Properties of Circulants and Related Graphs

Doğukan E. Türköz

Abstract

Numerous books and articles have been dedicated to exploring the properties of circulant graphs and their applications across both pure and applied mathematics. Recognizing circulant graphs as Cayley graphs of cyclic groups, we first introduce some results in more generality. We then discuss the properties of circulant graphs and examine their close relationship with Paley graphs. Additionally, we explore the significance of circulant graphs in relation to Ramsey numbers.

1 Introduction

Circulant graphs bring together several areas of mathematics, mainly algebra, number theory, and graph theory. A comprehensive survey on undirected circulant graphs is [6] by E. A. Monakhova. We first introduce some standard definitions from the theory of groups and graphs.

Let n be a positive integer. The additive cyclic group of order n is defined on the set $\mathbb{Z}_n := \{0, 1, 2, ..., n-1\}$, where the group operation is addition modulo n. Let $\mathbb{Z}_n^*$ to denote the set of units (elements with multiplicative inverses) in $\mathbb{Z}_n$, which form a group under multiplication modulo n.

Group actions allow us to translate many useful results from the theory of permutation groups to graph theory. We say that a group G acts *transitively* on a set Ω if for any two points $x, y \in \Omega$ there is an element $g \in G$ such that $g \cdot x = y$. We will only consider group actions on finite simple graphs.

For a graph X, $V(X)$ denotes the vertex set of X and $E(X)$ denotes the edge set of X. If there is an edge between the vertices v_1 and v_2 we write $\{v_1, v_2\} \in E(X)$. C_n denotes the cycle graph on n vertices and K_n denotes the complete graph on n vertices. The *complement* of a graph X is a graph $\overline{X}$ on the same vertices such that two distinct vertices of $\overline{X}$ are adjacent if and only if they are not adjacent in X.

Two (simple) graphs $X = (V, E)$ and $X' = (V', E')$ are said to be *isomorphic* if there exists a bijection $\phi : V \to V'$ such that $\{v_1, v_2\} \in E$ if and only if $\{\phi(v_1), \phi(v_2)\} \in E'$. In this case, we say that ϕ is an *isomorphism* from X to X'. An *automorphism* of a graph X is an isomorphism from X to itself. The set of all automorphisms of a graph X forms a group under composition, which we denote by $\mathrm{Aut}(X)$.

A graph X is called *vertex-transitive* if $\mathrm{Aut}(X)$ acts transitively on $V(X)$ and *edge-transitive* if $\mathrm{Aut}(X)$ acts transitively on $E(X)$. Note that a graph X is vertex-transitive if and only if $\overline{X}$ is vertex-transitive. We will use this fact in the next example.

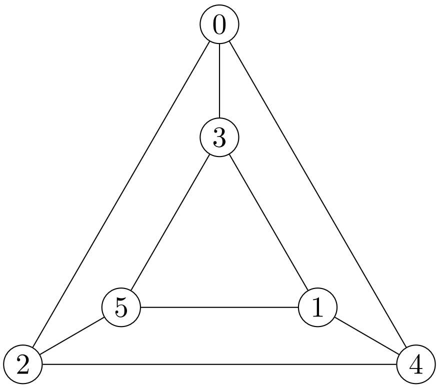

Figure 1: The triangular prism graph

Example 1.1. The graph $\overline{C_6}$ (also known as the triangular prism graph) is vertex-transitive but not edge-transitive.

Proof. Since C_6 is vertex-transitive, it follows that $\overline{C_6}$ is also vertex-transitive. The action of $\mathrm{Aut}(\overline{C_6})$ on $E(\overline{C_6})$ has two orbits, and these orbits are $\mathcal{O}_1 := \{\{0,3\},\{2,5\},\{1,4\}\}$ and $\mathcal{O}_2 := \{\{0,2\},\{2,4\},\{4,0\},\{1,3\},\{3,5\},\{5,1\}\}$. One way to distinguish between $\mathcal{O}_1$ and $\mathcal{O}_2$ is to note that the edges in $\mathcal{O}_1$ are not contained in a 3-cycle. Therefore, $\overline{C_6}$ is not edge-transitive. □

2 Cayley Graphs

In this section, we will use the additive notation for groups.

Definition 2.1. Let S be a subset of a group G such that $0 \notin S$ and $S = -S$, i.e., if $s \in S$ then $-s \in S$. The Cayley graph $C(G, S)$ is defined as the graph with vertices corresponding to the elements of G and two vertices $g, h \in G$ are joined by an edge if and only if $g - h \in S$.

Remark. The term Cayley (di)graph is also often used to denote an edge-colored directed graph variant of the definition above. We will only consider simple graphs, which is the reason for the conditions on set S.

Example 2.2. The Cayley graph $C(\mathbb{Z}_2^3, \{(1,0,0),(0,1,0),(0,0,1)\})$ is the well-known cube graph given in Figure 2.

