AUTOMORPHISM GROUPS AND SPECTRA OF CIRCULANT GRAPHS

MAX GOLDBERG

Abstract. We explore ways to concisely describe circulant graphs, highly symmetric graphs with properties that are easier to generalize than other graphs. We introduce connection sets as a way to describe isomorphism among some circulant graphs and discuss Ádám's conjecture that attempts to generalize this idea to all circulant graphs, exploring cases in which the conjecture holds and cases in which it fails.

Contents

1. Preliminaries

We begin by defining groups and graphs along with other necessary objects.

Definition 1.1. A *group* $(G, \cdot)$ is an ordered pair consisting of a set G and a binary operation $\cdot : G \times G \to G$ that fulfills the following three properties:

(1) $x \cdot (y \cdot z) = (x \cdot y) \cdot z$ for all $x, y, z \in G$
(2) There exists $e \in G$ such that for all $g \in G$, $e \cdot g = g \cdot e = g$
(3) For all $g \in G$, there exists $g^{-1} \in G$ such that $g \cdot g^{-1} = g^{-1} \cdot g = e$.

Definition 1.2. Let $(G, \cdot)$, $(H, \star)$ be groups. A map $\phi : G \to H$ is a *homomorphism* if $\phi(a \cdot b) = \phi(a) \star \phi(b)$ for all $a, b \in G$.

In other words, ϕ preserves the group structure of G inside H. This allows us to define an equivalence relation on groups.

An *isomorphism* is a homomorphism that is bijective. An isomorphism allows us to create an inverse homomorphism, making the two groups look essentially the same. Formally, if there exists an isomorphism between two groups G and H, we say that G and H are *isomorphic*, denoted by $G \cong H$. We regard isomorphic groups as equivalent, differing only in notation.

Definition 1.3. Let G be a group. Then, a nonempty subset $S \subseteq G$ is a *subgroup* of G if $s \in S$ implies $s^{-1} \in S$, and $s, t \in S$ implies $st \in S$.

Date: AUGUST 29, 2016.

Groups appear in a variety of fields and can be difficult to represent and understand, but we will be mainly concerned with one of the simplest types of groups, the cyclic group. A group is cyclic if there exists an element $g \in G$ such that for all $h \in G$, $g^n = h$ for some integer n, where exponentiation represents repeated application of the group operation. The element g is called the generator of the group, although it is not necessarily unique.

Cyclic groups have a simple structure that admit a definition using addition of integers. Let the elements of Z/nZ be the integers from 0 to $n-1$ and let the group operation be addition modulo n. Then the element 1 clearly generates the group. It can be easily shown that if G is a finite cyclic group of order n, then G is isomorphic to the group Z/nZ. Additionally, all infinite cyclic groups are isomorphic to the group of integers under addition. The following result completely characterizes which elements can be a generator of Z/nZ.

Lemma 1.4. *A subset $S \subseteq Z/nZ$ generates Z/nZ if and only if* $\gcd(S \cup \{n\}) = 1$.

Proof. Suppose $gcd(S \cup \{n\}) \neq 1$, call that number x. Then, any integer combination of the elements of $S \cup \{n\}$ modulo n is still divisible by x and will never sum to 1.

Suppose $gcd(S \cup \{n\}) = 1$. Bézout's lemma tells us that there exist integers x_s, y such that

$$\sum_{s \in S} x_s s + yn = 1.$$

Taking the congruence modulo n, we have found an integer combination that sums to 1. Since 1 is always a generator of Z/nZ, we can reach any element by combining this sum $\sum_{s \in S} x_s s$ an appropriate number of times. □

An immediate corollary is that if n is prime, any nonzero element of Z/nZ is a generator.

Definition 1.5. An *action* of a group G on a mathematical object X is a map from $G \times X \to X$ such that

(1) $e \cdot x = x$ for all $x \in X$
(2) $g \cdot (h \cdot x) = (gh) \cdot x$ for all $g, h \in G$ and $x \in X$.

We denote G acting on X by $G \curvearrowright X$. We say that G acts *faithfully* on X if, for all $g \in G \setminus \{e\}$, there exists $x \in X$ such that $g \cdot x \neq x$. So, there is no element of G that acts on X in the same way that the identity element does.

