unity, which we may assume includes 1. Rewrite this sum in the form $\sum_{\zeta^3=1} \zeta s_\zeta$, where each s_ζ is a sum of 1's and −1's. Since $1 + x + x^2$ is irreducible over $\mathbb{Q}$, every s_ζ must have the same value. If this common value is zero, then by minimality our vanishing sum is $-1 + 1$. If the common value is not zero, then by minimality our vanishing sum is the sum of the cube roots of unity. □

6. Proof of main result

In this section we complete the proof of Theorem 1.1 by proving

Theorem 6.1. *Let $\mathfrak{A} = \{\alpha_1, \alpha_2, \alpha_3, \bar{\alpha}_1, \bar{\alpha}_2, \bar{\alpha}_3\}$ and $\mathfrak{B} = \{\beta_1, \beta_2, \beta_3, \bar{\beta}_1, \bar{\beta}_2, \bar{\beta}_3\}$ be multisets of n^{th} roots of unity, where $\prod \alpha_j = 1 = \prod \beta_j$. Suppose that the two multisets $\{\sum_{\phi\in\mathfrak{A}} \phi^r : 1 \le r \le n\}$ and $\{\sum_{\psi\in\mathfrak{B}} \psi^r : 1 \le r \le n\}$ are identical. Then there is an integer u coprime to n such that $\mathfrak{A} = \{\psi^u : \psi \in \mathfrak{B}\}$.*

First we show that this result implies Theorem 1.1.

Proof of Theorem 1.1. The implication (1) ⇒ (2) is Proposition 2.3, the implication (2) ⇒ (3) is Proposition 2.4, and the implication (3) ⇒ (4) is obvious. Thus it suffices to prove (4) ⇒ (1). So let A and B be $(0, 1)$ circulants with residue sets $\mathcal{A} := \{a_1, \ldots, a_k\}_n$ and $\mathcal{B} := \{b_1, \ldots, b_k\}_n$, where $k \le 3$, and suppose that AA^T and BB^T are similar. To complete the proof, we must show that $\mathcal{A}$ and $\mathcal{B}$ are affinely equivalent. For $k \le 2$ this was proved in Theorem 3.1, so suppose $k = 3$. By Proposition 4.2, it suffices to prove that $\hat{\mathcal{A}} := \Delta(\mathcal{A})$ and $\hat{\mathcal{B}} := \Delta(\mathcal{B})$ are linearly equivalent. On the other hand, since AA^T and BB^T are similar, they have the same eigenvalues; recalling their eigenvalues from (1), it follows that

$$\left\{ \sum_{1\le i,j\le 3} \zeta^{(a_i-a_j)r} : 0 \le r < n \right\} = \left\{ \sum_{1\le i,j\le 3} \zeta^{(b_i-b_j)r} : 0 \le r < n \right\},$$

where ζ is a fixed primitive n^{th} root of unity. Write $\alpha_i := \zeta^{a_i - a_{i+1}}$ for $1 \le i \le 3$, where arithmetic on indices is done modulo 3. Then the α_i

are n^{th} roots of unity with $\prod_{i=1}^{3}\alpha_i = 1$. Put $\mathfrak{A} := \{\alpha_1, \alpha_2, \alpha_3, \bar{\alpha}_1, \bar{\alpha}_2, \bar{\alpha}_3\}$. Define β_i and $\mathfrak{B}$ similarly. Then the equality of eigenvalues implies that

$$\left\{\sum_{\phi\in\mathfrak{A}} \phi^r : 1 \le r \le n\right\} = \left\{\sum_{\psi\in\mathfrak{B}} \psi^r : 1 \le r \le n\right\}.$$

Now Theorem 6.1 implies there is an integer u coprime to n such that $\mathfrak{A} = \{\psi^u : \psi \in \mathfrak{B}\}$. Since $\mathfrak{A} \cup \{1, 1, 1\} = \{\zeta^a : a \in \hat{\mathcal{A}}\}$, it follows that $\hat{\mathcal{A}} = u\hat{\mathcal{B}}$, which as noted above is sufficient to complete the proof. □

Our proof of Theorem 6.1 uses the following lemmas.