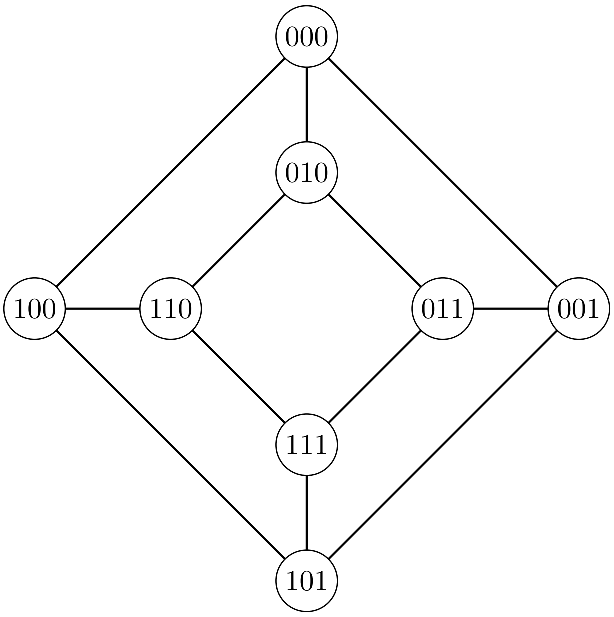

Figure 2: The cube graph

Let G be a group, and let A be a non-empty subset of G. We write $\langle A \rangle$ to denote the subgroup of G generated by A.

Theorem 2.3. *The Cayley graph $C(G, S)$ is connected if and only if G is generated by S.*

Proof. Suppose $C(G,S)$ is connected. Let $g \in G$. Then, there exists a path from 0 to g, say through the vertices $g_1, \ldots, g_k$ in the given order. Hence, $g_1, g_2 - g_1, \ldots, g_{k-1} - g_k \in S$ and $g_1 + (g_2 - g_1) + \ldots + (g_{k-1} - g_k) = g \in \langle S \rangle$. For the converse, suppose $\langle S \rangle = G$ and let $g, h \in G$ be two vertices of $C(G,S)$. Since $\langle S \rangle = G$ and $h - g \in G$ there exists $s_i \in S$ for $1 \leq i \leq k$ such that $h - g = s_1 + \ldots + s_k$. Then, $(g, g + s_1, g + s_1 + s_2, \ldots, g + \sum_{i=1}^{k-1} s_i, h)$ is a path from g to h. □

Theorem 2.4. *Cayley graphs are vertex-transitive.*

Proof. Let $X := C(G,S)$ be a Cayley graph. For all $g \in G$, consider the (bijective) map $f_g : v \mapsto v + g$. We first show that f_g is an automorphism for all $g \in G$. Suppose $\{v_1, v_2\} \in E(X)$, i.e., $(v_1 - v_2) \in S$. Then, $(v_1 + g - g - v_2) \in S$ and $(v_1 + g) - (v_2 + g) \in S$, so $f_g(v_1) - f_g(v_2) \in S$. Thus, $\{v_1, v_2\} \in E(X)$ if and only if $\{f_g(v_1), f_g(v_2)\} \in E(X)$. The set $\{f_g : g \in G\}$ is a subgroup of $\mathrm{Aut}(X)$, and this subgroup acts transitively on $V(X)$ since given any $v_1, v_2 \in V(X)$ we can take v_1 to v_2 via the map $f_{v_2 - v_1}$. □

Remark. There are vertex-transitive graphs which are not Cayley graphs, with the classic example being the Petersen graph.

A natural question to ask is: When are two Cayley graphs of the same group isomorphic? Although this question is not the main focus of this essay, we will briefly discuss related results. We first give a partial answer to this question by providing a sufficient condition using group automorphisms.

An automorphism of a group G is a bijection $\theta : G \to G$ which satisfies $\theta(a + b) = \theta(a) + \theta(b)$ for all $a, b \in G$. The set of all automorphisms of a group G forms a group under composition, which we denote by $\mathrm{Aut}(G)$.

Theorem 2.5. *Let $\theta \in \mathrm{Aut}(G)$. Then, $C(G, \theta(S)) \cong C(G,S)$, where $\theta(S) = \{\theta(s) \mid s \in S\}$.*

Proof. Let $X_1 := C(G,S)$ and $X_2 := C(G, \theta(S))$. Suppose $\{v_1, v_2\} \in E(X_1)$, i.e., $(v_1 - v_2) \in S$. Then, by definition, $\theta(v_1 - v_2) \in \theta(S)$ and $\theta(v_1) - \theta(v_2) \in \theta(S)$ since θ is an isomorphism. Thus, $\{v_1, v_2\} \in E(X_1)$ if and only if $\{\theta(v_1), \theta(v_2)\} \in E(X_2)$, as desired. □

Definition 2.6. The graph $C(G,S)$ is called a *CI-graph* (CI stands for Cayley isomorphism) of G if, whenever $C(G,S) \cong C(G,T)$, there is an element $\theta \in \operatorname{Aut}(G)$ such that $\theta(S) = T$. A finite group G is called a *CI-group* if all Cayley graphs of G are CI-graphs.

