ON THE COMBINATORIAL PARAMETERS OF HIGHLY SYMMETRIC GRAPHS

ANUSHKA MURTHY

Abstract. In this paper, we study the automorphism groups of highly symmetric graphs, and relate the algebraic structure of their automorphism groups to their combinatorial parameters. We exhibit infinite families of vertex-primitive, arc-transitive (VPAT) graphs with $\Omega(n)$ degree and $\Omega(\sqrt{n})$ independence number. We also exhibit an infinite family of VPAT graphs with degree increasing to infinity and bounded chromatic number. Along the way to proving these results, we study combinatorial properties of Paley Graphs, Kneser Graphs, Johnson Graphs, Hamming Graphs, and Cayley Graphs. In addition to results related to the independence number, degree, and chromatic number of these graphs, we also study their universality, girth, and clique number.

Contents

Date: August 2021.

1. Introduction

The overarching theme of this paper is the interplay between Group and Graph Theory. Viewing graphs as geometric objects immediately leads to the study of their symmetries, which opens up a natural avenue for the use of group-theoretic methods to study the graph's automorphism group. In this manner, we can classify graphs into families via the amount of symmetry their automorphism group holds. Furthermore, we can investigate the combinatorial properties that highly symmetric graphs have.

In this paper, the measures of symmetry we are interested in are vertex-transitivity, vertex-primitivity, arc-transitivity, and distance-transitivity; we investigate how a graph's combinatorial parameters are affected when we impose these various symmetry conditions. We give special attention to vertex-primitive, arc-transitive (denoted VPAT) graphs, with the goal of proving the following two results:

Theorem 1.1. *There exists an infinite family of VPAT graphs with degree d and independence number α such that $d > \frac{n-1}{2}$ and $\alpha > \sqrt{n}$, where n denotes the number of vertices.*

Theorem 1.2. *There exists an infinite family of VPAT graphs such that $d \to \infty$ yet the chromatic number χ stays bounded.*

1.1. Outline of Paper.

We begin with an overview of the prerequisite concepts from Group Theory that are needed in our study. Drawing from general Group Theory, we focus on elementary Abelian, solvable, and characteristic groups, ultimately proving a classification criterion for characteristically simple groups. From here, we discuss the theory of Permutation Groups, which are central to our study as we are viewing graphs as the domain for the group action of their automorphism group. We start by introducing the concepts of transitivity and primitivity, giving a sufficient and necessary condition that relates a primtive permutation group to the stabilizer of its action, and investigating the subgroups of primitive permutation groups. We then introduce the concepts of regular group actions and regular representations of a group, and give a necessary and sufficient condition for certain regular representations to be primitive.

After we have given the necessary results from Group Theory, we put these results in the context of highly symmetric graphs. We start the third section by introducing key graph-theoretic concepts, and we include an interesting result relating some of these concepts to the Feit-Thompson Theorem, a key result from group theorem. Then, we describe the measures of symmetry that we are interested in, and discuss the various inclusions that they hold in relation to each other. We end the third section with a brief study of Platonic solids, illustrating how we can view graphs in a geometric context.

In the fourth section, we introduce the Paley Graph, Kneser Graph, Johnson Graph, and Hamming Graph, which are four families of highly symmetric graphs that are important to our study. The Paley and Kneser Graphs are particularly important because they are both VPAT. The fifth section is devoted to the study of Cayley digraphs, where we give a characterization of arc-transitive Cayley graphs of prime order, and we also include the classic result of Elspas and Turner that gives a sufficient condition for two Cayley Graphs of prime order to be isomorphic.

The sixth, seventh, and eighth sections are dedicated to proving combinatorial properties of our highly symmetric graphs that follow from their symmetry properties. We then end the paper by proving Theorems 1.1 and 1.2, which appear as Theorems 10.1 and 10.2. Along the way to proving our main results, we study vertex-transitivity, arc-transitivity, vertex-primitivity, and prove many other results relating these concepts to our highly symmetric graphs and their combinatorial parameters.

2. Group Theory Preliminaries

The purpose of this section is to detail the relevant group-theoretic results that are needed to make the results of our paper understandable to readers with a basic background in group theory. In the first subsection, we collect some results from general group theory, with the main result of the subsection being the characterization of characteristically simple groups. We then move to the Theory of Permutation Groups, focusing on primitivity in particular. For basic background in group theory, we refer the reader to [16] and [26]. A more extensive treatment of Permutation Groups can be found in [15].

2.1. General Group Theory.

Remark 2.1. All of the groups in this paper are finite.

Definition 2.2. The symmetric group acting on Ω is denoted by $Sym(\Omega)$ and the symmetric group acting on $[n]$ is denoted by S_n.

Definition 2.3. A *p-group* is a group where the order of all non-trivial elements is a power of p.

Proposition 2.4. *G is a p-group if and only if $|G| = p^k$ for some k.*

Proof. The reverse direction follows from Lagrange's Theorem. For the forward direction, suppose $|G| = p^k m$ for $m > 1$ relatively prime to p. Then there exists a prime divisor q of m that is also relatively prime to p. By Cauchy's Theorem, G has an element of order q, so the group H generated by this element has order q. Since G is a p-group, the order of any non-trivial element in H must be divisible by p. However, this is impossible since p and q are relatively prime. □

Definition 2.5. A non-trivial group G is *simple* if it contains no proper non-trivial normal subgroups.

Fact 2.6. *If G is simple and Abelian, then $G \cong \mathbb{Z}_p$ for some p.*

Definition 2.7. An *elementary Abelian p-group* is a group of the form $\mathbb{Z}_p^k$.

Definition 2.8. Given a group G and $g, h \in G$, the *commutator* $[g, h] = g^{-1}h^{-1}gh$. We write $[G, H]$ to mean $\{[g, h] : g \in G, h \in H\}$. The *commutator subgroup* G' is the subgroup generated by all commutators. In other words, $G' = [G, G]$.

Definition 2.9. The *commutator chain* of G is the iterated chain of commutator subgroups

$$G \geqslant G' \geqslant G^{''} \geqslant \dots$$

We say G is *solvable* if its commutator chain terminates at $\{e\}$.

There are a few immediate sufficient conditions for solvability. First of all, any Abelian group is solvable. Furthermore, if G is solvable then any subgroup of G is solvable. Finally, the semi-direct product of solvable groups is solvable. We also have the following classic result in group theory:

Theorem 2.10. *(Feit-Thompson) Any group with odd order is solvable.*

Definition 2.11. We say that a subgroup H of G is *characteristic* if for any automorphism σ of G, $\sigma(H) \leqslant H$ (and so $\sigma(H) = H$). We denote this by H *char* G.

One notes that conjugation is an automorphism of G, so if H is a characteristic subgroup of G then it is also a normal subgroup of G. Furthermore, we have the following proposition:

Proposition 2.12. *If $H \trianglelefteq G$ and K char H, then $K \trianglelefteq G$.*

Proof. For any element g in G, consider the action of conjugation restricted to elements of H. This is an automorphism of H since $H \trianglelefteq G$, and thus $gKg^{-1} \leqslant K$. □

Definition 2.13. We say G is *characteristically simple* if its only characteristic subgroups are G and the trivial group.

We immediately are able to deduce the following lemma:

Lemma 2.14. *For any group G, the commutator $G' = [G, G]$ is a characteristic subgroup of G.*

Proof. Let σ be an automorphism of G. Take $k \in \sigma(G')$, so $k = \sigma(ghg^{-1}h^{-1)}$ for some $g, h \in G$. Since σ is a automorphism, we have $k = \sigma(g)\sigma(h)\sigma(g^{-1})\sigma(h^{-1}) = g'h'g'^{-1}h'^{-1}$ where $g', h' \in G$. Therefore, $\sigma(G') \leqslant G'$ so G' is a characteristic subgroup. □

Now we are ready to describe the structure of characteristically simple groups.

Proposition 2.15. *G is characteristically simple if and only if it is the direct product of isomorphic simple groups*

Proof. Suppose G is a finite product $H_1 \times \dots \times H_n$ where the H_i are isomorphic simple groups. We treat the two cases where the H_i are non-Abelian or Abelian. For the non-Abelian case, we need the following lemma:

Lemma 2.16. *If $G = H_1 \times \cdots \times H_n$ where the H_i are non-Abelian and simple, then any normal subgroup N of G is the direct product of some of the H_i.*

Proof. Let $\pi_j : G \to H_j$ be the projection of G onto the jth coordinate. By definition, if $N \trianglelefteq G$, then $\pi_j(N) \trianglelefteq H_j$, so $\pi_j(N) = \{e\}$ or H_j by the simplicity of H_j. We also have that $N \subset \pi_1(N) \times \cdots \times \pi_n(N)$, so the lemma will be complete if we can prove the reverse inclusion.

Before proving the reverse inclusion, we note that since $\pi_j(N)$ is a normal subgroup of H_j, one can check directly from the definitions that $C_{H_j}(\pi_j(N))$ is a normal subgroup of H_j, where $C_{H_j}(\pi_j(N))$ denotes the centralizer of $\pi_j(N)$ in H_j, Since H_j is simple,$C_{H_j}(\pi_j(N))$ must be trivial or all of H_j, but H_j is non-Abelian so $C_{H_j}(\pi_j(N))$ is trivial. In other words, any non-trivial element of $\pi_j(N)$ is non-central in H_j.