Lemma 6.2. *Suppose $\mathfrak{A}$ and $\mathfrak{B}$ are multisets of n^{th} roots of unity with $\#\mathfrak{A} = \#\mathfrak{B}$, and the multisets $\mathcal{E} := \{\sum_{\phi\in\mathfrak{A}} \phi^r : 1 \le r \le n\}$ and $\{\sum_{\psi\in\mathfrak{B}} \psi^r : 1 \le r \le n\}$ are the same. Then the least common multiple $m_{\mathfrak{A}}$ of the orders of the elements of $\mathfrak{A}$ equals the corresponding $m_{\mathfrak{B}}$. Moreover, $\mathcal{E}$ consists of $n/m_{\mathfrak{A}}$ copies of $\{\sum_{\phi\in\mathfrak{A}} \phi^r : 1 \le r \le m_{\mathfrak{A}}\}$.*

Proof. This is similar to Proposition 2.5. The number $\sum_{\phi\in\mathfrak{A}} \phi^r$ equals $\#\mathfrak{A}$ precisely when r is divisible by the stated least common multiple $m_{\mathfrak{A}}$, so the number of such r in $\{1, 2, \dots, n\}$ equals $n/m_{\mathfrak{A}}$. Since $\#\mathfrak{A} = \#\mathfrak{B}$, it follows that $n/m_{\mathfrak{A}} = n/m_{\mathfrak{B}}$ and thus $m_{\mathfrak{A}} = m_{\mathfrak{B}}$. The final assertion is obvious. □

Lemma 6.3. *Suppose $\{\alpha_1, \dots, \alpha_k\}$ is a set of roots of unity which includes two complex conjugate roots of unity. Let m be the least common multiple of the orders of the various α_i/α_j. Then every α_i has order dividing $2m$.*

Proof. If $\alpha_i = \bar{\alpha}_k$ then $\alpha_i^2 = \alpha_i\bar{\alpha}_k = \alpha_i/\alpha_k$ is an m^{th} root of unity, so α_i is a $(2m)^{\text{th}}$ root of unity. Since every α_i/α_j is an m^{th} root of unity, it follows that every α_j has order dividing $2m$. □

We now prove our main result.

Proof of Theorem 6.1. Suppose the multisets $\mathfrak{A}$ and $\mathfrak{B}$ provide a counterexample. By Lemma 6.2, we may assume that n is the least common multiple of the orders of the elements of $\mathfrak{A}$, and also that n is the corresponding least common multiple for $\mathfrak{B}$. By hypothesis, the sum of the elements of $\mathfrak{A}$ equals the sum of the r^{th} powers of the elements of $\mathfrak{B}$, for some r. Thus $\sum_{\alpha\in\mathfrak{A}} \alpha + \sum_{\beta\in\mathfrak{B}} (-\beta^r) = 0$ is a vanishing sum of twelve roots of unity. For notational convenience, we will write this vanishing sum as $\sum_{j=1}^{3}(\gamma_j + \bar{\gamma}_j - \delta_j - \bar{\delta}_j)$, where $\prod \gamma_j = 1 = \prod \delta_j$ and where moreover all γ_j's and δ_j's are n^{th} roots of unity and n is the least common multiple of the orders of either the γ_j's or the δ_j's. Note that multiplying the sum by -1 has the affect of switching the γ_j's and δ_j's.

In what follows, we implicitly use this symmetry, as well as possibly relabeling the γ_j's and δ_j's or replacing all the γ_j's (or δ_j's) by their complex conjugates.

First we treat some small values of n, namely the values $n \in \{840, 132, 90\}$ and their divisors. A simple MAGMA program verifies the result in these cases.

Henceforth assume n does not divide 840, and consider a minimal vanishing subsum which includes a root of unity whose order does not divide 420. First suppose this subsum includes two complex conjugate roots of unity. Let m be the least common multiple of the orders of the ratios of roots of unity involved in the subsum. By Lemma 6.3, every root of unity in the subsum has order dividing $2m$. By Lemma 5.1, m divides either $2 \cdot 3 \cdot 5 \cdot 7 = 210$ or $2 \cdot 3 \cdot 11 = 66$, so we must have $m \mid 66$ and $11 \mid m$. Since $11 \mid m$, Lemma 5.1 implies that the subsum has weight twelve, and all twelve roots of unity have order dividing 132, so $n \mid 132$, a case which was treated by our MAGMA program.

Thus any root of unity in our vanishing sum whose order does not divide 420 must be contained in a minimal vanishing subsum which does not include two complex conjugates, and hence has weight at most six. Consider one such subsum.

If the weight is six then the sum includes one element from each pair $(\gamma_j, \bar{\gamma}_j)$ and one from each pair $(-\delta_j, -\bar{\delta}_j)$. By Lemma 5.1, every element of the sum is a 30^{th} root of unity times some fixed constant c. Since $\prod \gamma_j = 1$, we see that either c or c^3 is a 30^{th} root of unity. Thus $n \mid 90$, a case which was treated by our MAGMA program.