In general, it is very difficult to determine whether a group is a CI-group. In the end of next section, we will discuss this problem briefly for $G = \mathbb{Z}_n$.

3 Circulant Graphs

Definition 3.1. A Cayley graph $C(G,S)$ where G is a cyclic group is called a *circulant* graph (circulant for short).

Remark. The term *cyclic* graph is also used for circulant graphs. Unfortunately, this term has many other meanings in graph theory and is ambiguous.

Example 3.2. The graph C_6 is a circulant as $C(\mathbb{Z}_6, \{1,5\}) \cong C_6$. Since $\{1,2,3,4,5\} \setminus \{1,5\} = \{2,3,4\}$, it follows that $C(\mathbb{Z}_6, \{2,3,4\}) \cong \overline{C_6}$. So, the triangular prism graph $\overline{C_6}$ (Figure 1) is also a circulant. This reasoning can be extended to any graph X: If X is a circulant, then so is $\overline{X}$.

Remark. Recall that $\overline{C_6}$ is not edge-transitive (Example 1.1), so circulant graphs need not be edge-transitive.

Example 3.3. The Cayley graph $C(\mathbb{Z}_4, \{2\})$ is a disconnected circulant.

We will now obtain a condition for a circulant graph to be connected, but we first need a basic result from number theory, namely a generalisation of Bézout's Lemma (see the appendix of [5] for a proof).

Fact 3.4 (Generalised Bézout's Lemma)**.** *Let $a_1, a_2, \ldots, a_n$ be integers with $\gcd(a_1, a_2, \ldots, a_n) = d$. Then, there exist integers $\gamma_1, \gamma_2, \ldots, \gamma_n$ such that $d = \gamma_1 a_1 + \gamma_2 a_2 + \cdots + \gamma_n a_n$.*

Theorem 3.5. *The circulant $C(\mathbb{Z}_n, S)$, where $S = \{a_1, \ldots, a_k\}$ is a nonempty set, is connected if and only if $\gcd(a_1, a_2, \ldots, a_k, n) = 1$.*

Proof. By Theorem 2.3, it suffices to show that S generates $\mathbb{Z}_n$ if and only if $\gcd(a_1, a_2, \ldots, a_k, n) = 1$. Suppose $\langle S \rangle = \mathbb{Z}_n$. Then, there exists integers β_i with $1 \le \beta_i \le k$ such that $\sum_{i=1}^{k} \beta_i a_i \equiv 1 \pmod{n}$, as $1 \in \mathbb{Z}_n$. Hence, $\sum_{i=1}^{k} \beta_i a_i + mn = 1$ for some integer m, and so, $\gcd(a_1, a_2, \ldots, a_k, n) = 1$.

For the converse, suppose $\gcd(a_1, a_2, \ldots, a_k, n) = 1$. Then, by Fact 3.4, there exist integers γ_i with $1 \leq \gamma_i \leq k+1$ such that $\sum_{i=1}^{k} \gamma_i a_i + \gamma_{k+1} n = 1$. Hence, $\sum_{i=1}^{k} \gamma_i a_i \equiv 1 \pmod{n}$, and by scaling γ_i any element of $\mathbb{Z}_n$ can be written as a linear combination of $\{a_1, \ldots, a_k\}$, so $\langle S \rangle = \mathbb{Z}_n$. □

A subgroup $H \leq \mathrm{Aut}(X)$ is said to be *transitive* H acts transitively on $V(X)$. A transitive subgroup $H \leq \mathrm{Aut}(X)$ such that $|H| = |V(X)|$ is called *regular* subgroup of $\mathrm{Aut}(X)$.

Theorem 3.6. *A graph X is a circulant if and only if* $\mathrm{Aut}(X)$ *has a regular cyclic subgroup.*

Proof. Let X be a circulant. Consider the map $\theta : v \mapsto v + 1$, which is an automorphism of X. Then, $\langle \theta \rangle$ is a regular cyclic subgroup of $\mathrm{Aut}(X)$. The converse requires more work to prove, but a proof can be found in [4]. □

Example 3.7. The cube graph Q_3 defined in Example 2.2 does not have an automorphism of order 8, so $\mathrm{Aut}(Q_3)$ does not contain a regular cyclic subgroup of order 8. Hence, Q_3 is not a circulant.

We will now discuss the Cayley isomorphism problem for circulant graphs. In 1967, Ádám conjectured that $\mathbb{Z}_n$ is a CI-group for all n [13]. In 1970, Elspas and Turner [2] gave a counterexample to Ádám's conjecture, which is the content of Theorem 3.9. For the counterexample, we need a well-known result from group theory.

Fact 3.8. $\mathrm{Aut}(\mathbb{Z}_n) = \{f_a \mid a \in \mathbb{Z}_n^*\}$*, where the function* $f_a : \mathbb{Z}_n \longrightarrow \mathbb{Z}_n$ *is given by* $f_a(x) = ax$.