By the previous paragraph, if we take a non-trivial element $(g_1, \ldots, g_n) \in N$ (without loss of generality assume $g_1 \neq e$), then g_1 is not central in H_1 so there exists $h \in H_1$ such that $hg_1h^{-1}g_1^{-1} \neq e$. Since N is normal, we conclude

$$(hg_1h^{-1}, g_2, \ldots, g_n) = (h, e, \ldots, e)(g_1, \ldots, g_n)(h^{-1}, e, \ldots, e) \in N$$

multiplying on the right by $(g_1, \ldots, g_n)^{-1}$ gives

$$(hg_1h^{-1}g_1^{-1}, e, \ldots, e) \in N$$

Since $hg_1h^{-1}g_1^{-1} \neq e$, $N \cap (H_1 \times \{e\} \times \cdots \times \{e\})$ is non-trivial. However, $N \cap (H_1 \times \{e\} \times \cdots \times \{e\}) = K \times \{e\} \times \cdots \times \{e\}$ where $K \trianglelefteq H_1$ so we must have $K = H_1$. This imples $H_1 \times \{e\} \times \cdots \times \{e\} \subset N$.

Since we could repeat the above argument with arbitrary index j, we conclude that if the projection $\pi_j(N)$ is nontrivial, then $\{e\} \times \cdots \times H_j \times \cdots \times \{e\} \subset N$. This gives us the reverse inclusion, and completes the lemma. □

Turning back to the proof of the structure of characteristically simple groups, suppose first that the H_i are non-Abelian. By the previous lemma, any proper and non-trivial normal subgroup of G is isomorphic to a direct product of k of the factors, where $k < n$. Without loss of generality, we may assume this non-trivial subgroup is of the form $H_1 \times \cdots \times H_k$. However, this group is not characteristic, since we can take the automorphism that switches the element in any of the H_j with the corresponding element in H_{k+1}. Therefore, G has no non-trivial proper characteristic subgroups, so G is characteristically simple.

We now assume that the H_i are Abelian. By the Classification of Finite Simple Groups, these H_i are isomorphic to $\mathbb{Z}_p$ for some prime number p. Therefore, G is elementary Abelian. We know that $Aut(G)$ contains the direct product of k copies of $Aut(\mathbb{Z}_p)$, and this direct product acts transitively on $\mathbb{Z}_p^k$. Therefore, G must be characteristically simple because for any subgroup H, we can find an automorphism sending an element of H to an element outside of H.

Now suppose G is characteristically simple. Among all nontrivial normal subgroups of G, let H be a minimal normal subgroup with minimal order among all nontrivial normal subgroups. Now consider all possible direct products $H_1 \times \cdots \times H_n$

where $H_1 = H$ and $H_j \cong H$ (so each $H_j \trianglelefteq G$). Let K be the maximal direct product. We claim that K is a characteristic subgroup of G. Let σ be an automorphism of G. We know that $H_j \cong H \implies \sigma(H_j) \cong H$. Furthermore, since g $= \sigma(k)$ for some $k \in G$, $g\sigma(H_j)g^{-1} = \sigma(kH_jk^{-1}) \leqslant \sigma(H_j)$ so $\sigma(H_j) \trianglelefteq G$. Suppose $\sigma(H_j) \nleqslant K$. Then $\sigma(H_j) \cap K$ is a normal subgroup of G and $|\sigma(H_j) \cap K| < |H|$. Since H is minimal, we must have $\sigma(H_j) \cap K = e$. But then $\sigma(H_j) \times K$ is another direct product of isomorphic copies of H, which contradicts the fact that K is maximal. Therefore, we must have $\sigma(H_j) \leqslant K$, so $\sigma(K) \leqslant K$. Since K is a non-trivial proper characteristic subgroup, K=G so G is a direct product of isomorphic copies of H. H is simple because a normal subgroup of H would be a normal subgroup of G (since G is a direct product), so the normal subgroup cannot be proper or non-trivial since H is minimal. Therefore, G is a direct product of isomorphic simple groups. □

Now that we have described the structure of characteristically simple groups, we may connect this concept to normal subgroups and solvable groups.

Definition 2.17. We say N is a *minimal normal subgroup* of G if N is a nontrivial normal subgroup of G and it contains no proper nontrivial normal subgroups of G. We denote this by $N \trianglelefteq^{\min} G$.

Proposition 2.18. *If $N \trianglelefteq^{min} G$ then N is characteristically simple.*

Proof. If N contained a proper non-trivial characteristic subgroup, then it would contain a proper non-trivial normal subgroup of G by Proposition 2.12. Therefore, N must be characteristically simple. □

Proposition 2.19. *If G is characteristically simple and Abelian then G is elementary Abelian.*

Proof. This follows from the lemma below:

Lemma 2.20. *If an Abelian group is simple then it has prime order.*

Proof. If $|G|$ is not prime, then there is some prime $q < |G|$ dividing the order of G. By Cauchy's theorem, there is an element of order q in G, and the subgroup generated by this element is a proper, non-trivial subgroup of G. This contradicts the fact that G is simple since any subgroup of an Abelian group is normal. □

□

Proposition 2.21. *If G is solvable and $N \trianglelefteq^{min} G$ then N is elementary Abelian.*

Proof. Let $N' = [N, N]$, so N' is a characteristic subgroup of N, and therefore it is a normal subgroup of G. Since N is the minimal such subgroup, we must have $N' = N$ or $N' = 1$. In the latter case, N would not be solvable since its commutator chain terminates at a non-trivial group, which would imply that G is not solvable. Therefore, $N' = 1$, which implies that N is Abelian. By Proposition 2.18, N is also characteristically simple, so it must be elementary Abelian by Proposition 2.19. □

2.2. **Permutation Groups.**

Definition 2.22. Given $r \in \mathbb{N}$, let $[r]$ denote the set $\{0, \dots, r-1\}$. Let Ω be a finite set. We refer to the r-element subsets of Ω as r-subsets of Ω. Let $\binom{\Omega}{r}$ denote the set of all r-subsets of Ω. The power set of Ω is denoted as $\mathcal{P}(\Omega)$.

Definition 2.23. A *G-action* on a set Ω is a homomorphism $\phi : G \mapsto Sym(\Omega)$. We then say that G acts on Ω. The *degree* of G is the size of Ω.

Definition 2.24. Given some $x \in \Omega$, the *orbit* of x under a G-action is the set of all $\phi(g)(x)$ for $g \in G$. The *stabilizer* of x is the subgroup H of G such that $\phi(h)(x) = x$ for all $h \in H$. We refer to the stabilizer subgroup of x in G as G_x and the orbit of x as x^G.

If we consider the bijection from $G \backslash G_x$ to x^G given by $gG_x \mapsto g \cdot x$, we immediately have the following relationship between the orbits and stabilizer of a group action:

Lemma 2.25 (Orbit-Stabilizer Lemma)**.** $|G_x| \cdot |x^G| = |G|$

Definition 2.26. A *Permutation Group* G is a subgroup of $Sym(\Omega)$ for some set Ω.

Definition 2.27. A G-action is *transitive* if for any $x, y \in \Omega$, there exists $g \in G$ such that $g(x) = y$. We say that a G-action is *doubly-transitive* if for any two pairs (x, y), (w, z) such that $x \neq y, w \neq z$, there exists $g \in G$ such that $(g(x), g(y)) = (w, z)$.

Proposition 2.28. *Let $|\Omega| = p^k$. If G acts transitively on Ω and P is a Sylow p-subgroup of G, then the action of P on Ω is transitive.*

Proof. Suppose $|G| = p^\alpha m$ where p $\nmid$ m. If we fix $s \in \Omega$, we see that $|s^G| = p^k \mid |G|$ by the Orbit-Stabilizer Lemma. Let P be a Sylow p-subgroup of G so $|P| = p^\alpha$. Then $k \leq \alpha$. We consider the action of G on S restricted to P; let Stab(s)$_P$ denote the stabilizer of s when the action is restricted to P, and Stab(s)$_G$ be the stabilizer when we consider the action of G on s. We know Stab(s)$_P$ and Stab(s)$_G$ are groups, so Stab(s)$_P \leqslant$ Stab(s)$_G$. Furthermore, since Stab(s)$_P \leqslant$ P, |Stab(s)$_P$ | $= p^j$ for some j. Since |Stab(s)$_G$ | $= p^{\alpha-k}m$, |Stab(s)$_P$ | $\leq p^{\alpha-k}$. Then $|orb(s)_P| \geq \frac{p^\alpha}{p^{\alpha-k}} = p^k$ and P also acts transitively. □

Definition 2.29. (Systems of imprimitivity). Let G act on a set Ω transitively. Let R be a G-invariant equivalence relation on Ω. Then the resulting equivalence classes are called *blocks of imprimitivity*, and the resulting set of blocks is called a *system of imprimitivity*. We say that a system of imprimitivity is *trivial* if there is only one block (ie. all of Ω), or all the blocks are singletons.

We say that a group action is *primitive* if it has no non-trivial systems of imprimitivity. Furthermore, we say that a permutation group G is primitive when it acts primtively as a subgroup of $Sym(\Omega)$.