If the weight is five then we may assume the sum includes one element from each pair $(\gamma_j, \bar{\gamma}_j)$ and one from $(-\delta_1, -\bar{\delta}_1)$ and one from $(-\delta_2, -\bar{\delta}_2)$. By Corollary 5.2, the roots of unity in this sum are fifth roots of unity times one another. Since $\prod \gamma_j = 1$, we see as above that the γ_j are 15^{th} roots of unity, so δ_1 and δ_2 are 30^{th} roots of unity. Thus $\delta_3 = 1/(\delta_1\delta_2)$ has order dividing 30. But $\delta_3 + \bar{\delta}_3 = 0$ implies $\delta_3 = -\bar{\delta}_3 = -1/\delta_3$, so $\delta_3^2 = -1$, a contradiction.

There are no minimal vanishing sums of weight four, by Corollary 5.2.

Suppose the weight is three. By Corollary 5.2, the three roots of unity in the sum are cube roots of unity times one another (and all three are distinct). Since the sum involves an element of order not dividing 420, it follows that all three roots of unity in the sum have order not dividing 420. If the sum includes only elements of the form $\gamma_j^{\pm 1}$, then since $\prod \gamma_j = 1$ we see that the γ_j's are cube roots of unity, a contradiction. Thus, without loss we may assume the sum is $\gamma_1 + \gamma_2^{\pm 1} - \delta_1$. Since the order of $-\delta_1$ does not divide 420, and $\delta_2\delta_3 = 1/\delta_1$, we may assume the order of δ_2 does not divide 420. Thus the minimal vanishing subsum involving $-\delta_2$ does not include any complex conjugates, and has weight at most three. The possibilities are

(1) $\gamma_3^{\pm 1} - \delta_2 - \delta_3^{\pm 1} = 0$
(2) $-\delta_2 - \delta_3^{\pm 1} = 0$
(3) $\gamma_3^{\pm 1} - \delta_2 = 0$.

In case (2) we have $\gamma_3 + \bar{\gamma}_3 = 0$, so $\gamma_3 = \pm\iota$ has order 4. In cases (1) and (3), $\gamma_3^{\pm 1}$ is a sixth root of unity times δ_2, so the order of γ_3 does not divide 420. Thus in every case γ_3 is not a cube root of unity, so $\bar{\gamma}_2$ is not a cube root of unity times γ_1.

Hence the minimal vanishing subsum involving γ_1 is $\gamma_1 + \gamma_2 - \delta_1$, so $\gamma_2 = \omega\gamma_1$ and $\delta_1 = -\omega^2\gamma_1$ where ω is a primitive cube root of unity. Thus $\gamma_3 = \omega^2/\gamma_1^2$.

In case (2) we have $\delta_2 = -\delta_3^{\pm 1}$ and $\gamma_3 = \pm\iota$, so γ_1 and γ_2 have order 24 while δ_1 has order 8, so we must have $\delta_2 = -\delta_3$ and thus δ_2 and δ_3 have order 16. But then $\#\langle\gamma_1,\gamma_2,\gamma_3\rangle = 24$ and $\#\langle\delta_1,\delta_2,\delta_3\rangle = 16$, which is a contradiction since neither of 16 or 24 divides the other. In case (3) we have $\delta_2 = \gamma_3^{\pm 1}$ and $\delta_3 = \pm\iota$, so $\delta_2 = 1/(\delta_1\delta_3) = \pm\iota\omega/\gamma_1$; since $\gamma_3 = \omega^2/\gamma_1^2$, it follows that the order of γ_1 divides 12, a contradiction. So suppose we are in case (1). Since $\delta_1 = 1/(\delta_2\delta_3)$ is not a cube root of unity, it follows that δ_2 is not a cube root of unity times $\bar{\delta}_3$, so we must have $\gamma_3^{\pm 1} - \delta_2 - \delta_3 = 0$. By Corollary 5.2, $\delta_2\delta_3 = \gamma_3^{\pm 2} = (\omega/\gamma_1^4)^{\pm 1}$, but also $\delta_2\delta_3 = 1/\delta_1 = -\omega/\gamma_1$, so the order of γ_1 divides 30, a contradiction.

We have shown that every summand whose order does not divide 420 is involved in a minimal vanishing sum of weight two. Suppose $\{\gamma_j, \bar{\gamma}_j : 1 \le j \le 3\} = \{\delta_j, \bar{\delta}_j : 1 \le j \le 3\}$. From the definition of the γ_j and δ_j, it follows that $\{\alpha_j, \bar{\alpha}_j : 1 \le j \le 3\} = \{\beta_j^r, \bar{\beta}_j^r : 1 \le j \le 3\}$. In particular, the least common multiple of the orders of the β_j^r equals the corresponding least common multiple for the α_j, which we know equals the corresponding least common multiple for the β_j, namely n. Thus r is coprime to n, contradicting our assumption that the α_j and β_j are a counterexample to the desired result.