Theorem 3.9. $\mathbb{Z}_{16}$ *is not a CI-group.*

Proof. Let $S_1 = \{1, 2, 7, 9, 14, 15\}$ and $S_2 = \{2, 3, 5, 11, 13, 14\}$. Consider the Cayley graphs $X_1 = C(\mathbb{Z}_{16}, S_1)$ and $X_2 = C(\mathbb{Z}_{16}, S_2)$. We first claim that there does not exist an automorphism $\phi \in \mathrm{Aut}(X_1)$ that maps S_1 to S_2. This result follows by noting that $aS_1 \neq S_2$ for all $a \in \mathbb{Z}_{16}^* = \{1, 3, 5, 7, 9, 11, 13, 15\}$ and by Fact 3.8. To complete the proof, all that remains is to show that the graphs X_1 and X_2 are isomorphic. Although it is not too difficult to show this isomorphism by hand, we verify it using SageMath in the Appendix. □

The next theorem, which is attributed to Muzychuk, gives a complete description of when $\mathbb{Z}_n$ is a CI-group.

Theorem 3.10 (Muzychuk [7])**.** *$\mathbb{Z}_n$ is a CI-group if and only if either $n = 8, 9, 18$, or $n = mk$ where $m = 1, 2, 4$ and k is odd and square-free.*

4 Paley Graphs

Paley graphs were named after Raymond E.A.C. Paley (1907 − 1933), an English mathematician who died young in a skiing accident. Although Paley's original paper [8] does not include any graph theory, Paley's construction of Hadamard matrices using finite fields inspired the Paley graph construction [3]. We first recall some results from number theory.

Definition 4.1. Let p be an odd prime and m an integer not divisible by p. Then, m is a *quadratic residue (residue for short)* of p if there exists an integer x such that $x^2 \equiv m \pmod p$. Otherwise, it is a *non-residue.*

Fact 4.2 (Wilson's Theorem)**.** *If p is prime then $(p-1)! \equiv -1 \pmod p$.*

Theorem 4.3. *If p is a prime such that $p \equiv 1 \pmod 4$, then -1 is a residue modulo p.*

Proof. We observe that

$$\begin{aligned}\left(\frac{p-1}{2}\right)! &\equiv \left(1 \cdot \ldots \cdot \frac{p-1}{2}\right) \pmod p\\ &\equiv \left((1-p) \cdot \ldots \cdot \frac{-p-1}{2}\right) \pmod p\\ &\equiv \left((p-1) \cdot \ldots \cdot \frac{p+1}{2}\right) \cdot (-1)^{\frac{p-1}{2}} \pmod p.\end{aligned}$$

Hence,

$$\begin{aligned}\left(\left(\frac{p-1}{2}\right)!\right)^2 &\equiv \left(1 \cdot \ldots \cdot \frac{p-1}{2}\right)\left((p-1) \cdot \ldots \cdot \frac{p+1}{2}\right) \cdot (-1)^{\frac{p-1}{2}} \pmod p\\ &\equiv (p-1)! \cdot (-1)^{\frac{p-1}{2}} \pmod p\\ &\equiv -1 \pmod p\end{aligned}$$

where the last line follows from Wilson's Theorem and the fact that $(-1)^{\frac{p-1}{2}} \equiv 1 \pmod p$ as $p \equiv 1 \pmod 4$. □

Let $(\mathbb{Z}_p^*)^2 = \{x^2 : x \in \mathbb{Z}_p^*\}$, which corresponds to the quadratic residues in $\mathbb{Z}_p^*$ for an odd prime p.

Lemma 4.4. *Let p be a prime. Then, $(\mathbb{Z}_p^*)^2$ is a subgroup of $\mathbb{Z}_p^*$.*

Proof. Since $\mathbb{Z}_p^*$ is closed under multiplication, it follows that $(\mathbb{Z}_p^*)^2 \subseteq \mathbb{Z}_p^*$. Clearly, $1 \in (\mathbb{Z}_p^*)^2$. Suppose $a \in (\mathbb{Z}_p^*)^2$ and $b \in (\mathbb{Z}_p^*)^2$. These imply $a \equiv k^2 \pmod{p}$ for some $k \in \mathbb{Z}_p^*$ and $b \equiv l^2 \pmod{p}$ for some $l \in \mathbb{Z}_p^*$. Since $\mathbb{Z}_p^*$ is a group $kl \in \mathbb{Z}_p^*$. Then, $(kl)^2 \equiv k^2 l^2 \equiv ab \pmod{p}$, so $ab \in (\mathbb{Z}_p^*)^2$. Now, suppose $c \in (\mathbb{Z}_p^*)^2$. Then, $c \equiv m^2 \pmod{p}$ for some $m \in \mathbb{Z}_p^*$. Since $\mathbb{Z}_p^*$ is a group, $m^{-1} \in \mathbb{Z}_p^*$. Note that $(m^{-1})^2 \equiv (m^2)^{-1} \equiv c^{-1} \pmod{p}$, so $c^{-1} \in (\mathbb{Z}_p^*)^2$, as desired. □

Definition 4.5. Let p be a prime such that $p \equiv 1 \pmod{4}$. The Paley graph of order p, denoted $\mathrm{QR}(p)$, is the Cayley graph $C(\mathbb{Z}_p, (\mathbb{Z}_p^*)^2)$.