Lemma 2.30. *Every doubly-transitive group is primitive.*

Proof. If we have a non-trivial block B, we can take two elements $y_1, y_2 \in B$ and some $x \notin B$, and there exists an automorphism σ such that $\sigma(y_1) = x, \sigma(y_2) = y_2$, so the block is not preserved. □

The following proposition gives a useful characterization of primitive groups:

Proposition 2.31. *Let G act transitively on a set Ω. G is primitive if and only if $\forall x \in \Omega$, G_x is a maximal subgroup of G.*

Proof. We establish a one-to-one correspondence between blocks containing x and subgroups of G containing G_x: Suppose $x \in B$. We map B to $H = \{g \in G : g(B) = B\}$, and we claim this is a group. Indeed, $1 \in H$, and $g(B) = B \implies g^{-1}(B) = B$. Furthermore, if $g, h \in H$, $g(h(B)) = g(B) = B$ so $gh \in H$. Now suppose $h \in G_x$. Since B is a block, either $h(B) = B$ or $h(B) \cap B = \emptyset$. But $h(x) = x \in B$, so we must have $h(B) = B$, and thus H contains G_x. Suppose H is a subgroup containing G_x. We claim that x^H is a block. If we call this set B, then if $g \in H$ we have $g(B) = B$ (and namely $g(B) \cap B \neq \emptyset$) since $\forall b \in B$, b=$k(x)$ for $k \in H$ so $g(b) = (gk)(x)$ and $gk \in H$ so $(gk)(x) \in x^H$. Now suppose $g(B) \cap B \neq \emptyset$. Take, $k \in g(B) \cap B$. then $k = m(x) \in H$ and $k = gn(x)$ for $n \in H$. Since $m(x) = gn(x)$, $m^{-1}gn(x) = x$ so $m^{-1}gn \in G_x \subset H$. Since $m, n \in H$, this yields $g \in H$. We have shown $g(B) \cap B \neq \emptyset \iff g \in H$, in which case $g(B) = B$, so B is indeed a block. Since $1 \in H$, we know $x \in B$.

If a block contains x, it gets mapped to a subgroup H containing G_x such that $h(B) = B$. The orbit of x under H is the block stabilized by H (by our previous work), so the subgroup maps back to B. Now if H contains G_x, it gets mapped to x^G under H. If we call this block B, it gets mapped to the subgroup that stabilizes it, which we have shown is H. Therefore, we have established a one-to-one correspondence between blocks containing x and subgroups of G containing G_x. G is primitive iff the block B containing x is either $\{x\}$ or Ω. However, $B = \{x\} \iff H = G_x$ and $B = \Omega \iff H = G$. We conclude G is primitive iff G_x is maximal. □

We now give an explicit example of a primitive group action:

Example 2.32. If $S_n^{(k)}$ denotes the natural action of S_n on $k-$subsets of $[n]$ and $k < \frac{n}{2}$, then $S_n^{(k)}$ is primitive. Note that this action has degree $\binom{n}{k}$.

Proof. Let X be the set of k-subsets. By the previous proposition, we need to show that G_x is maximal in G for any k-subset x. Let H be a subgroup containing G_x. Suppose $\exists\ h \in H - G_x$. We want to show that $H = G$, so it suffices to show that $\forall g \in G - G_x$, we have $< g, G_x >= G$.

Since x is a k-subset, its complement y in X is an $(n-k)$-subset, and $|y| > |x|$. We know that g stabilizes x if and only if g permutes the elements of x and g permutes the elements of y. Thus, $G_x = Sym(x) \times Sym(y)$.

We know that if $m \in G = S_n$, then m can be written as the product of transpositions. These transpositions are either between two elements of x, two of y, or one from each subset. The transpositions between two elements of x and two of y are contained in G_x, so if we can show that the "mixed" transposition is in $< g, G_x >$, then this will generate all of G.

We know that $h(x) = x$ setwise if and only if $h(y) = y$ setwise. Therefore, since $g \notin G_x$, there exists $p \in y$ such that $g(p) \in x$. Suppose $g(p) \in x$ for all $p \in y$. Then we would have an injection from y into x, which would imply $|y| \leq |x|$, which is a contradiction. Therefore, there must also be some $q \in y$ such that $g(q) \in y$. We have that (pq) is in G_x since it's in $Sym(y)$, so $g(pq)g^{-1} = (xy) \in< g, G_x >$. Therefore, $H = G$, so G_x is maximal and G is primitive. □

Proposition 2.33. *Let G be a primitive permutation group. If N is a non-trivial normal subgroup of a G, then N is transitive.*

Proof. Let N be a non-identity normal subgroup, and let $\mathcal{F}$ be the collection of N-orbits of x for some fixed $x \in \Omega$. Since $N \trianglelefteq G$, automorphisms of G permute the elements of $\mathcal{F}$. Therefore, $\mathcal{F}$ forms a partition of Ω that is G-invariant. Since G is primitive, $\mathcal{F}$ must be a collection of singletons or all of Ω. The former case would imply N is the identity group, so we must have the latter. Therefore, N acts transitively on Ω. □

Proposition 2.34. *Let G be a primitive and solvable group acting on Ω. Then G has prime-power degree.*

Proof. G has a minimal normal subgroup N (where we allow N=G), and N is elementary Abelian by Proposition 2.21. Furthermore, N is transitive by the previous proposition so $|\Omega|$ divides $|N|$. Since $|N| = p^k$, $|\Omega|$ is a prime power. □

Remark 2.35. We note that in this proof, we can actually conclude $|\Omega| = |N|$ by Lemma 2.38

Proposition 2.36. *Given any prime power q, we can construct a primitive solvable group:*

Since q is a prime power, there exists a finite field $\mathbb{F}_q$. Let Aff($\mathbb{F}_q$) denote the affine transformations of $\mathbb{F}_q$. In other words, every element $\sigma \in$ Aff($\mathbb{F}_q$) is of the form $\sigma(x) = ax + b$ with $a \in \mathbb{F}_q^\times, b \in \mathbb{F}_q$. Then Aff($\mathbb{F}_q$) is a semidirect product of the additive subgroup of $\mathbb{F}_q$ with $GL(1, q)$. Both of these groups are abelian, so they are solvable. Therefore, Aff($\mathbb{F}_q$) is solvable. Now, we claim Aff($\mathbb{F}_q$) is doubly-transitive. Take $(x, x'), (y, y')$ such that $x \neq x'$ and $y \neq y'$. We want to find $\alpha \in \mathbb{F}_q^\times$ and $\beta \in \mathbb{F}_q$ such that $\alpha x + \beta = y$ and $\alpha x' + \beta = y'$. In other words, we want to solve

$$\begin{bmatrix} x & 1 \\ x' & 1 \end{bmatrix} \begin{bmatrix} \alpha \\ \beta \end{bmatrix} = \begin{bmatrix} y \\ y' \end{bmatrix}$$

This has a solution since $x \neq x'$ implies the leftmost matrix is invertible, and $\alpha \neq 0$ since $y \neq y'$. We conclude Aff($\mathbb{F}_q$) is indeed doubly-transitive. Since Aff($\mathbb{F}_q$) must be primitive by Lemma 2.30, Aff($\mathbb{F}_q$) is a primitive and solvable permutation group of degree q.

Definition 2.37. Let G act on Ω. If, for any $g \in G$, $gx = x$ for some $x \in \Omega$ implies g=1, We say that this action is *semiregular.* The action of G is *regular* if it is transitive and semiregular.

Lemma 2.38. *If G acts regularly on Ω then $|G| = |\Omega|$.*

Proof. Let G be regular and fix $x \in \Omega$. Take $\phi : G \mapsto \Omega$ where $\phi(g) = g(x)$. Since G is transitive, orb(x)=X so $\forall p \in X$, $\exists g$ such that $g(x) = p$ so ϕ is surjective. Suppose $g_1(x) = g_2(x)$. Then $g_2^{-1} g_1(x) = x \implies g_2^{-1} g_1 \in stab(x) \implies g_2^{-1} g_1 = 1$ since G is semiregular. Therefore, $g_1 = g_2$ so ϕ is injective. Thus, $|G| = |\Omega|$. □

Proposition 2.39. *If G is a transitive Abelian group, then G is regular.*

Proof. Let G be Abelian and take $x \in \Omega$. Suppose $g \neq 1$ and $g \in stab(x)$. Take $y \in \Omega$. Then $\exists h \in G$ such that h(y) = x. Then $y = (h^{-1}g)(x) = (gh^{-1})(x) = g(y)$

so $g \in stab(y)$. Then g stabilizes all of Ω so g=1. Therefore, G is semiregular so it is regular since it is also transitive. □

Definition 2.40. The *left and right regular representations* of a group G, denoted by L_G and R_G, are the actions of G on itself defined respectively by $L_g : x \mapsto g^{-1}x$ and $R_g : x \mapsto xg$.