Next suppose that $\gamma_1 = -\gamma_2$ and the order of γ_1 does not divide 840. Then $\gamma_3 = -1/\gamma_1^2$ has order not dividing 420, so we may assume $\gamma_3 = \delta_3$. Next, $\delta_1\delta_2 = 1/\delta_3$ has order not dividing 420, so we may assume δ_1 has order not dividing 420, whence $\delta_1 = -\delta_2^{\pm 1}$. We do not have $\delta_1 = -1/\delta_2$, since that would imply $\delta_3 = -1$. Thus $\delta_1 = -\delta_2$, so $-1/\gamma_1^2 = \gamma_3 = \delta_3 = -1/\delta_1^2$, whence $\gamma_1 = \pm\delta_1$. Thus $\{\gamma_1, \gamma_2, \gamma_3\} = \{\delta_1, \delta_2, \delta_3\}$, and we have already achieved a contradiction in this situation.

Suppose that $\gamma_1 = \delta_1$ and the order of γ_1 does not divide 840. Since $\gamma_1\gamma_2\gamma_3 = 1$, we may assume the order of γ_2 does not divide 840 as well.

Thus, after possibly switching δ_2 and δ_3, we must have either $\gamma_2 = \delta_2^{\pm 1}$ or $\gamma_2 = -\bar{\gamma}_3$. If $\gamma_2 = \delta_2^{\pm 1}$, then $\gamma_3 + \bar{\gamma}_3 - \delta_3 - \bar{\delta}_3$ is a vanishing sum, but there are no minimal vanishing sums of weights four or one so we must have $\gamma_3 = \delta_3^{\pm 1}$, which is a case we have already handled. Thus $\gamma_2 = -\bar{\gamma}_3$, so $\gamma_1 = -1$, contradiction.

Finally, we may assume that the order of α_1 does not divide 840. The minimal vanishing subsum involving α_1 must have weight two, and is not of the form $\alpha_1 + \alpha_j$ or $\alpha_1 - \beta_j^{\pm r}$. The only remaining possibility is $\alpha_1 + \bar{\alpha}_j$; here we know $j \neq 1$, so we may assume $j = 2$, whence $\alpha_3 = -1$. Switching the roles of α_i and β_i, we may also assume that $\beta_2 = -\bar{\beta}_1$ and $\beta_3 = -1$. Since $\alpha_2 = -\bar{\alpha}_1$, at least one of α_1 and α_2 has even order, so by possibly switching α_1 and α_2 we may assume that α_1 has even order. Then $n = \#\langle \alpha_1, \alpha_2, \alpha_3 \rangle = \#\langle \alpha_1 \rangle$. Similarly we may assume that β_1 has even order, so β_1 has order n. Thus there is an r coprime to n such that $\alpha_1 = \beta_1^r$, and it follows that $\alpha_2 = \beta_2^r$ and $\alpha_3 = \beta_3^r$. This again is a contradiction, and as we have now treated every case it follows that the supposed counterexample does not exist. □

In the above argument, we used that all the eigenvalues of AA^T and BB^T are the same. One can actually obtain a lot of information from just the hypothesis that these matrices have a single eigenvalue in common. Namely, by expanding on the above argument, one can show:

Proposition 6.4. *If $\alpha_1, \alpha_2, \alpha_3, \beta_1, \beta_2, \beta_3$ are roots of unity with $\prod \alpha_i = \prod \beta_i = 1$ and $\sum(\alpha_i + \bar{\alpha}_i) = \sum(\beta_i + \bar{\beta}_i)$, then the multisets $\mathfrak{A} = \{\alpha_1, \alpha_2, \alpha_3, \bar{\alpha}_1, \bar{\alpha}_2, \bar{\alpha}_3\}$ and $\mathfrak{B} = \{\beta_1, \beta_2, \beta_3, \bar{\beta}_1, \bar{\beta}_2, \bar{\beta}_3\}$ satisfy one of the following, with $\omega^3 = 1$,$\iota^4 = 1$,$\phi^5 = 1$,$\sigma^7 = 1$,$\mu^8 = 1$,$\nu^{16} = 1$ being roots of unity with the orders indicated.*