Remark. Paley graphs can be defined more generally for all prime power orders using the existence of finite fields of all prime powers. However, we will follow Definition 4.5, in which case, Paley graphs are circulants.

We have to show that Paley graphs satisfy the definition of a Cayley graph (recall Definition 2.1).

Theorem 4.6. *Paley graphs are well-defined Cayley graphs.*

Proof. For an integer a and a prime p, since $p \mid a^2$ implies $p \mid a$, it follows that $0 \notin (\mathbb{Z}_p^*)^2$. We next need to show that $s \in (\mathbb{Z}_p^*)^2$ implies $-s \in (\mathbb{Z}_p^*)^2$. This result follows since we already know that $-1 \in (\mathbb{Z}_p^*)^2$ by Theorem 4.3 and that $(\mathbb{Z}_p^*)^2$ is closed under multiplication. □

Example 4.7. Consider $\mathrm{QR}(5)$ and $\mathrm{QR}(13)$. Note that $(\mathbb{Z}_5^*)^2 = \{1, 4\}$, so $\mathrm{QR}(5) \cong C_5$. For $\mathrm{QR}(13)$, we note that $(\mathbb{Z}_{13}^*)^2 = \{1, 3, 4, 9, 10, 12\}$. Figure 3 is a plot of $\mathrm{QR}(13)$.

We will now discuss some general properties of Paley graphs.

Theorem 4.8. *Paley graphs are connected.*

Proof. Since 1 is always a residue, the result follows from Theorem 3.5. □

Definition 4.9. A *symmetric graph* is a graph that is both vertex-transitive and edge-transitive.

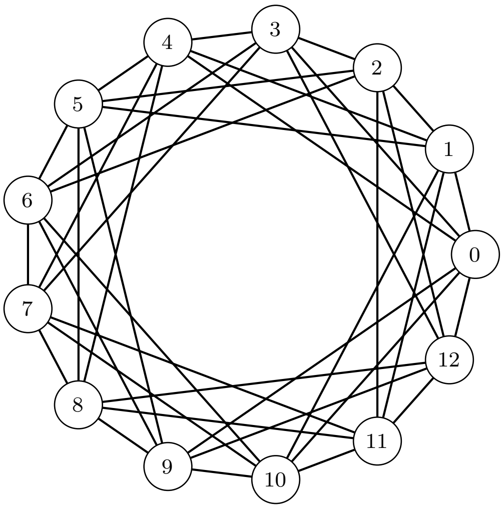

Figure 3: Paley Graph QR(13)

Theorem 4.10. *Paley graphs are symmetric.*

Proof. Since Paley graphs are Cayley graphs, they are vertex-transitive. We will now show that Paley graphs are edge-transitive. Let $X := \mathrm{QR}(p)$ be a Paley graph for a prime p. Let $a, b \in V(X)$ with $a \in (\mathbb{Z}_p^*)^2$ and consider the map $\phi : V(X) \to V(X)$ given by $\phi(x) = ax + b$. We claim that $\phi \in \mathrm{Aut}(X)$.

We first show that ϕ is a bijection. For $x, y \in V(X)$ suppose $\phi(x) = \phi(y)$. Then, $ax + b = ay + b$, and $ax = ay$. Since $a \in (\mathbb{Z}_p^*)^2$, it follows that $x = y$ and so, ϕ is injective. Let $v \in V(X)$ and note that $\phi(a^{-1}(v - b)) = v$, so ϕ is also surjective. Thus, ϕ is a bijection.

We also need to show that $\{v_1, v_2\} \in E(X)$ if and only if $\{\phi(v_1), \phi(v_2)\} \in E(X)$. This follows by noting that $\phi(v_1) - \phi(v_2) = (av_1 + b) - (av_2 + b) = a(v_1 - v_2)$ and the fact that $(\mathbb{Z}_p^*)^2$ is closed under multiplication. Thus, ϕ is an automorphism.

Let $\{u_1, v_1\}, \{u_2, v_2\} \in E(X)$. To show that X is edge-transitive, we can use the family of automorphisms ϕ defined above if we can find a and b such that $\phi(u_1) = u_2$ and $\phi(v_1) = v_2$. Solving the equations $au_1 + b = u_2$ and $av_1 + b = v_2$, we obtain $a = (u_2 - v_2)\,(u_1 - v_1)^{-1} \in (\mathbb{Z}_p^*)^2$ and $b = u_2 - au_1 \in V(X)$. The map ϕ with a and b taken as above maps $\{u_1, v_1\}$ to $\{u_2, v_2\}$. Therefore, X is edge-transitive. □

Definition 4.11. A *self-complementary* graph is a graph that is isomorphic to its complement.