Lemma 2.41. *The left and right regular representations are regular actions.*

Proof. We will just show that R_G is regular since the proof for L_G is analogous. Given some x, $xg = x \iff g = 1$ so the stabilizer of x under R_G is 1. Therefore, R_G is semiregular. Furthermore, given x and y, $x(x^{-1}y) = y$ so $\rho_{x^{-1}y}(x) = y$ and R_G is transitive. Thus, R_G is regular. □

Proposition 2.42. *Systems of imprimitivity for R_G are precisely the right cosets of subgroups of G. An analogous statement holds for L_G.*

Proof. If $H \leqslant G$, right cosets partition G and the collection of cosets is invariant under R_G, so the collection of cosets form a system of imprimitivity. Now suppose $\mathcal{B}$ is a system of imprimitivity for R_G and B is the block containing 1. We claim B forms a subgroup of G. Suppose $a, b \in B$. Since $ab = R_b(a)$ and $b = R_b(1) \in B$, we must have $ab \in B$. Furthermore, since $a^{-1} = R_{a^{-1}}(1)$ and $1 = R_{a^{-1}}(a) \in B$, we must have $a^{-1} \in B$, so B is indeed a subgroup. Therefore, $\mathcal{B}$ consists of all right cosets of B. □

The above proposition also allows us to characterize systems of imprimitivity for R_GL_G. We notice that R_GL_G is a group since $R_GL_G = L_GR_G$.

Proposition 2.43. *A system of imprimitivity for R_GL_G is the set of all cosets for a normal subgroup.*

Proof. Let H be a normal subgroup of G. Let $R_G \times 1$ be the subgroup of R_GL_G where $y = 1$, and $1 \times L_G$ be the subgroup of R_GL_G where $x = 1$. The blocks of any system of imprimitivity take the form $x^{-1}Hy$ since $\mathcal{B}$ is a system of imprimitivity for R_GL_G if and only if it is a system of imprimitivity for $R_G \times 1$ and $1 \times L_G$. Furthermore, R_g and $L_{g^{-1}}$ both send H to the same block for any $g \in G$ since both permutations send 1 to g. This is equivalent to saying that $gH = Hg$ so H is a normal subgroup of G. □

Corollary 2.44. *R_GL_G is primitive if and only if G is simple.*

Proof. This is immediate from the previous proposition and the fact that H is trivial if and only if the corresponding blocks are singletons and H=G if and only if the corresponding block is all of G. □

We end the section with the statement of Burnside's Theorem, which is a classic result from the theory of permutation groups that we will utilize throughout this paper. A remarkably short and beautiful proof of this result can be found in [25].

Theorem 2.45 (Burnside's Theorem)**.** *Every transitive group with prime degree is either doubly-transitive or solvable.*

3. Symmetry Conditions on Graphs

Having laid the foundations of Group Theory, we now discuss symmetry conditions on graphs. We begin by describing some elementary concepts from graph theory and fixing notation. We then describe the various measures of symmetry a graph may have. Out of the measures we mention, we are especially concerned with vertex-primitivity and arc-transitivity. We conclude the section by giving a discussion of the Platonic Solids, with the purpose of illustrating how one can switch between the graph-theoretic and geometric notions of a graph.

3.1. **Graph Theory Preliminaries.**

Definition 3.1. We call X = (V, E) a *graph* with vertex set V(X) and edge set E(X), where an *edge* is an unordered pair of vertices. We will refer to the edge e joining x and y as xy. We say that x and y are *adjacent* if xy is an edge, in which case x and y are *neighbors.* Furthermore, x is *incident* with an edge if it is one of the two vertices on the edge. The *degree* or *valency* of x is the number of neighbors it has, and a graph is *regular* if all of its vertices have the same degree. We say $X = (V, E)$ is a *directed graph* or *digraph* where $E \subset V \times V$ is a set of directed edges. A vertex x is *incident* with e if $e = xy$ or $e = yx$. Vertices x and y are *adjacent* if $xy \in E$ or $yx \in E$. Then *indegree* of a vertex v, denoted $deg_X^-(v)$, is the number of vertices u such that $uv \in E$. Similarly, the *outdegree* $deg_X^+(v)$ is the number of vertices u such that $vu \in E$. If E is the edge set of a digraph Y, E^- denotes the edges uv such that $vu \in E$.

Fact 3.2. *Given a graph $X = (V, E)$, we can construct a digraph $Y = (V, E')$ where we add the edges uv and vu to E' for every edge uv in E. In this way, a graph can be viewed as a digraph. Given a digraph $X = (V, E)$, we can construct a graph $Y = (V, E')$ where $E' = E \cup E^-$.*

Definition 3.3. A *loop* is an edge from a vertex to itself. A graph is *simple* if it contains no loops and there is at most one edge between any two vertices.

The graphs we consider in this paper are simple. In addition, they are *finite*, meaning that the vertex set V is a finite set.

Definition 3.4. A graph is *complete* if its edge set is maximal. We denote the complete graph on n vertices by K_n. A graph with no edges is called *empty.*

Definition 3.5. Let $X = (V, E)$ be a graph. Given $u, v \in V$, a *walk* of length l from u to v is a sequence of vertices $z_0, z_1, \ldots, z_l$ where $z_0 = u$, $z_l = v$, and $z_i z_{i+1} \in E$ for $0 \leq i \leq l - 1$.

Definition 3.6. Let $X = (V, E)$ be a digraph. Given $u, v \in V$, a *directed walk* of length l from u to v is a sequence of vertices $z_0, z_1, \ldots, z_l$ where $z_0 = u$, $z_l = v$, and $z_i z_{i+1} \in E$ for $0 \leq i \leq l - 1$.

Definition 3.7. A *cycle* of length l is a walk where the only repeated vertices are z_0 and z_l.

A graph $X = (V, E)$ is *connected* if for any $u, v \in V$, there exists a walk from u to v. A digraph $X = (V, E)$ is *weakly connected* if the graph resulting from the construction in **Fact 1** is connected. A digraph $X = (V, E)$ is *strongly connected* if for any $u, v \in V$, there exists a directed walk from u to v.

Definition 3.8. Given a graph X, the *distance* between vertices u and v is the length of the shortest walk from u to v. This is denoted $d(u, v)$.

Definition 3.9. The *diameter* of a graph is the maximum distance between two vertices.

Definition 3.10. If $X = (V, E)$ is a digraph, the $|V| \times |V|$ *adjacency matrix* A(X)= $(m_{i,j})$ is defined by:

$$m_{i,j} = \begin{cases} 1 & v_i v_j \in E \\ 0 & \text{otherwise} \end{cases} \tag{3.11}$$

where v_i, v_j range over all elements of V.

Definition 3.12. A *tournament* on n vertices is an orientation of a complete graph, where we assign a direction to each edge of K_n.

Fact 3.13. *There are* $2^{\binom{n}{2}}$ *possible tournaments on n vertices.*

We include the following proposition, which details some interesting properties of tournaments. This proposition uses the notions of vertex-transitivity and vertex-primitivity, which are defined in the next subsection as Definition 3.23.

Proposition 3.14. *Let T be a tournament with n vertices. Then*

(1) Aut(T) has odd order
(2) If T is vertex-transitive, then n is odd.
(3) If T is vertex-primitive, then n is an odd prime power.

Proof. To prove (1), suppose some $\sigma \in$ Aut(T) had order 2. Then σ contains some transposition. This is not possible, however, because the transposition would reverse the orientation of the directed edge between the corresponding vertices. Therefore, there is no element of order 2 and by Cauchy's Theorem Aut(T) has odd order. We immediately obtain (2) from (1) and the definition of transitivity. Finally, we notice that Feit-Thompson's Theorem implies that Aut(T) is solvable. Therefore, under the assumption of vertex-primitivity, we may apply Proposition 2.34 to obtain (3). □

The first part of the above proposition shows that Feit-Thompson implies that the automorphism group of every tournament is solvable. In the next proposition, we prove that these two statements are in fact equivalent.

Proposition 3.15. *The Feit-Thompson Theorem is equivalent to the statement that the automorphism group of every tournament is solvable.*

Proof. In light of the previous proposition, it suffices to show that if the automorphism group of every tournament is solvable, then this statement implies Feit-Thompson.

Let G be a group of odd order. If we take V to be the elements of G, then G_L acts regularly on V. Let E' be all ordered pairs of elements in V. Since G has odd order, no element of G_L can send $(x, y) \mapsto (y, x)$ when it acts on E', since this would imply that this element has even order.Therefore, the orbits of E' under the action of G_L can be matched into pairs $< S, S' >$ such that $S = \{(x, y) : (y, x) \in S'\}$.

If we take the union of exactly one set from each pair to be our edge set E and V to be our vertex set, then the result is a G_L-invariant tournament on V whose automorphism group includes G. If we call our tournament X, then $Aut(X)$ is solvable by assumption, and since G is a subgroup of $Aut(X)$ it is also solvable. □

Definition 3.16. Given a digraph X, a set $B \subset V$ is *independent* if it does not contain any edges. The size of the largest independent set is called the *independence number*, denoted by $\alpha(X)$.

Definition 3.17. A set $P \subset V$ is called a *clique* if any two vertices in G are adjacent. If P has size t, the subgraph induced by P is K_t. We define the *clique number* $\omega(X)$ as the maximum t such that K_t is a subgraph of X.

Definition 3.18. Given a graph $X = (V, E)$ the *complement* $\bar{X} = (V, E')$ is the graph with vertex set V, where we require that $(x, y) \in E' \iff (x, y) \notin E$.