From now on, we will indicate the group operation by juxtaposition and the group action by a dot (i.e. $g \cdot x$ for $g \in G$ and $x \in X$).

Definition 1.6. A group G acting on a set X is *transitive* if for all $x, y \in X$, there exists $g \in G$ such that $g \cdot x = y$.

Another useful definition is that of an orbit. If $G \curvearrowright X$ and $x \in X$, the orbit G_x of x is the image of x under G, i.e. $G_x = \{g \cdot x : g \in G\}$. A group action is transitive if there is only one orbit.

Now, we will give precise but abstract definitions for graphs.

Definition 1.7. An *undirected graph* $G = (V, E)$ is an ordered pair of a set of vertices V and a multiset of edges E where for all $e \in E$, $e = \{v, w\}$ for some distinct $v, w \in V$.

If $\{v, w\} \in E$, we say that v and w are adjacent, or $v \sim w$. Additionally, if $v \in e \in E$, we say that e is incident on v.

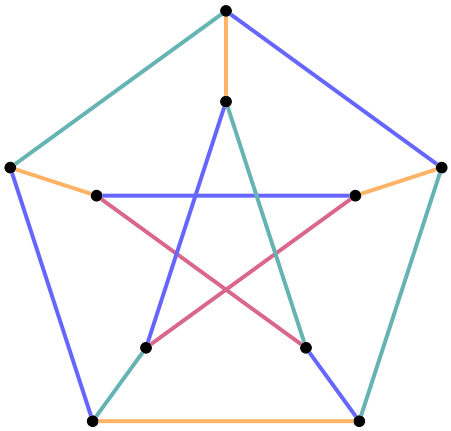
Definition 1.8. A *directed graph* (or digraph) $G = (V, E)$ is an ordered pair of a set of vertices V and a multiset of edges E where for all $e \in E$, $e = (v, w)$ for some $v, w \in V$.

If for $G = (V, E)$ there are no duplicate edges in E, we say that G is a simple graph. Note that adjacency is not symmetric for directed graphs. In other words, $v \sim w$ does not necessarily imply $w \sim v$. If $v \sim w$ implies $w \sim v$ for all vertices in a directed graph, we can represent it more simply as an undirected graph.

We will often associate objects to vertices and edges in the graph. In other words, we make mappings from V or E to other sets. This is called a vertex coloring or edge coloring respectively, or in general, decorations on the graph. Though there is much to study in creating vertex and edge decorations for a given graph, we will only use them to track edges when constructing a graph.

A few other definitions will be useful. The *degree* of a vertex v is the number of edges e incident to v. In addition, a graph is *connected* if there is a continuous path of edges between any two vertices, regardless of edge orientation.

It will often be easier to consider graphs as geometric structures. A common example is the Petersen graph, a highly symmetric graph with some unusual properties for a graph of its size. This diagram illustrates an edge coloring.



Groups are often used to formalize the symmetries, or automorphisms, of mathematical objects. The structure of this symmetry group can help us understand the structure of the graph itself.

Definition 1.9. The *automorphism group* of a simple undirected graph $G = (V, E)$, denoted $Aut(G)$, is the set of all permutations $\sigma : V \to V$ such that, for all $v, w \in V$, $v \sim w$ if and only if $\sigma(v) \sim \sigma(w)$, where the group operation is composition of permutations.

When we speak of groups acting on graphs, we are actually speaking of groups acting on the vertices of the graph. Also, we generally wish for the group action to preserve adjacency. So, a group G acting on a graph Γ is a homomorphism from G to $Aut(\Gamma)$.

We say that a graph $G = (V, E)$ is vertex transitive if its automorphism group acts transitively on the vertices of G. In other words, for all $v, w \in V$, there exists

$g \in Aut(G)$ such that $g \cdot v = w$. Similarly, we say that a graph is edge transitive if its automorphism group acts transitively on the edges of G.