The classic example of a self-complementary graph is C_5. We will next prove that all Paley graphs are self-complementary. For the proof, we will need some facts from number theory. We already know that the product of two residues is a residue by Theorem 4.4. We now state further well-known facts (see [12, p. 10]) about products of residues and non-residues.

Fact 4.12. *The following are true:*

(i) If neither of a, b are residues, then ab is a residue.

(ii) If a or b is a residue and the other is a non-residue, ab is a non-residue.

Theorem 4.13. *Paley graphs are self-complementary.*

Proof. Let $X := \mathrm{QR}(p)$ be a Paley graph and q be a quadratic non-residue modulo p. We claim $\phi : V(X) \longrightarrow V(\overline{X})$ given by $\phi(x) = qx$ is an isomorphism. Since $\gcd(p, q) = 1$, the map ϕ is injective. For the surjectivity of ϕ, note that by Bézout's Lemma there exists integers a, b such that $ap+bq = 1$, so $bq \equiv 1 \pmod{p}$. Now, $\phi(bx) = qbx \equiv x \pmod{p}$, so ϕ is surjective. Thus, ϕ is a bijection.

We next need to show that $\{x, y\} \in E(X)$ if and only if $\{\phi(x), \phi(y)\} \notin E(X)$. To prove this equivalence, it suffices to prove that $(x - y) \in (\mathbb{Z}_p^*)^2$ if and only if $q(x-y) \notin (\mathbb{Z}_p^*)^2$ since $\phi(x)-\phi(y) = qx-qy = q(x-y)$. Now, the forward implication follows from Fact 4.12 (*ii*), and the other implication follows from Fact 4.12 (*i*). □

Remark. See [9] for a complete description of self-complementary symmetric graphs (note that the more general definition of a Payley graph is used in [9]). A complete characterization of self-complementary graphs is unknown.

5 An Application to Ramsey Numbers

Ramsey numbers are an active research area in combinatorics and graph theory, named after the British mathematician Frank Ramsey. Ramsey's work marked the beginning of Ramsey theory, which is a field of mathematics generally focusing on questions of the type: How large a structure should be to ensure that there must exist a substructure with a given property?

An *independent (vertex) set* of a graph X is a subset of the vertices such that no two vertices in the subset are adjacent. A *clique* of a graph X is a complete subgraph of X.

Definition 5.1. The Ramsey number $R(s, t)$ is the minimum number n such that any graph on n vertices contains either a clique of size s or an independent set of size t.

The existence of Ramsey numbers for all s and t is justified by the well-known Ramsey's Theorem. We will mainly be interested in obtaining lower bounds for Ramsey numbers. If there exists a graph with k vertices that contains neither a clique of size s nor an independent set of size t, then we can conclude that the Ramsey number $R(s, t)$ is greater than k.

The following lemma will simplify the proofs of Theorems 5.3 and 5.4.

Lemma 5.2. *Let $X := C(\mathbb{Z}_n, S)$ be a circulant. The following are true:*

(i) Consider a vertex $a \in \mathbb{Z}_n$ of X. Let the vertices adjacent to both 0 and a be $B := \{b_1, \dots, b_k\} \subseteq \mathbb{Z}_n$ for some integer k. Then, the vertices adjacent to both 0 and $-a$ are precisely $-B = \{-b_1, \dots, -b_k\}$.

(ii) Let $C := \{c_1, \dots, c_k\} \subseteq \mathbb{Z}_n$ be a set of vertices of X such that none of the vertices in C is adjacent to another. Then, it is also true that none of the vertices in $-C = \{-c_1, \dots, -c_k\}$ is adjacent to another.

Proof. Both of these parts follow from the fact that if two vertices x and y of X are adjacent, then $x-y \in S$ and $y-x \in S$ since $S = -S$ by definition. □

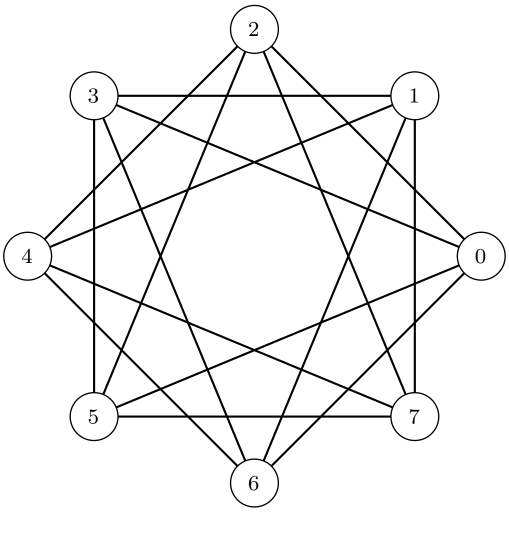

Figure 4: $C(\mathbb{Z}_8, \{2, 3, 5, 6\})$

It is known that $R(4, 3) = 9$ and $R(4, 4) = 18$. As examples, we will establish sharp lower bounds on $R(4, 3)$ and $R(4, 4)$ using circulant graphs.