Proposition 3.19. *Let $X = (V, E)$ be a graph. Then $\alpha(X) = \omega(\bar{X})$.*

Proof. Since u and v are nonadjacent in X iff they are adjacent in $\bar{X}$, $S \subset V$ is an independent set in X iff it is a clique in $\bar{X}$. □

Definition 3.20. Suppose we fix a finite set C of colors and a graph X. A map f from $V(X)$ to C is a *proper coloring* if no two adjacent vertices are assigned the same color. If $|C| = k$ and there exists a proper coloring f, we say that X is *k-colorable.* The *chromatic number* $\chi(X)$ is the minimum k such that X is k-colorable.

Definition 3.21. Let X and Y be graphs. A mapping f from $V(X)$ to $V(Y)$ is called a *homomorphism* if $f(x)$ and $f(y)$ are adjacent whenever x and y are adjacent. If f is a bijection, we call it an *isomorphism*, and we say that X and Y are *isomorphic.* An *automorphism* is an isomorphism from X to itself. We summarize some facts about graph automorphisms:

Lemma 3.22. *For any graph X, the following are true of $Aut(X)$:*

(1) *If $v \in V(X)$ then $deg(v) = deg(\sigma(v))$ for all $\sigma \in Aut(X)$.*
(2) *If $\sigma \in Aut(X)$ then $d(u, v) = d(\sigma(u), \sigma(v))$.*
(3) *$Aut(X) = Aut(\bar{X})$.*

Proof. (1) If $N(v)$ denotes the set of neighbors of v, we immediately have that $S = \{\sigma(u) : u \in N(v)\} \subset N(\sigma(v))$ since automorphisms preserve adjacency. Futhermore, if $s \in N(\sigma(v))$ then $\sigma^{-1}(s) \in N(v)$ so $s \in S$. We conclude $S = N(\sigma(v)$, so $deg(v) = deg(\sigma(v))$.
(2) Set $d(u, v) = d$, and let $u = v_0 \dots v_d = v$ be a shortest path from u to v. Since $\sigma(v_0) \dots \sigma(v_d)$ is a path from $\sigma(u)$ to $\sigma(v)$, we have $d(\sigma(u), \sigma(v)) \leq d$. If $\sigma(u) = s_0 \dots s_m = \sigma(v)$ is a shortest path from $\sigma(u)$ to $\sigma(v)$, then $\sigma^{-1}(s_0) \dots \sigma^{-1}(s_m)$ is a path from u to v, so we must have $d \leq m$. Therefore, $d(u, v) = d(\sigma(u), \sigma(v))$.
(3) This is trivially true since automorphisms preserve adjacency (and also inadjacency).

□

3.2. Measures of Symmetry.

Definition 3.23. A Graph X is *vertex-transitive* if its automorphism group acts transitively on its vertices. We say X is *vertex-primitive* if $Aut(X)$ acts primitively on its vertices.

We notice that a vertex-transitive graph must be regular since automorphisms cannot map one vertex to another vertex with different degree. However, the converse is not true. Indeed, let X be the disjoint union of a 3-cyle and a 4-cycle. Then X is 2-regular but not vertex-transitive. In fact, we can even obtain a connected graph that is regular but not vertex-transitive by taking the complement of X.

Definition 3.24. An *arc* is an ordered pair of adjacent vertices. A graph is *arc-transitive* if its automorphism group acts transitively on its arcs.

Central to the study of this paper are "Vertex-Primitive, Arc-Transitive" graphs. We will refer to these as VPAT graphs. We note that edge-transitivity is the same as arc-transitivity for digraphs, and we illustrate a special connection between vertex-transitivity and edge-transitivity:

Lemma 3.25. *Let X be a connected, edge-transitive graph with no isolated vertices. If X is not vertex-transitive, then X is bipartite.*

Proof. Let $G = Aut(X)$, and fix some vertex x. Since x cannot be isolated, we may choose some vertexx y that is adjacent to x. We now claim that $x^G \cup y^G = V$. Indeed, if $v \in V$ then we may select some vertex u that is adjacent to v, and by edge-transitivity there exists an automorphism sending (x, y) to (u, v), so $v \in x^G \cup y^G$.

Now, we claim that $x^G \cap y^G \neq \emptyset$ implies that X is vertex-transitive. Take any $v \in V$. Suppose $x^G \neq V$ so there exists $v \notin x^G$. By the previous paragraph, $v \in y^G$ so there is an automorphism σ such that $\sigma(y) = v$. However, we may take $k \in x^G \cap y^G$ so there is an automorphism that sends x to k and another (possibly the same) automorphism that sends k to y. Composing these two automorphisms with σ creates an automorphism ρ such that $\rho(x) = v$, so $v \in x^G$. This is a contradiction, so we must have $x^G = V$, which implies that X is vertex-transitive. However, this is a contradiction to the assumption of the lemma, so we conclude $x^G \cap y^G = \emptyset$.

Suppose $u, v \in x^G$ and $u \sim v$. By edge-transitivity of X, there is an automorphism that sends (x, y) to (u, v), which would imply for instance that $v \in y^G$. This contradicts the previous paragraph, where we showed that x^G and y^G are disjoint, so no two vertices of x^G can be adjacent. A similar argument shows that no two vertices of y^G can be adjacent either. In other words, all edges of X are incident to exactly one vertex of x^G and one vertex of y^G. This allows us to conclude that X is bipartite. □

Definition 3.26. A graph is *distance-transitive* if, given any two pairs of vertices $(u, v), (x, w)$ such that $d(u, v) = d(x, w)$, there exists an automorphism sending u to x and v to w.

By definition, vertex-primitive graphs are also vertex-transitive, and distance-transitive graphs are also arc-transitive.

Lemma 3.27. *There exist graphs which are vertex-primitive but not arc-transitive.*

Proof. Take the cycle C_7 and add chords of length 2. If we call this graph X, then we can immediately observe that $\mathbb{Z}_7 \leqslant Aut(X)$. Since $\mathbb{Z}_7$ acts primitively on the vertices of X, X is vertex-primitive. If we label the vertices in our graph as $v_0, v_1, \dots, v_6$, we claim that no automorphism can send the arc (v_1, v_2) to (v_1, v_3). Such an automorphsim would have to send v_2 to v_3 while keeping v_1 fixed, but this would force $\sigma(v_3) = v_2$ since v_3 is adjacent to both v_1 and v_2. However, this would force either $\sigma(v_4)$ or $\sigma(v_5)$ to be adjacent to v_1, but v_1 is not adjacent to v_4 or v_5. Therefore, no such automorphism can exist. □

Lemma 3.28. *There exist graphs which are arc-transitive but not distance transitive.*

Proof. As we will show in Proposition 4.14, the Kneser Graphs $Kn(r, s)$ are arc-transitve for all parameters r and s, but they are not distance-transitive for $2 < s \leq \frac{r}{2} - 1$. □

Lemma 3.29. *If X is distance-transitive, then it is also vertex-transitive.*

Proof. If we consider the pairs of vertices $(u, u), (v, v)$, for any $u, v \in V$, then $d(u, u) = 0 = d(v, v)$ so there is an automorphism sending u to v □

Therefore, we have distance-transitive $\implies$ arc-transitive $\implies$ vertex-transitive.

3.3. **Platonic Solids.**

Definition 3.30. Let $Cong(\mathbb{R}^n)$ denote all congruences of $\mathbb{R}^n$. By *congruence,* we mean distance-preserving transformations under the Euclidean norm.

Definition 3.31. An *orthogonal transformation* is one that fixes the origin. We denote the group of orthogonal transformations on $\mathbb{R}^n$ by $O(\mathbb{R}^n)$, or $O(n)$. If we fix an orthonormal basis for $\mathbb{R}^n$, we may represent the elements of $O(n)$ by $n \times n$ orthogonal matrices (ie. all matrices A such that $A^{-1} = A^T$).

Remark 3.32. From the fact that $A^{-1} = A^T$, $det(A^{-1}) = \frac{1}{det(A)}$, and $det(A^T) = det(A)$ for any square matrix A, we see that $det(A) = \pm 1$ for all orthogonal matrices A. Let $O^+(n)$ denote the subgroup of $O(n)$ such that all elements have determinant 1. We call this the group of direct symmetries.

Lemma 3.33. *The direct symmetries $O^+(n)$ are a normal subgroup of $O(n)$ with index* 2.

Proof. Let ϕ be a map from $O(n)$ to $\mathbb{Z}_2$ such that ϕ maps matrices with determinant 1 to 0, and matrices with determinant -1 to 1. One can verify that ϕ is a surjective homomorphism, and its kernel is $O^+(n)$ so we have $\frac{|O(n)|}{|O^+(n)|} = 2$ by the First Isomorphism Theorem. The fact that $O^+(n)$ is a normal subgroup immediately follows from the fact that it has index 2. □

Definition 3.34. The *central reflection* about the origin takes x to $-x$ for all $x \in \mathbb{R}^n$. It is represented by the matrix $-I$, where I is the identity. We see that $< -I >$ is a normal subgroup of index 2 since $-I$ is in the center of $O(n)$.