1. $\mathfrak{A} = \mathfrak{B}$.
2. $\mathfrak{A} = \{\alpha, -\bar{\alpha}, -1, \bar{\alpha}, -\alpha, -1\}$ *and* $\mathfrak{B} = \{\beta, -\bar{\beta}, -1, \bar{\beta}, -\beta, -1\}$.
3. *After possibly switching $\mathfrak{A}$ and $\mathfrak{B}$ we have one of the following*
   - (a) $\mathfrak{A} = \{\mu, -\mu, -\bar{\mu}^2, \bar{\mu}, -\bar{\mu}, -\mu^2\}$ *and* $\mathfrak{B} = \{\omega, \omega^2, 1, \omega^2, \omega, 1\}$
   - (b) $\mathfrak{A} = \{\phi, \phi^2, \bar{\phi}^3, \bar{\phi}, \bar{\phi}^2, \phi^3\}$ *and*
     $\mathfrak{B} = \{\omega, -\omega\phi^2, -\omega\bar{\phi}^2, \omega^2, -\omega^2\bar{\phi}^2, -\omega^2\phi^2\}$
   - (c) $\mathfrak{A} = \{\omega, \sigma^3\omega, \bar{\sigma}^3\omega, \omega^2, \bar{\sigma}^3\omega^2, \sigma^3\omega^2\}$ *and*
     $\mathfrak{B} = \{-\sigma\omega, -\sigma\omega^2, \bar{\sigma}^2, -\bar{\sigma}\omega^2, -\bar{\sigma}\omega, \sigma^2\}$
   - (d) $\mathfrak{A} = \{\nu, -\nu, -\bar{\nu}^2, \bar{\nu}, -\bar{\nu}, -\nu^2\}$ *and*
     $\mathfrak{B} = \{\omega\nu^2, \omega^2\nu^2, \bar{\nu}^4, \omega^2\bar{\nu}^2, \omega\bar{\nu}^2, \nu^4\}$
   - (e) $\mathfrak{A} = \{\omega, \omega\phi^2, \omega\bar{\phi}^2, \omega^2, \omega^2\bar{\phi}^2, \omega^2\phi^2\}$ *and*
     $\mathfrak{B} = \{\phi, \iota\phi^2, -\iota\bar{\phi}^3, \bar{\phi}, -\iota\bar{\phi}^2, \iota\phi^3\}$
   - (f) *both $\mathfrak{A}$ and $\mathfrak{B}$ are among the multisets (with sum -1)*
     - (i) $\{\sigma, \sigma^2, \bar{\sigma}^3, \bar{\sigma}, \bar{\sigma}^2, \sigma^3\}$;

(ii) $\{\iota\omega, -\iota\omega, \omega, -\iota\omega^2, \iota\omega^2, \omega^2\}$;
(iii) $\{-\omega\phi, -\omega^2\phi, \bar{\phi}^2, -\omega^2\bar{\phi}, -\omega\bar{\phi}, \phi^2\}$.

Note. In the above proposition, there is a solution which uses case 3.f.iii for both $\mathfrak{A}$ and $\mathfrak{B}$ but with ϕ a different primitive fifth root of unity in $\mathfrak{B}$ than $\mathfrak{A}$. This is the only case where we need different choices of $\omega, \iota, \phi, \sigma, \mu$ and ν in $\mathfrak{A}$ and $\mathfrak{B}$.

7. The cases $k = 4$ and $k = 5$

New phenomena occur when we move to $k = 4$. For instance, in Section 2 we showed that the residue sets $\{0, 1, 4, 7\}_8$ and $\{0, 1, 3, 4\}_8$ correspond to $(0, 1)$ circulants which are P-Q equivalent but not affinely equivalent. Also, one can show that the autocorrelation matrices of the circulants corresponding to $\{0, 1, 2, 6\}_{12}$ and $\{0, 2, 3, 6\}_{12}$ are similar, but are not conjugate via a permutation matrix (so the circulants are not P-Q equivalent). These examples show that, when $k = 4$, condition (2) of Theorem 1.1 does not imply condition (1), and condition (4) does not imply condition (3).

Still, for $k = 4$ and $k = 5$ we now show that Theorem 1.1 is true whenever n is not divisible by small primes. As in the case $k = 3$, we proceed by proving $\mathrm{SDA}(n, k)$ and then examining vanishing sums of roots of unity.

Lemma 7.1. $\mathrm{SDA}(n, 4)$ *is true if* n *is odd.* $\mathrm{SDA}(n, 5)$ *is true if* n *is coprime to* 10.