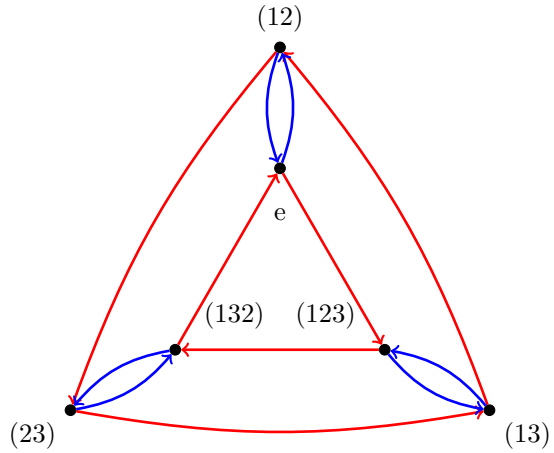
If a graph is vertex transitive, then all vertices have the same degree.

2. Cayley Graphs

Similarities in the definitions of groups and graphs motivate a construction of a graph from a given group that relates the elements of the group to the vertices of the graph.

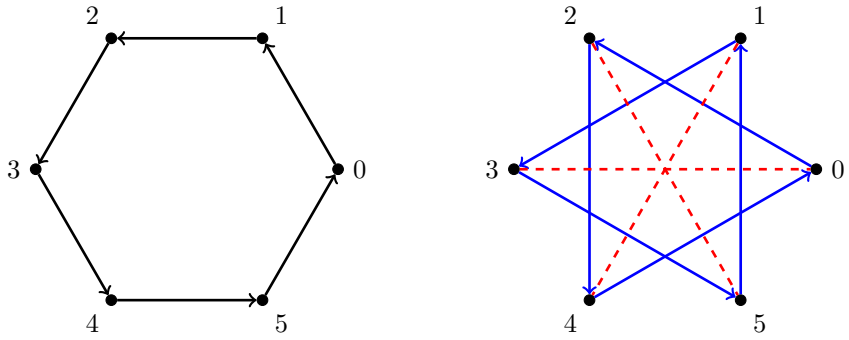
Suppose G is a group generated by the finite set S. We will construct a directed graph, $Cay(G, S)$, that represents the group. Make the vertex set of $Cay(G, S)$ to be the set of elements of G. For each vertex v_g and each $s \in S$, construct a directed edge from v_g to v_{gs}. Generally we will associate each edge with the generator used to generate it, often indicated by an edge coloring. The graph constructed here is called the Cayley graph of G generated by S.

We will present some examples of Cayley graphs to see how they can represent groups in a useful way. The symmetric group S_n is the set of all permutations of n elements where the group operation is composition. Below is the Cayley graph of S_3 generated by $\{(12), (123)\}$, where red arrows are (123) and blue arrows are (12).



Naturally, the structure of Cayley graphs changes dramatically with the generating set. Both graphs below are Cayley graphs of $Z/6Z$, but on the left the generating set is $\{1\}$ and on the right the generating set is $\{2, 3\}$. For edges corresponding to the generator 3 (which is its own inverse), we have used a dashed line

to indicate two opposite directed edges in the graph.



These varied graphs lead us to the question of which graphs can be interpreted as Cayley graphs. The following theorem characterizes which digraphs are Cayley graphs of a group.

Theorem 2.1. *A digraph $\Gamma = (V, E)$ with an edge coloring is a Cayley graph of a group G generated by S if and only if all of the following are true:*

(1) For all $s \in S$, for all $v \in V$, there exists a single edge corresponding to s leading in and out of v
(2) Γ is connected
(3) Γ is vertex-transitive.

Proof. Suppose Γ is a Cayley graph of G generated by S. Since each element $g \in G$ corresponds with a vertex $v_g \in V$, for each $s \in S$, there is no more than one edge leading out from v_g to v_{gs}. There is also no less than one edge, since $gs \neq gs'$ if $s \neq s'$. Since the same is true for s^{-1}, there is exactly one edge leading in and out of v_g.

Now, suppose $g, h \in G$. By the definition of a generating set, we can combine the generators and their inverses to get from v_e to v_g and from v_e to v_h. So, there is a path from v_g to v_h by following v_g to v_e and then to v_h. Therefore Γ is connected.

Now, let $g \in G$ and let $L_g(x) = g \cdot x$ be a left translation by g. We will show that the action L_g is an automorphism on Γ, i.e., that it preserves adjacency and non-adjacency. Indeed,

$$(v_{g'}, v_{g''}) \in E \iff (g')^{-1}g'' \in S \iff (gg')^{-1}gg'' \in S \iff (L_g(v_{g'}), L_g(v_{g''})) \in E.$$

So Γ is vertex transitive.