We now consider the problem of representing $O(n)$ as a direct product of its group of direct symmetries with the group generated by its central reflection. If n is even, then $det(-I) = (-1)^n = 1$, so $-I \in O^+(n)$. This implies that $Z(O^+(n) \times < -I >) = < -I > \times < -I >$, so in particular the center of this group has size 4.

This means that $O(n) \ncong O^+(n) \times < -I >$ as the orthogonal group has center of size 2. In the case where n is odd, we now show that $O(n)$ can be expressed as this direct product:

Lemma 3.35. *If n is odd then $O(n) = O^+(n) \times < -I >$.*

Proof. Since n is odd, $det(-I) = (-1)^n = -1$, so $-I \notin O^+(n)$. This also implies that $A \in O^+(n) \iff -A \notin O^+(n)$, so if $G = \{AB : A \in O^+(n), B \in < -I >\}$ then $G = O(n)$. By Lemma 3.33 and Definition 3.34, both of these groups are normal subgroups, and their intersection is I. Therefore, their direct product is $O(n)$. □

Definition 3.36. A *Platonic solid* is a 3-dimensional convex polyhedron whose faces are regular. The five platonic solids are the tetrahedron, cube, octahedron, dodecahedron, and icosahedron. Given some Platonic solid P, let $V(P)$ denote the set of its vertices and $E(P)$ denote the set of its edges.

Definition 3.37. Let $Cong(P)$ denote the subgroup of $Cong(\mathbb{R}^3)$ that take P to itself. Since $Cong(P)$ always fixes the center of gravity of P, we always assume that P is centered at the origin. Furthermore, let $Cong^+(P) = Cong(P) \cap O^+(3)$. We say that P is centrally symmetric if the central reflection is a congruence of P, so $-I \in Cong(P)$

If P is a centrally symmetric solid (not necessarily a Platonic solid), then we can repeat the similar arguments as Lemma 3.33 and Definition 3.34 to show that $Cong^+(P)$ is a normal subgroup of $Cong(P)$ with index 2, and $< -I >$ is a normal subgroup of $Cong(P)$ with order 2. Now, given that n is odd (since we are working in 3 dimensions), we also have that $Cong^+(P) \cap < -I >= I$, and we can repeat the same argument as in the proof of Lemma 3.35 to show that if $G = \{AB : A \in Cong^+(P), B \in < -I >\}$ then $G = Cong(P)$. Putting these arguments together, we have the following lemma:

Lemma 3.38. *If P is a centrally symmetric solid then $Cong(P) = Cong^+(P) \times < -I >$.*

Definition 3.39. Two Platonic solids are *dual* if one can be constructed by placing a vertex at the center of each face of the other polyhedron, and letting two vertices be adjacent if the corresponding faces were adjacent. If two Platonic solids are dual, then they have the same group of congruences.

We may now compute the congruence groups of all five Platonic solids. Since the cube and octahedron are dual, and the dodecahedron and icosahedron are dual, it suffices to compute the automorphism groups of the tetrahedron, cube, and dodecahedron.

Proposition 3.40. *If P is a tetrahedron then $Cong(P) \cong S_4$.*

Proof. Since any pair of vertices in P are adjacent, we can send the first vertex anywhere and each successive vertex to any remaining point, so the number of symmetries is $4 * 3 * 2 * 1 = 24$. Label the vertices of the tetrahedron 1, 2, 3, and 4 and consider the action of $Cong(P)$ on the set. This gives a homomorphism ϕ from $Cong(P)$ to S_4. Clearly, $id \in ker(\phi)$. Suppose $\sigma \neq id$ and $\sigma \in Cong(P)$. Then without loss of generality we may assume $\sigma(1) \neq 1$, so $\sigma \notin ker(\phi)$. Therefore, ϕ is injective, and since the domain and codomain are the same size, we must have $Cong(P)$ is isomorphic to S_4. □

For the next two propositions the Platonic solids in question are centrally symmetric, so we may apply Lemma 3.38 to conclude that $Cong(P) \cong Cong^{+}(P) \times \mathbb{Z}_2$, so it suffices to compute $Cong^{+}(P)$.

Proposition 3.41. *If P is a cube then $Cong(P) \cong S_4 \times \mathbb{Z}_2$.*

Proof. Since every direct symmetry permutes the cube's 4 main diagonals and only the identity automorphism fixes all 4 diagonals, the group of direct symmetries is contained in S_4. Since we may map each edge to any other edge by 2 direct symmetries and the cube has 12 edges, the cube has at least 24 direct symmetries. Therefore, $Cong^{+}(P) \cong S_4$. □

Proposition 3.42. *If P is a dodecahedron then $Cong(P) \cong A_5 \times Z_2$.*

Proof. Since the dodecahedron has 5 diagonals, $Cong^{+}(P) \leqslant S_5$. Now, we claim that $|Cong^{+}(P)| = 60$:

Consider the action of $Cong^{+}(P)$ on the vertices of P. Since P is a Platonic solid, this action is transitive on its vertices so if we fix a vertex v, we know $|orb(v)| = 20$. Since the only symmetries that fix v are the rotations about the axis passing through v, we know $|stab(v)| = 3$. By the Orbit-Stabilizer Lemma, we conclude that $|Cong^{+}(P)| = 60$.

Our previous work shows that $Cong^{+}(P)$ is an index 2 subgroup of S_5, but the only such subgroup is A_5, so we conclude $Cong^{+}(P) \cong A_5$. □

We can associate any Platonic solid P with a graph $X(P) = (V, E)$ as follows: Let $V = V(P)$ and E be all pairs of points $\{x, y\}$ such that the segment xy is an edge of P. It is clear that every congruence of P induces an automorphism of $X(P)$, which leads one to ask whether the converse is true for Platonic solids:

Observation 3.43. *If $f : Cong(P) \mapsto Sym(V)$ is the restriction map, then f gives an injective homomorphism from $Cong(P)$ to $Sym(V)$, so $f(Cong(P)) \leqslant Aut(X)$ and $Cong(P)$ is isomorphic to a subgroup of $Aut(X)$.*

Given the above observation, in order to show that $Cong(P) \cong Aut(X)$ for each Platonic solid P, it suffices to show that $|Cong(P)| \geq |Aut(X)|$. Since we have computed $Cong(P)$ for each Platonic solid in Propositions 3.40-3.42, we simply need to show that $|Aut(X)|$ is less than or equal to the size of the congruence groups we computed for each Platonic solid. We accomplish this in the next 5 propositions, which show that the resulting automorphism group from when we view each Platonic solid as a graph has the same structure as the congruence group.

Proposition 3.44. *If X is the Tetrahedron then $|Aut(X)| \leq 24$.*

Proof. Since X has 4 vertices its automorphism group must be a subgroup of S_4 so $|Aut(X)| \leq 24$. □

Proposition 3.45. *If X is the Cube then $|Aut(X)| \leq 48$.*

Proof. If we pick some vertex v, then any given automorphism can send v to each of the 8 vertices in the cube. Since the three vertices that are adjacent to the image of v must be some permutation of the three vertices that are adjacent to v, we conclude $|Aut(X)| \leq 8 \times (3!) = 48$. □

Proposition 3.46. *If X is the Octahedron then $|Aut(X)| \leq 48$.*

Proof. We notice that if we fix a vertex v then any vertex adjacent to v is also adjacent to 2 other neighbors of v. Label the neighbors of v as v_1, v_2, v_3, and v_4 and assume without loss of generality that v_1 is adjacent to v_2 and v_3. There are 6 vertices in the octahedron, so any automorphism of X could send v to one of 6 places. Furthermore, v_1 could go to any of the 4 vertices adjacent to the image of v, and v_2 could go either of the two vertices adjacent to $im(v_1)$ and $im(v)$. This fixes where v_3 and v_4 must go, since v_3 must go to the only remaining vertex adjacent to $im(v_1)$ and $im(v)$, and v_4 could only go to the remaining vertex adjacent to v. Therefore, $|Aut(X)| \leq 6 \times 4 \times 2 = 48$. □

Proposition 3.47. *If X is the Dodecahedron then $|Aut(X)| \leq 120$.*

Proof. If we fix a vertex v, then there are 20 vertices where v can end up under any automorphism, and the 3 vertices adjacent to the image of v must be some permutation of the 3 vertices that were adjacent to v, so $|Aut(X)| \leq 20 \times (3!) = 120$. □

Proposition 3.48. *If X is the Icosahedron then $|Aut(X)| \leq 120$.*

Proof. If we fix a vertex v then any vertex adjacent to v shares 2 common neighbors with v. If $v_1, \ldots v_5$ represent the vertices adjacent to v, then we may assume that v_1 is adjacent to v_2 and v_3, v_4 is adjacent to v_2, and v_5 is adjacent to v_3. There are 12 places v could go, and 5 places v_1 could go under any automorphism. Furthermore, v_2 must go to one of the two vertices adjacent to $im(v)$ and $im(v_1)$. This fixes where the rest of the vertices must go, since v_3 must go to the remaining vertex adjacent to $im(v)$ and $im(v_1)$, v_4 must go to the remaining vertex adjacent to $im(v_2)$ and $im(v)$, and v_5 must go to the remaining vertex adjacent to $im(v_3)$ and $im(v)$. Therefore, $|Aut(X)| \leq 12 \times 5 \times 2 = 120$. □

Definition 3.49. We construct the *Petersen Graph* P as follows: let the vertices of P correspond to $2-$subsets of $[5]$ and let 2 vertices be adjacent if and only if the corresponding $2-$subsets are disjoint. The resulting graph is $3-$regular with 10 vertices and 15 edges.