Proof. Suppose $X := \{x_1, x_2, x_3, x_4\}$ and $Y := \{y_1, y_2, y_3, y_4\}$ are 4-element subsets of $\mathbb{Z}/n\mathbb{Z}$ with $\Delta(X) = \Delta(Y)$. Then there is a permutation π of the set T of 2-element subsets of $\{1, 2, 3, 4\}$, and a map $\sigma : T \to \{1, -1\}$, such that

$$(2)\quad x_{\min(A)} - x_{\max(A)} = \sigma(A)(y_{\min(\pi(A))} - y_{\max(\pi(A))}) \quad \text{for every } A \in T.$$

We tested via computer that, for every choice of π and σ, the above identity implies that X and Y are affinely equivalent so long as n is odd. In fact, if we think of the x_i's and y_i's as indeterminates, then there exist $\rho \in S_4$ and $c \in \{1, -1\}$ such that, for each $1 \leq i \leq 3$, the equation

$$(3)\qquad x_i - x_4 = c(y_{\rho(i)} - y_{\rho(4)})$$

is a rational linear combination of the equations (2) (for any fixed choice of π and σ). Moreover, the denominators of the coefficients in this combination have no prime factors besides 2 and 13. This proves $\mathrm{SDA}(n, 4)$ when n is coprime to 26. Values of n which are odd multiples of 13 require an additional argument: for such n, consider a pair (π, σ) for which the above linear combination has a coefficient with denominator divisible by 13. It turns out that $13(x_i - x_j)$ and $13(y_i - y_j)$ are $\mathbb{Z}$-linear combinations of the equations (2), for every $1 \leq i, j \leq 4$, so viewing x_i, y_i as members of $\mathbb{Z}/nZ$, it follows that all the x_i's are congruent to one another mod $n/13$, and likewise the y_i's. We can translate the x_i's and y_i's so that (say) $x_1 = y_1 = 0$, without affecting the pairwise differences between x_i's or y_i's. Thus we may assume that every x_i and y_i is divisible by $n/13$, so it suffices to prove that $\{x_i/(n/13)\}$ and $\{y_i/(n/13)\}$ are affinely equivalent subsets of $\mathbb{Z}/13\mathbb{Z}$. In each case, it turns out that (2) allows one to write every x_i and y_i as a multiple of y_4, so we get two explicit subsets of $\mathbb{Z}/13\mathbb{Z}$ and they do indeed turn out to be affinely equivalent.

We treated the case $k = 5$ in a similar manner. In this case it turns out that there is always a system of equations like (3) which are rational linear combinations of the equations like (2), and the denominators of the coefficients in these combinations are not divisible by any primes besides 2 and 5. □

Remark. Experimentally, it seems that $\mathrm{SDA}(n, 4)$ fails if and only if n is divisible by 8, and that $\mathrm{SDA}(n, 5)$ fails if and only if $n > 8$ and $\gcd(n, 10) > 1$. However, such refinements of Lemma 7.1 would not affect our next result.

Theorem 7.2. *If $k \in \{4, 5\}$ and every prime factor of n is greater than $2k(k-1)$, then the properties (1), (2), (3), (4) from Theorem 1.1 are equivalent conditions on n-by-n $(0, 1)$ circulants A and B of weight k.*

Proof. Suppose k and n satisfy the hypotheses. If the circulants corresponding to $\mathcal{A} := \{a_1, \ldots, a_k\}_n$ and $\mathcal{B} := \{b_1, \ldots, b_k\}_n$ have similar autocorrelation matrices, then as in the previous section by considering eigenvalues we find a vanishing sum S of $2k(k-1)$ $(2n)^{\text{th}}$ roots of unity. By Lemma 5.1, since the prime factors of n are larger than $2k(k-1)$, every minimal vanishing subsum of S must be a pair $(\alpha, -\alpha)$. Since n is odd, no two n^{th} roots of unity are negatives of one another, so we must have an equality of multisets

$$\{\zeta^{a_i - a_j} : 1 \leq i, j \leq k\} = \{\zeta^{(b_i - b_j)u} : 1 \leq i, j \leq k\}$$

for some integer u, where ζ is a primitive n^{th} root of unity. By Lemma 6.2, we may assume $\gcd(u, n) = 1$. Thus, the multisets of differences $\Delta(\mathcal{A})$ and $\Delta(\mathcal{B})$ are linearly equivalent, so Lemma 7.1 implies $\mathcal{A}$ and $\mathcal{B}$ are affinely equivalent. □

8. The situation for $k > 5$

When $k \geq 6$, there are examples showing that our spectral approach will not work, even if the prime factors of n are large. More precisely, for every $k \geq 6$ and every $n > 2k+10$, we will exhibit two n-by-n weight-k $(0,1)$ circulants which are not P-Q equivalent but yet have the same autocorrelation matrices. We emphasize that this shows one cannot relate P-Q equivalence to affine equivalence by means of autocorrelation similarity; but it may still be true for $k \geq 6$ that P-Q equivalence and affine equivalence are related for some other reason.