To show the converse, let Γ be a graph with properties (1), (2), and (3). Construct G by associating each vertex in Γ with an element in G and construct S by associating each edge leaving a vertex with an element in S. Then the product v_{gh} can be computed using the sequence of generators for h. Track which edges are used to go from v_e to v_h. Then follow those edges corresponding to those generators but starting from v_g. This will give the vertex v_{gh}. □

Theorem 2.2. *The group G acts on $Cay(G, S)$ faithfully and the elements of G are automorphisms of $Cay(G, S)$.*

Suppose there exists $g \in G$ such that $g \cdot Cay(G, S) = Cay(G, S)$, where the graphs are equal and not just isomorphic. Then, $v_h \mapsto v_{gh}$ implies that $h = gh$. Therefore g is the identity of the group.

Let $g \in G$. Then, $g \cdot Cay(G, S)$ takes v_h to v_{gh}. Since we use left multiplication for the group action, but right multiplication for the definition of the edges in the Cayley graph, the structure of the Cayley graph is unchanged. In other words, $v_h \sim v_{hs}$ if and only if $v_{gh} \sim v_{ghs}$.

3. Circulant Graphs

Let $(a_0, \ldots, a_{n-1})$ be an n-tuple. Then, the matrix

$$A = \begin{bmatrix} a_0 & a_1 & a_2 & \cdots & a_{n-1} \\ a_{n-1} & a_0 & a_1 & \cdots & a_{n-2} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ a_1 & a_2 & a_3 & \cdots & a_0 \end{bmatrix}$$

is called a *circulant matrix*. Circulant matrices are useful because they are defined by only their first row. In addition, the eigenvalues and eigenvectors of circulant matrices are easily expressed. In particular, all circulant matrices of a given size have the same set of eigenvectors.

We will leave the following result unproven, although it can be verified with some tedious and not particularly enlightening algebra.

Theorem 3.1. *If A is an $n \times n$ circulant matrix as defined above, then the eigenvectors of A are $v_j = (\omega^j, \omega^{2j}, \omega^{3j}, \ldots, \omega^{nj})$, $j = 1, 2, \ldots, n$ where $\omega = \exp(2\pi i/n)$ is the n-th root of unity. Moreover, the corresponding eigenvalues are*

$$\alpha_j = a_0 + a_1\omega^j + a_2\omega^{2j} + \ldots + a_{n-1}\omega^{(n-1)j}.$$

Consider a (possibly directed) graph G on n vertices labeled $v_1, \ldots, v_n$. Associate a unique number $1, \ldots, n$ with each vertex. Then, the *adjacency matrix* of G is the $n \times n$ matrix $A = (a_{ij})$ where $a_{ij} = 1$ if $v_i \sim v_j$ and 0 otherwise. If the adjacency matrix of a graph is a circulant matrix, we call that graph a *circulant graph*.

Cyclic groups allow us to link Cayley graphs and circulant graphs. The following results formalize this idea.

Theorem 3.2. *If S generates Z/nZ, then the Cayley graph of Z/nZ generated by S is a circulant graph.*

Proof. Numbering the vertices v_i for $i \in \{0, \ldots, n-1\}$, $v_i \sim v_j$ if and only if $j - i \in S$. So the adjacency matrix will have 1 in the columns corresponding to $S + i$ for the i-th row. □

The converse is also true:

Theorem 3.3. *If G is a connected circulant digraph on n vertices, then there exists a generating subset $S \subseteq Z/nZ$ such that G is the Cayley graph of Z/nZ generated by S.*

Proof. Let $A = (a_{ij})$ be a circulant adjacency matrix of G. Let $S = \{j : a_{ij} = 1\}$. Then $Cay(Z/nZ, S)$ is isomorphic to G. □

Theorem 3.4. *Let G be a circulant graph on n vertices with adjacency matrix A. If A has non-repeated eigenvalues, the automorphism group $Aut(G)$ is equal to Z/nZ.*