Theorem 5.3. *$R(4,3) > 8$.*

Proof. Consider the circulant $X := C(\mathbb{Z}_8, \{2,3,5,6\})$ given in Figure 4. We need to show that this graph does not contain a K_4 and its complement does not contain a K_3. Suppose X contains a K_4. Note that by the vertex-transitivity of circulants we can assume 0 is one of the vertices of this K_4. The vertex 0 is adjacent to the vertices $\{2,3,5,6\}$. If 2 is contained in the K_4, then the only vertex adjacent to both 0 and 2 is 5, so 2 cannot be in the K_4. If instead 3 is contained in the K_4, then the only vertices adjacent to both 0 and 3 are $\{5,6\}$, but these are not adjacent to each other. By symmetry (see Lemma 5.2), the two remaining cases follow from the previous two cases. Hence, X does not contain a K_4. The fact that $\overline{X} = C(\mathbb{Z}_8, \{1,4,7\})$ does not contain a K_3 follows similarly. □

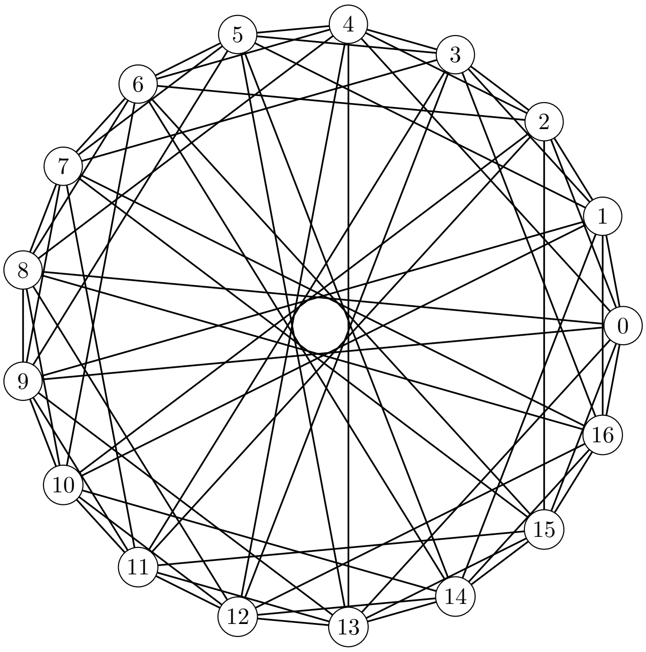

Figure 5: Paley Graph QR(17)

Theorem 5.4. *$R(4,4) > 17$.*

Proof. Consider the Paley graph QR(17), or equivalently, the circulant graph $C(\mathbb{Z}_{17}, \{1,2,4,8,9,13,15,16\})$ given in Figure 5. This is a self-complementary graph by Theorem 4.13; hence, it suffices to show that QR(17) does not contain a K_4 to conclude $R(4,4) > 17$.

Suppose QR(17) contains a K_4, and assume 0 is one of the vertices of this K_4. The vertex 0 is adjacent to the vertices $\{1, 2, 4, 8, 9, 13, 15, 16\}$. If 1 is contained in the K_4, then the only vertices adjacent to both 0 and 1 are {2, 9, 16}, but none of these vertices are adjacent to each other. If 2 is contained in the K_4, the vertices to check are {1, 4, 15}; if 4 is contained in the K_4, the vertices to check are {2, 8, 13}; if 8 is contained in the K_4, the vertices to check are {4, 9, 16}, but none of the vertices in these sets are adjacent to each other. By symmetry (see Lemma 5.2), the remaining cases follow from the previous cases. Thus, QR(17) does not contain a K_4. □

Remark. It is known that QR(17) is the unique graph which establishes the lower bound for $R(4, 4)$ [1].

Table 1: Circulants That Give Sharp Lower Bounds for Ramsey Numbers

k	l	$R(k,l)$	Circulant
3	3	6	$C(\mathbb{Z}_5, \{1, 4\})$
3	4	9	$C(\mathbb{Z}_8, \{1, 4, 7\})$
3	5	14	$C(\mathbb{Z}_{13}, \{1, 5, 8, 12\})$
3	9	36	$C(\mathbb{Z}_{35}, \{1, 7, 11, 16, 19, 24, 28, 34\})$
4	4	18	$C(\mathbb{Z}_{17}, \{1, 2, 4, 8, 9, 13, 15, 16\})$
4	5	25	$C(\mathbb{Z}_{24}, \{1, 2, 4, 8, 9, 15, 16, 20, 22, 23\})$

Tables 1 and 2 show updated and slightly modified versions of Tables II and III from [1]. Table 1 lists the values of k, l for which circulant graphs can be used to establish sharp lower bounds for known values of $R(k, l)$, and the Appendix provides an example demonstrating the use of SageMath to verify that the specified circulants establish these bounds.