To compute the automorphism group of the Petersen Graph, we introduce the concept of a Line Graph and state a theorem of Whitney describing the relationship between the automorphism group of a graph and its corresponding line graph.

Definition 3.50. If X is an undirected graph, its *line graph* $L(X)$ is a graph whose vertices correspond to the edges of X, where two vertices in $L(X)$ are adjacent if the corresponding edges intersect in X.

Theorem 3.51 (Whitney [29]). *If X is a connected graph with at least 5 vertices, then $Aut(X) \cong Aut(L(X))$.*

We now show that the automorphism group of the Petersen Graph is S_5. Notice that the Petersen Graph thus has the same number of automorphisms as the dodecahedron, but automorphism group is not isomorphic to the automorphism group of the dodecahedron since the latter has a center of size 2 while S_5 has a trivial center.

Proposition 3.52. *If P is the Petersen Graph then $Aut(P) \cong S_5$.*

Proof. By definition, the Petersen graph is the complement of the line graph $\mathrm{L}(K_5)$, so $\mathrm{Aut}(P) \cong \mathrm{Aut}(L(K_5))$ by Lemma 3.22. Since K_5 has 5 vertices, its automorphism group is isomorphic to the automorphism group of $\mathrm{L}(K_5)$ by Theorem 3.51. Since $\mathrm{Aut}(K_5) \cong S_5$, we conclude $Aut(P) \cong S_5$. □

4. Highly Symmetric Graphs

With our measures of symmetry in place, we introduce the families of Paley Graphs, Kneser Graphs, Johnson Graphs, and Hamming Graphs. In the subsequent sections of this paper, we will prove results that relate the symmetries of these graphs to their combinatorial parameters, but the goal of this section is to discuss how symmetric each of these families are.

4.1. **Paley Graphs.**

Definition 4.1. Let q be a prime power congruent to 1 mod 4. Consider a graph with vertex set $\mathbb{F}_q$, where $x, y \in V$ are adjacent if $x - y$ is a non-zero square. The resulting graph is known as the *Paley Graph $P(q)$*.

Remark 4.2. The Paley Graph is undirected since -1 is a square when $q \equiv 1$ mod 4. If we repeated the above construction with $q \equiv 3$ mod 4, we would obtain a tournament on q vertices which is known as the *Paley Tournament.*

Remark 4.3. Because there are $\frac{q-1}{2}$ quadratic residues in the finite field $\mathbb{F}_q$, $P(q)$ is $\frac{q-1}{2}$-regular.

Proposition 4.4. *The Paley Graph $P(q)$ is VPAT.*

Proof. We first prove two lemmas. The first lemma states that the automorphism group of P_q contains the affine semilinear transformations of F_q. In fact, the automorphism group of P_q is precisely these transformations, and later we give a proof of this fact when q is a prime.

Lemma 4.5. *If $A = \{f(x) = ax^\sigma + b : a \in (\mathbb{F}_q^\times)^2, \sigma \in Aut(\mathbb{F}_q), b \in F_q\}$, then $Aut(P_q)$ contains A.*

Proof. Let $f(x) = x + b$. Then $v - q$ is a quadratic residue iff $f(v) - f(q) = (v+b) - (q+b) = v - q$ is a quadratic residue so f preserves adjacency. Furthermore, f has the two-sided inverse $f(x) = x - b$ so f is an automorphism. Now suppose $f(x) = ax$ where a is a quadratic residue. Then $v \sim q \iff f(v) \sim f(q)$ since the product of two quadratic residues is a quadratic residue and the product of a quadratic residue with a non-residue is a non-residue. Furthermore, f has a two-sided inverse since $\mathbb{F}_q$ is a field so a has a multiplicative inverse. Thus, f is an automorphism. Finally, let $f(x) = x^\sigma$ where σ is a field automorphism. Since $\sigma(k^2) = \sigma^2(k)$, f sends quadratic residues to quadratic residues and quadratic non-residues to non-residues. Thus, f is an automorphism. Since the composition of automorphisms is an automorphism, $Aut(P_q)$ contains A. □

Lemma 4.6. *The blocks of imprimitivity of a transitive group have the same size.*

Proof. Suppose we have two blocks $\{x_1, \ldots x_m\}$ and $\{y_1, \ldots y_n\}$ of different size. Since the group acting on this set is transitive, there is a permutation sending x_1 to y_1. Since these are blocks in a system of imprimitivity, the permutation must send $\{x_1, \ldots x_m\}$ to $\{y_1, \ldots y_n\}$, but this is impossible since these blocks have different sizes. Therefore, all blocks must have the same size. □

Turning back to the proof that $P(q)$ is VPAT, suppose we have two vertices x and y. Then the automorphism f(v) = v +(y-x) sends x to y so P_q is transitive. Similarly, if we have two different arcs (x_1, x_2) and (y_1, y_2) , Then we want a and b such that a is a quadratic residue, $y_1 = ax_1 + b$, and $y_2 = ax_2 + b$. This is equivalent to

$$\begin{bmatrix} x_1 & 1 \\ x_2 & 1 \end{bmatrix} \begin{bmatrix} a \\ b \end{bmatrix} = \begin{bmatrix} y_1 \\ y_2 \end{bmatrix}$$

Since $x_1 \neq x_2$, the leftmost matrix is invertible, so we can solve for a and b. Furthermore, a= $\frac{y_1 - y_2}{x_1 - x_2}$ which is the quotient of two quadratic residues, so a is a quadratic residue. Therefore, P_q is arc-transitive.

Now, consider a non-trivial partition. If there is at least one singleton block, then all the blocks must be singletons by Lemma 4.6. Therefore, we assume that all blocks in the partition have at least 2 elements. Let K be the block containing 0. Then there is some non-zero element p in K. Suppose some element ap $(a \in (F_q^x)^2)$ is not in K. Then the automorphism $x \mapsto ax$ sends 0 to 0 but sends p to an element outside of K, and the partition is not preserved. Therefore, K contains 0 as well as elements of the form ap, so $|K| \geq \frac{q+1}{2}$. But as we showed in Lemma 4.6, all blocks in a system of imprimitivity must have the same size. This leads to a contradiction because if we had 2 blocks of size $\frac{q+1}{2}$, then this would already yield q+1 elements. Therefore, no system of imprimitivity exists, so P_q is vertex-primitive. □

We now generalize our definition of Paley Graphs:

Definition 4.7. Given a prime power q and an integer $r \geq 2$, we define the *rth residue Paley Graph* $P(q, r)$ to have vertex set F_q and require that $x \sim y$ if $x - y$ is an rth power in F_q.

4.2. **Kneser and Johnson Graphs.**

Definition 4.8. Consider a graph whose vertex set consists of all $s-$subsets of $[r]$, where two vertices are adjacent if the corresponding $s-$subsets are disjoint. The resulting graph is known as the *Kneser Graph* $Kn(r, s)$.

Remark 4.9. A simple counting argument reveals that $Kn(r, s)$ is $\binom{r-s}{s}-$regular. We also notice that $Kn(5, 2)$ is the Petersen Graph.

Proposition 4.10. *The graph* $Kn(r, s)$ *is VPAT.*

Proof. The statement is trivially true if $s \geq \frac{r}{2}$, so we assume $2s < r$. In this case, we first notice that the automorphism group of $Kn(r, s)$ is S_r^s, and by the proof in Example 2.24 we know this group acts primitively on s-subsets of $[r]$. Therefore, $Kn(r, s)$ is vertex-primitive.

Now, let $(A_1, A_2), (B_1, B_2)$ be two arcs. Once again arrange the elements of A_j and B_j so $a_{jk} = b_{jl} \implies k = l$. Then $(a_{11}b_{11}) \dots (a_{1s}b_{1s})(a_{21}b_{21}) \dots (a_{2s}b_{2s})$ is an automorphism sending A_1 to B_1 and A_2 to B_2 so Kn is arc-transitive. □

Definition 4.11. For $r \geq 2s$, we once again construct a graph whose vertex set consists of s-subsets of $[r]$, but we now define two vertices to be adjacent if their corresponding s-subsets have intersection of size s-1. The resulting graph is known as the *Johnson Graph* $J(r, s)$. Based on the relationship between this construction and the construction of the Kneser Graph, these two graphs have the same automorphism group. Furthermore, $Kn(r, s)$ is the complement of $J(r, s)$ when $s = 2$.

Proposition 4.12. *The Johnson Graph $J(r, s)$ is distance-transitive.*

Proof. Before we can prove the proposition we need the following lemma:

Lemma 4.13. *Let u and v be vertices of J(r,s). Then d(u,v) = m iff $|u \cap v| = s - m$.*

Proof. We will show this by induction. The base case m=1 follows by the definition of J(r,s). Now assume d(u,v) $= k \leq m - 1$ iff $|u \cap v| = s - k$.