Proof. We can represent an arbitrary automorphism of G by a permutation matrix $P = (\delta_{p(i),j})$ such that

$$P^{-1}AP = A.$$

Since A has distinct eigenvalues, it can be diagonalized by Ω such that $\Omega A\Omega^{-1} = (\alpha_k\delta_{ik})$ where α_k are eigenvalues of A, δ_{ik} is the Kronecker delta, and

$$\Omega = \begin{bmatrix} \omega & \omega^2 & \cdots & \omega^n \\ \omega^2 & \omega^4 & \cdots & \omega^{2n} \\ \vdots & \vdots & \ddots & \vdots \\ \omega^n & \omega^{2n} & \cdots & \omega^{n^2} \end{bmatrix} = (\omega^{ij})$$

is the matrix whose columns are the eigenvectors of A. Let $D_A = \Omega A\Omega^{-1}$, then $A = \Omega^{-1}D_A\Omega$. Substituting, we have $A = P^{-1}\Omega^{-1}D_A\Omega P$, so $D_A = \Omega P^{-1}\Omega^{-1}D_A\Omega P\Omega^{-1}$. Now, let $T = \Omega P\Omega^{-1}$, then $D_A = T^{-1}D_AT$. So $TD_A = D_AT$.

Let $T = (t_{ij})$. We will now calculate the ik-th entry of TD_A and D_AT:

$$(TD_A)_{ik} = \sum_j t_{ij}\alpha_k\delta_{jk}$$

$$(D_AT)_{ik} = \sum_j \alpha_j\delta_{ij}t_{jk}.$$

Since there is only one nonzero term in each sum, we can equate them, so $t_{ik}\alpha_k = \alpha_it_{ik}$. Since $\alpha_i \neq \alpha_k$ for all $i \neq k$, t_{ik} must vanish for all $i \neq k$. So T is a diagonal matrix.

Since $\Omega P^{-1} = T^{-1}\Omega$ by definition, we can expand the ih-th entry of both sides to get

$$\Omega P^{-1} = \begin{bmatrix} \omega & \omega^2 & \cdots & \omega^n \\ \omega^2 & \omega^4 & \cdots & \omega^{2n} \\ \vdots & \vdots & \ddots & \vdots \\ \omega^n & \omega^{2n} & \cdots & \omega^{n^2} \end{bmatrix} P^{-1} = \omega^{ip(h)}$$

and

$$T^{-1}\Omega = \begin{bmatrix} t_1^{-1} & 0 & \cdots & 0 \\ 0 & t_2^{-1} & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & t_n^{-1} \end{bmatrix} \begin{bmatrix} \omega & \omega^2 & \cdots & \omega^n \\ \omega^2 & \omega^4 & \cdots & \omega^{2n} \\ \vdots & \vdots & \ddots & \vdots \\ \omega^n & \omega^{2n} & \cdots & \omega^{n^2} \end{bmatrix} = t_i^{-1}\omega^{ih}$$

Equating, we have

$$\omega^{ip(h)} = t_i^{-1}\omega^{ih}.$$

Let $\lambda_i \in \mathbb{Z}$ such that $t_i^{-1} = \omega^{\lambda_i}$. So

$$ip(h) \equiv ih + \lambda_i \pmod{n}$$

for all i, h. Setting $i = 1$, this becomes

$$p(h) \equiv h + \lambda_1 \pmod{n}.$$

Therefore P is a cyclic permutation of the vertices encoded by A. □

Why is the restriction that the eigenvalues are distinct needed? Consider an undirected circulant graph, such as a cycle. Then, reflections of the graph are also automorphisms in addition to rotations. So Z/nZ is still a subgroup of the automorphism group, but it is not the entire group. In general, since the adjacency matrix of an undirected graph is symmetric, and since it can be easily shown that symmetric circulant matrices have repeated eigenvalues, we must restrict to distinct eigenvalues.

4. Ádám's Conjecture

The most striking problem that becomes easier for circulant graphs is graph isomorphism. To study this, we introduce another abstract concept to describe circulant graphs that turns out to be useful.

Definition 4.1. If G is a graph on n vertices with circulant adjacency matrix A, the *connection set* of A is the set $C = \{k_1, \ldots, k_m\}$ for integers $0 < k_1 < \cdots < k_m < n$ such that the first row of A is 1 in precisely the k_i positions.