Table 2: $C(k, l)$ and Best Known Bounds for Ramsey Numbers [10]

k	l	$C(k,l)$	Lower Bound for $R(k,l)$	Upper Bound for $R(k,l)$
3	6	16	18	18
3	7	21	23	23
3	8	26	28	28
3	10	38	40	42
4	6	33	36	41
5	5	41	43	48
5	6	56	58	87
6	6	101	102	165

In Table 2, $C(k, l)$ denotes the number of vertices of the largest (not necessarily unique) circulant which does not contain a clique of size k or an independent set of size l. Table 2 compares $C(k, l)$ with some of the best known upper and lower bounds on $R(k, l)$ for larger values of k, l. These bounds are from [10], by Stanisław Radziszowski, which is the main reference for values and bounds for Ramsey numbers and is periodically updated (with the last update being in 2021).

Tables 1 and 2 illustrate that circulant graphs are good candidates for establishing lower bounds on Ramsey numbers for small parameters. We note that the brief discussion of the Cayley isomorphism problem for $\mathbb{Z}_n$ in sections 2 and 3 is particularly useful in reducing the search space of circulant graphs when trying to obtain lower bounds on Ramsey numbers. For an algorithmic perspective on Ramsey numbers, see [11].

References

[1] F. R. K. Chung and C. M. Grinstead. A survey of bounds for classical ramsey numbers. *Journal of Graph Theory*, 7(1):25–37, 1983. URL `https://doi.org/10.1002/jgt.3190070105`.

[2] Bernard Elspas and James Turner. Graphs with circulant adjacency matrices. *Journal of Combinatorial Theory*, 9(3):297–307, 1970. ISSN 0021-9800. URL `https://doi.org/10.1016/S0021-9800(70)80068-0`.

[3] Gareth A. Jones. Paley and the Paley graphs. In Gareth A. Jones, Ilia Ponomarenko, and Jozef Širáň, editors, *Isomorphisms, Symmetry and Computations in Algebraic Graph Theory*, pages 155–183. Springer International Publishing, 2020. ISBN 978-3-030-32808-5.

[4] F T Leighton. Circulants and the characterization of vertex-transitive graphs. *Journal of Research of the National Institute of Standards and Technology*, 88(6):395–402, Nov-Dec 1983. ISSN 0160-1741. URL `https://doi.org/10.6028/jres.088.020`.

[5] Ian D. Macdonald. *The Theory of Groups.* Oxford University Press, 1970.

[6] E. A. Monakhova. A survey on undirected circulant graphs. *Discrete Mathematics, Algorithms and Applications*, 04(01):1250002, 2012. URL `https://doi.org/10.1142/S1793830912500024`.

[7] Mikhail Muzychuk. On Ádám's conjecture for circulant graphs. *Discrete Mathematics*, 167-168:497–510, 1997. ISSN 0012-365X. URL https://doi.org/10.1016/S0012-365X(96)00251-8.

[8] R. E. Paley. On orthogonal matrices. *Journal of Mathematics and Physics*, 12 (1-4):311–320, 1933. URL https://doi.org/10.1002/sapm1933121311.

[9] Wojciech Peisert. All self-complementary symmetric graphs. *Journal of Algebra*, 240(1):209–229, 2001. ISSN 0021-8693. URL https://doi.org/10.1006/jabr.2000.8714.

[10] Stanisław P. Radziszowski. Small Ramsey numbers. *Electronic Journal of Combinatorics*, 2021.

[11] Steven Van Overberghe. *Algorithms for computing Ramsey numbers.* PhD thesis, Ghent University, 2020.

[12] Steve Wright. *Quadratic Residues and Non-Residues: Selected Topics.* Springer International Publishing, Cham, 2016. ISBN 978-3-319-45955-4. URL https://doi.org/10.1007/978-3-319-45955-4_2.

[13] A. Ádám. Research problem 2-10. *Journal of Combinatorial Theory*, 2:393, 1967.

A SageMath Computations

In Theorem 3.9, the isomorphism between C_1 and C_2 can be verified as follows in SageMath.

```
C1 = graphs.CirculantGraph(16, [1, 2, 7, 9, 14, 15])
C2 = graphs.CirculantGraph(16, [2, 3, 5, 11, 13, 14])
C1.is_isomorphic(C2)
Output: True
```

Using Table 1, the fact $R(4,5) > 24$ can be verified in Sage as follows.

```
circ = graphs.CirculantGraph(24, [1,2,4,8,9,15,16,20,22,23])
circ_complement = circ.complement()

K_4 = graphs.CompleteGraph(4)
K_5 = graphs.CompleteGraph(5)
```

```
subgraph_K_4 = circ.subgraph_search(K_4)
subgraph_K_5 = circ_complement.subgraph_search(K_5)

if subgraph_K_4:
    print("K_4 is a subgraph of circ.")
else:
    print("K_4 is not a subgraph of circ.")

if subgraph_K_5:
    print("K_5 is a subgraph of the complement of circ.")
else:
    print("K_5 is not a subgraph of the complement of circ.")
Output:
K_4 is not a subgraph of circ.
K_5 is not a subgraph of the complement of circ.
```