For $k \geq 6$, consider the sets of integers $\mathcal{A}$ and $\mathcal{B}$ defined as the complements in $\{0,1,2,\dots,k+5\}$ of the sets $\{1,2,4,6,k+1,k+2\}$ and $\{1,3,6,k+1,k+2,k+3\}$, respectively. In other words,

$$\mathcal{A} = \{0,3,5,k+3,k+4,k+5\} \cup \{7,8,9,\dots,k\}$$

and

$$\mathcal{B} = \{0,2,4,5,k+4,k+5\} \cup \{7,8,9,\dots,k\}.$$

We will show that $\mathcal{A}$ and $\mathcal{B}$ have the same multisets of differences, i.e., $\Delta(\mathcal{A}) = \Delta(\mathcal{B})$, but that for any $n > 2k+10$ they define n-by-n $(0,1)$ circulants which are not P-Q equivalent.

Proposition 8.1. *If $k \geq 6$ then $\Delta(\mathcal{A}) = \Delta(\mathcal{B})$.*

Proof. We compute $\Delta(\mathcal{A}) \setminus \Delta(\mathcal{A} \cap \mathcal{B})$. Since $\mathcal{A} \setminus (\mathcal{A} \cap \mathcal{B}) = \{3, k+3\}$, this consists of all differences between two elements of $\mathcal{A}$ which involve 3 or $k+3$. Thus, this is the multiset of elements $\pm i$ with i in the union of the two multisets $\{-3,0,2,k,k+1,k+2,4,5,6,\dots,k-3\}$ and $\{-k-3,-k+2,0,1,2,4-k,5-k,6-k,\dots,-3\}$. The corresponding multiset for $\mathcal{B}$ is the union of $\{-2,0,2,3,k+2,k+3,5,6,7,\dots,k-2\}$ and $\{-4,0,1,k,k+1,3,4,5,\dots,k-4\}$. Thus $\Delta(\mathcal{A}) \setminus \Delta(\mathcal{A} \cap \mathcal{B}) = \Delta(\mathcal{B}) \setminus \Delta(\mathcal{A} \cap \mathcal{B})$, so $\Delta(\mathcal{A}) = \Delta(\mathcal{B})$. □

Let $\mathcal{A}_n$ and $\mathcal{B}_n$ be the images of $\mathcal{A}$ and $\mathcal{B}$ in $\mathbb{Z}/n\mathbb{Z}$, and let A_n and B_n be the corresponding n-by-n circulants.

Proposition 8.2. *If $k \geq 6$ and $n > 2k+10$, then A_n and B_n are not P-Q equivalent.*

Proof. First assume $k \geq 9$. The top row of A_n has dot-product 1 with precisely ten rows of A_n, namely the shifts of the top row by $k+1,\dots,k+5$ in either direction. The bound $n > 2k+10$ ensures that in computing these dot-products, it suffices to add or subtract an integer from the indices: we need not reduce the indices mod n. Likewise, the top row of A_n has dot-product 2 with precisely two rows of A_n, namely the shifts of the top row by $k-1$ in either direction.

The componentwise product of the top row of A_n with the sum of these twelve rows is the vector

$$\mathbf{a} := (4, 0, 0, 2, 0, 1, 0, 0, \dots, 0, 1, 0, 0, 0, 1, 3, 2, 0, 0, \dots),$$

where the '4' occurs in position 0 and the '3' occurs in position $k+4$. The corresponding product for B is

$$\mathbf{b} := (3, 0, 2, 0, 1, 1, 0, 0, \dots, 0, 1, 0, 0, 0, 0, 3, 3, 0, 0, \dots),$$

where the entries '3' are in positions 0, $k+4$ and $k+5$. If B_n were gotten by permuting the rows and columns of A_n, then $\mathbf{b}$ would be a permutation of $\mathbf{a}$. But this is not the case, since '4' is an entry in $\mathbf{a}$ but not in $\mathbf{b}$.

If $6 \le k \le 8$ then the top row of A_n has dot-product 2 with more than two rows of A_n, but its componentwise product with the sum of all such rows is not a permutation of the corresponding product for B_n. This proves the result in every case. □

9. Relationship with the Ádám problem

A much-studied problem is the

Ádám Problem. For which n do there exist n-by-n $(0, 1)$ circulants A and B which are not linearly equivalent but for which $B = PAP^{-1}$ for some permutation matrix P?

Actually, Ádám made the conjecture that this P-P^{-1} equivalence was always the same as linear equivalence, but a counterexample was published soon thereafter. This led many authors to seek ways to weaken the original conjecture to make it true.

This problem resembles the problem studied in this paper, which we now rename:

Bipartite Ádám Problem. Describe the $(0, 1)$ circulants A and B which are not affinely equivalent but for which $B = PAQ$ for some permutation matrices P and Q.