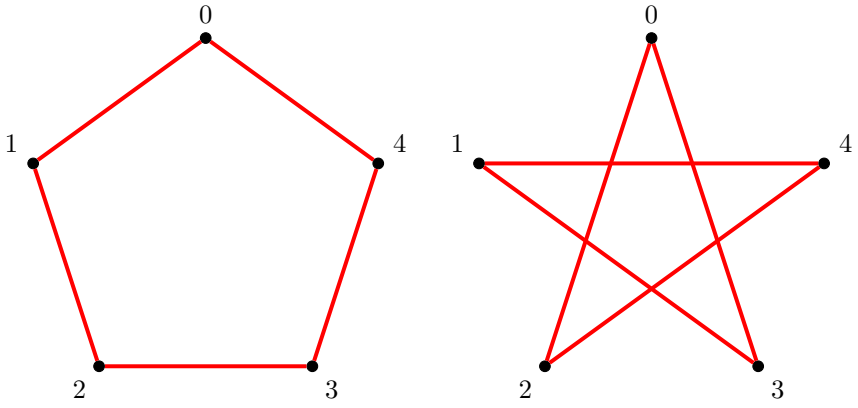
In other words, if the vertices are numbered $v_0, \ldots, v_{n-1}$, v_0 is adjacent to v_j if and only if $j \in C$.

Now, we can introduce an equivalence relation for connection sets. Let $C_1 = \{k_1, \ldots, k_m\}$ and $C_2 = \{k'_1, \ldots, k'_m\}$ be connection sets of graphs G_1 and G_2 on n vertices. Then, we say that C_1 and C_2 are equivalent if there exists a number r coprime to n such that

$$C_2 = \{rk_i : k_i \in C_1\}$$

with multiplication modulo n. We will denote this by $C_2 = rC_1$.

For example, consider the following isomorphic graphs with different vertex numbering:



The connection set of the first is $\{1, 4\}$ and the second is $\{2, 3\}$. Multiplying the first set by 2 gives

$$2 \cdot 1 \equiv 2 \pmod 5 \qquad \text{and} \qquad 2 \cdot 4 \equiv 3 \pmod 5.$$

So the sets are equivalent.

We will show that this relation on connection sets is an equivalence relation.

First, it is reflexive, setting $r = 1$ makes any C equivalent to itself.

Next, we show that it is symmetric. Suppose $rC_1 = C_2$. So $k'_i \equiv rk_i \pmod n$. Because $\gcd(r, n) = 1$, Bézout's lemma guarantees that there are $s, t \in \mathbb{Z}$ such that

$rs + tn = 1$. Since $rs \equiv 1 \pmod{n}$,

$$sk_i' \equiv srk_i \equiv k_i \pmod{n}.$$

So $C_1 = sC_2$.

Finally, we will show that it is transitive. Suppose $rC_1 = C_2$ and $sC_2 = C_3$. Let $t \equiv rs \pmod{n}$. Then, $tC_1 = C_3$.

The power of connection sets is apparent from the following result, along with exploration of its converse. Suppose G_1 and G_2 are circulant graphs on n vertices with connection sets equivalent under our relation. The relation $rC_1 = C_2$ is a mapping on the vertex set taking $v \mapsto rv$. Since this mapping preserves adjacency and non-adjacency, it is an automorphism. Therefore, G_1 and G_2 are isomorphic.

Our equivalence relation on connection sets allows us to partition all connection sets into classes of graphs that are all isomorphic. But are the connection sets of all isomorphic graphs in the same equivalence class?

In 1967, Ádám conjectured that if two circulant graphs are isomorphic, then their connection sets are equivalent. Counterexamples were found shortly afterwards, but it has turned out to be true for some n, in particular for square-free n. We give the proof for prime n below.

We will demonstrate the smallest known undirected counterexample. Let $n = 16$, $C_1 = \{1, 2, 7, 9, 14, 15\}$, and $C_2 = \{2, 3, 5, 11, 13, 14\}$. To prove these connection sets are not equivalent, we must consider the multipliers $3, 5, 7, 9, 11, 13, 15$ coprime to n and show that an element of C_1 maps to an integer not contained in C_2.

r	Invalid mapping	r	Invalid mapping
3	$2 \mapsto 6$	11	$2 \mapsto 6$
5	$2 \mapsto 10$	13	$2 \mapsto 10$
7	$1 \mapsto 7$	15	$1 \mapsto 15$
9	$1 \mapsto 9$		

So the connection sets are not equivalent under any of the multipliers. But consider the mapping $i \mapsto i$ for even i and $i \mapsto i + 4$ for odd i. This mapping takes $1 \mapsto 5$, $2 \mapsto 2$, $7 \mapsto 11$, $9 \mapsto 13$, $14 \mapsto 14$ and $15 \mapsto 3$ which gives us C_2. So the mapping preserves adjacency and non-adjacency and the graphs are isomorphic.

Lemma 4.2. *Suppose $c_{p-1}\omega^{p-1} + c_{p-2}\omega^{p-2} + \ldots + c_0 = 0$ where $c_i \in \mathbb{Z}$, p is prime, and $\omega = \exp(2\pi i/p)$ is a p-th root of unity. Then there exists $q \in \mathbb{Z}$ such that $c_i = q$ for $0 \leq i \leq p - 1$.*

Proof. The given equation can be rewritten as the polynomial

$$P(x) = c_{p-1}x^{p-1} \ldots + c_1 x + c_0$$

that vanishes at $x = \omega$. The cyclotomic polynomial for prime p,

$$Q(x) = x^{p-1} + \ldots + x + 1$$

is the polynomial of lowest degree that vanishes at $x = \omega$. Since $P(x)$ and $Q(x)$ have the same degree and $Q(x)$ divides $P(x)$, $P(x)$ must be an integer multiple of $Q(x)$. Therefore c_i is constant for all $i \in \{0, \ldots, p - 1\}$. □

Theorem 4.3. *If G and G' are isomorphic circulant graphs on a prime number of vertices p, then the corresponding connection sets are equivalent.*

Proof. Suppose G is isomorphic to G'. Let A be a circulant adjacency matrix of G, with the first row $(a_0, a_1, \ldots, a_{p-1})$ and let A' be a circulant adjacency matrix of G', with the first row $(a'_0, a'_1, \ldots, a'_{p-1})$. An eigenvalue of A is

$$\alpha = a_0 + a_1\omega + a_2\omega^2 + \ldots + a_{p-1}\omega^{p-1}$$

where $\omega = \exp(2\pi i/p)$ is the p-th root of unity. In addition, the eigenvalues of A' are

$$\alpha_k = a'_0 + a'_1\omega^k + a'_2\omega^{2k} + \ldots + a'_{p-1}\omega^{k(p-1)}.$$

Since graph isomorphism implies that the eigenvalues of A are the same as A', there exists $k < p$ such that $\alpha = \alpha_k$. Therefore,

$$(a_k - a'_1)\omega^k + (a_{2k} - a'_2)\omega^{2k} + \ldots + (a_{k(p-1)} - a'_{p-1})\omega^{k(p-1)} + (a_0 - a'_0) = 0.$$

By the previous lemma, $a_{jk} - a_k = q$ for some $q \in \mathbb{Z}$. The only possible values for q are 0 or ± 1 since the a_i, a'_i are all zeros or ones. We will show $q = 0$.

Suppose $q = 1$. Then, $a_{jk} = 1$ and $a_k = 0$ for $1 \leq j \leq p-1$, so A is the null matrix. This is clearly impossible. Analogously, if $q = -1$, A' would be the null matrix.

Therefore, $a_{jk} = a'_j$, where the multiplication in the subscript is taken modulo p. This implies that there is a multiplicative correspondence between the connection sets of G and G'. In other words, $kC = C'$ where k is coprime to p because p is prime. □

Acknowledgments. It is a pleasure to thank my mentor, Santiago Chaves, for his invaluable comments and guidance. I would also like to thank Professor Babai, who graciously offered his time to provide suggestions of topics to pursue for this paper. His work in the problems presented here was vital in the eventual resolution of the conjecture. Finally, Professor May's dedication to this program is the only reason I had this wonderful opportunity as part of the REU.

References

[1] B. Elspas and J. Turner, Graphs with Circulant Adjacency Matrices, J. Combinatorial Theory **9** (1970), 297-307.

[2] J. Lazenby, Circulant Graphs and Their Spectra, Reed College Undergraduate Thesis (2008).

[3] M. Muzychuk, Ádám's conjecture is true in the square-free case, J. Combinatorial Theory, Series A, **72**, (1995), 118-134,

[4] J. Turner, Point-Symmetric Graphs with a Prime Number of Points, J. Combinatorial Theory **3** (1967), 136-145.