Ádám was interested in isomorphisms between directed graphs that had prescribed vertex transitive symmetry groups, in this case the cyclic group. Our problem asks the same question for directed bipartite graphs which have the same group acting on each part.

Muzychuk has given a magnificent solution to the original Ádám problem [9]: the answer is all n which are divisible by either 8 or by the square of an odd prime. His proof uses detailed considerations of Schur algebras, among other things. As far as we know, the n's occurring in solutions to the bipartite Ádám problem might be precisely the n's which solve the Ádám problem; however, it seems that Muzychuk's method does not apply to the bipartite problem. We note, however, that Babai's group-theoretic proof of the Ádám conjecture in the case of prime n can be extended (with some effort) to the bipartite situation.

There is evidence that these are different problems. The first counterexample to the Ádám conjecture (from [5]) was the pair of circulants $\{1,2,5\}_8$ and $\{1,5,6\}_8$. On the other hand, Theorem 1.1 shows that there are no weight three "counterexamples" (permutation equivalent but not affinely equivalent) for the bipartite Ádám problem.

However, there is often a connection between counterexamples in the two problems. Our original counterexample of circulants that are P-Q but not affinely equivalent was $\{0,1,4,7\}_8$ and $\{0,1,3,4\}_8$. These two circulants do not directly form a counterexample for the Ádám problem because they are not P-P^{-1} equivalent. But the affine equivalence class of $\{0,1,4,7\}_8$ includes $\{0,1,2,5\}_8$, which is P-P^{-1} equivalent to $\{0,1,5,6\}_8$, which in turn is affinely equivalent to $\{0,1,3,4\}_8$. Thus, by picking different members of the two affine equivalence classes, we can turn our bipartite Ádám counterexample into an Ádám counterexample.

We did some computer searches to find bipartite Ádám counterexamples, and most of the examples we found were affinely equivalent to Ádám counterexamples. However, in weight six there are bipartite Ádám counterexamples like $\{0,1,2,5,8,10\}_{16}$ and $\{0,2,3,7,8,10\}_{16}$ which are not affinely equivalent to Ádám counterexamples. We do not know how rare such examples will be for larger weights.

10. Acknowledgements and Future Directions

It is a pleasure to thank Bradley Brock for helpful discussions on vanishing sums of roots of unity, and Marshall W. Buck for help with equation solving.

There are several different directions for future research depending on what equivalence relations and what parameter ranges are of the most interest. For larger densites, say $k \approx n/2$, it may still be true that the autocorrelation spectra usually determine the affine equivalence classes.

In some applications it is natural to study sparse circulants whose nonzero entries can be -1 as well as 1. Also, the notion of spectral equivalence could be relaxed to simply having the same mimimal polynomial or having the same characteristic polynomial modulo some fixed prime.

References

[1] B. Alspach and T. D. Parsons, *Isomorphism of circulant graphs and digraphs*, Discrete Math. **25** (1979), 97–108.

[2] L. Babai, *Isomorphism problem for a class of point-symmetric structures*, Acta Math. Ada. Sci. Hung. **29** (1977), 329–336.

[3] P. J. Davis, Circulant Matrices, 2nd ed., Chelsea, 1994.

[4] D. Ź. Djoković, *Isomorphism problem for a special class of graphs*, Acta Math. Acad. Sci. Hung. **21** (1970), 267–270.

[5] B. Elspas and J. Turner, *Graphs with circulant adjacency matrices*, J. Comb. Th. **9** (1970), 297–307.

[6] Q. Huang and A. Chang, *Circulant digraphs determined by their spectra*, Discrete Math. **240** (2001), 261–270.

[7] H. B. Mann, *On linear relations between roots of unity*, Mathematika **12** (1965), 107–117.

[8] B. Mans, F. Pappalardi and I. Shparlinski, *On the spectral Ádám property for circulant graphs*, Discrete Math. **254** (2002), 309–329.

[9] M. Muzychuk, *A solution of the isomorphism problem for circulant graphs*, Proc. London Math. Soc. (3) **88** (2004), 1–41.

[10] P. P. Pálfy, *Isomorphism problem for relational structures with a cyclic automorphism*, Europ. J. Combinatorics **8** (1987), 35–43.

[11] B. Poonen and M. Rubinstein, *The number of intersections of the diagonals of a regular polygon*, SIAM J. Discrete Math. **11** (1998), 135–156.

Center for Communications Research, 805 Bunn Drive, Princeton, NJ 08540

E-mail address: `doug@idaccr.org`

E-mail address: `zieve@math.rutgers.edu`

URL: `www.math.rutgers.edu/∼zieve/`