Suppose d(u,v)=m. Take a vertex w such that d(u,w)= m-1 but d(w,v)=1. Then we must have $|u \cap w| = s - (m - 1)$ and $|w \cap v| = s - 1$. Then we must have $u = \{a_1, \dots, a_{s-(m-1)}, b_1, \dots, b_{m-1}\}$ and $w = \{a_1, \dots, a_{s-(m-1)}, c_1, \dots, c_{m-1}\}$ from our induction hypothesis. There are 4 cases for v:

(1) v= $\{a_1, \dots, a_{s-(m-1)}, c_1, \dots, c_{m-2}, b_j\}$
(2) v= $\{a_1, \dots, a_{s-(m-1)}, c_1, \dots, c_{m-2}, k\}$
(3) v= $\{a_1, \dots, a_{s-m}, c_1, \dots, c_{m-1}, b_j\}$
(4) v= $\{a_1, \dots, a_{s-m}, c_1, \dots, c_{m-1}, k\}$

Case 1 is not possible since it implies d(u,v) = m-2 from the induction hypothesis and $|u \cap v| = s - m + 2$. Cases 2 and 3 are not possible since they imply d(u,v)= m-1 from the induction hypothesis and $|u \cap v| = s - m + 1$. Therefore, we must have Case 4, with $|u \cap v| = s - m$.

Now suppose $|u \cap v| = s - m$. Then $u = \{a_1, \dots, a_{s-m}, b_1, \dots, b_m\}$ and $v = \{a_1, \dots, a_{s-m}, c_1, \dots, c_m\}$. Let $w = \{a_1, \dots, a_{s-(m-1)}, c_1, \dots, c_m, k\}$. Then d(u, w) = m-1 and d(w, v) = 1 by induction, so there exists a path from u to v of length m. If $d(u, v) \leq m - 1$, we would have $|u \cap v| \geq s - (m - 1)$ which is a contradiction, so we must have d(u,v)=m. □

Now, we notice $S_r^s \leqslant Aut(J(r, s))$, and S_r^s takes (s-m)-subsets to (s-m)-subsets. If we combine this with the previous lemma, we conclude that the action of S_r^s gives an injection from the collection of pairs of vertices at distance m into itself. Since this collection is finite, the map is a bijection. Thus, if we let (u,v) and (u', v') be two pairs of vertices with distance m, there is some $\sigma \in S_r^s \leqslant Aut(J(r, s))$ taking (u,v) to (u', v'), so J(r,s) is distance-transitive. □

In this subsection, we have shown symmetry properties that the Kneser and Johnson Graphs do satisfy, but we end the subsection by proving that the Kneser Graphs often do not satisfy the property of distance-transitivity.

Proposition 4.14. *The graph $Kn(r, s)$ is distance-transitive if and only if $s \leq 2$ or $s \geq \frac{r-1}{2}$.*

Proof. We first prove the reverse direction by verifying that the specified parameters result in distance-transitive graphs. The case $s = 1$ results in a complete graph, which is trivially distance-transitive. If $s > \frac{r}{2}$, the resulting graph is empty so it is also trivially distance transitive. From the previous proposition, we know $J(r, 2)$ is distance-transitive, so $Kn(r, 2)$ is distance-transitive since it is the complement of the corresponding Johnson Graph. If $s = \frac{r}{2}$, the resulting graph is distance-transitive since it is a disjoint union of $\frac{r}{2}$ copies of K_2.

In light of the previous paragraph, the only non-trivial case to verify is when $s = \frac{r-1}{2}$. Therefore, it suffices to show that $Kn(2s-1, s-1)$ is distance-transitive. Given that the automorphism group of $Kn(r, s)$ is S_r^s, we immediately have the following lemma:

Lemma 4.15. *$Aut(Kn(r, s))$ preserves the intersection sizes of the s-subsets when $1 \leq s < \frac{r}{2}$.*

Given this above lemma, we will have proved that $Kn(2s-1, s-1)$ is distance-transitive once we establish the following lemma:

Lemma 4.16. *Let u, v be vertices in $Kn(2s-1, s-1)$. Then the following relationship holds:*

$$d(u,v) = \begin{cases} 2m & \iff |u \cap v| = (s-1) - m \\ 2m+1 & \iff |u \cap v| = m \end{cases}$$

Proof. We split into two cases and prove each case by induction.

(1) Case 1: Assume $d(u, v)$ is even, so $d(u, v) = 2m$.

Base Case: In the case $m = 0$, we have $d(u, v) = 0$ iff $u = v$ iff $|u \cap v| = s - 1$.

Suppose $d(u, v) = 2k \iff |u \cap v| = (s-1) - k$ for all $k < m$. If $d(u, v) = 2m$ $(m > 1)$, we can select w such that $d(u, w) = 2(m-1)$ and $d(v, w) = 2$.

By induction, we know $|u \cap w| = (s-1) - (m-1)$ and $|v \cap w| = (s-1) - 1$. In particular, w has one element different from w. For convenience, we set $k = (s-1) - (m-1)$, and write $u = \{x_1, \ldots, x_k, u_{k+1}, \ldots, u_{s-1}\}$ and $w = \{x_1, \ldots, x_k, w_{k+1}, \ldots, w_{s-1}\}$. We may enumerate the four possibilities for the structure of v :

(a) $v = \{x_1, \ldots, x_k, w_{k+1}, \ldots, w_{s-2}, u_i\}$. In this case, $|u \cap v| = |u \cap w| + 1$.
(b) $v = \{x_1, \ldots, x_k, w_{k+1}, \ldots, w_{s-2}, y\}$ for $y \in \omega - (u \cup w)$. In this case, $|u \cap v| = |u \cap w|$.
(c) $v = \{x_1, \ldots, x_{k-1}, u_j, w_{k+1}, \ldots, w_{s-1}\}$. In this case, $|u \cap v| = |u \cap w|$.
(d) $v = \{x_1, \ldots, x_{k-1}, y, w_{k+1}, \ldots, w_{s-1}\}$ for $y \in \omega - (u \cup w)$. In this case, $|u \cap v| = |u \cap w| - 1$.

By the induction hypothesis, the first case would imply $d(u, v) = 2(m-2)$ and the next two cases would imply $d(u, v) = 2(m-1)$. These are all contradictions, so we are left with the fourth case, and we conclude $|u \cap v| = (s-1) - m$.

Conversely, suppose $|u \cap v| = (s-1) - m$. Let w be equal to v except for the last element, which is an element from u. In this case, $|u \cap w| = (s-1) - (m-1)$ and $|v \cap w| = (s-1) - 1$. By induction, $d(v, w) = 2$ and $d(u, w) = 2(m-1)$. Therefore, there exists a path of length $2m$ from u to v.

If $d(u,v) < 2m$, then by induction we would have $|u \cap v| \geq (s-1)-(m-1)$, which is a contradiction, so $d(u,v) = 2m$.

(2) Case 2: Assume $d(u,v)$ is odd, so $d(u,v) = 2m+1$.

Base Case: If $m = 0$, then $d(u,v) = 1$ iff u is adjacent to v iff $|u \cap v| = 0$.

Assume $d(u,v) = 2k+1$ iff $|u \cap v| = k$ for all $k < m$. If $d(u,v) = 2m+1$, we can select w such that $d(u,w) = 2(m-1)+1$ and $d(v,w) = 2$. By the induction hypothesis and the first case we conclude that $|u \cap w| = m-1$ and $|v \cap w| = (s-1)-1$. We can therefore use the same reasoning as the first case to conclude that v has the same four possibilities for its structure.

The fourth case would imply $d(u,v) = 2(m-2)+1$ and the middle two cases would imply $d(u,v) = 2(m-1)+1$. These are all contradictions, so we are left with the first case, where $|u \cap v| = m$.

Conversely, suppose $|u \cap v| = m$. This implies that there are elements $y_1, \ldots, y_m \in \Omega - (u \cup v)$. If we write $u = \{x_1, \ldots, x_m, u_{m+1}, \ldots, u_{s-1}\}$ and $v = \{x_1, \ldots, x_m, v_{m+1}, \ldots, v_{s-1}\}$, then set $w = \{u_{m+1}, \ldots, u_{s-1}, y_1, \ldots, y_m\}$, so $|w \cap v| = 0$ and $|u \cap w| = (s-1)-m$. By the previous case, this means $d(w,v) = 1$ and $d(u,w) = 2m$, so there exists a path of length $2m$ from u to v. If $d(u,v) < 2m+1$, then by induction we would have $|u \cap v| < m$ which is a contradiction, so we conclude $d(u,v) = 2m+1$. This concludes the proof of the lemma.

□

By the previous two lemmas, we can apply the same reasoning as the proof with the Johnson Graph to conclude $Kn(2s-1, s-1)$ is distance-transitive. We have thus established the reverse direction of Proposition 4.13.

For the forward direction, consider $Kn(r,s)$ where $2 < s \leq \frac{r}{2} - 1$. In this case, we know that $[r]$ contains $\{1, \ldots, 2s+2\}$. Without loss of generality, fix some vertex $u = \{1, \ldots, s\}$. This vertex is adjacent to $v_1 = \{s+1, \ldots, 2s\}$ and $v_2 = \{s+1, \ldots, 2s-1, 2s+1\}$. Since v_1 is adjacent to $t_1 = \{1, \ldots, s-1, 2s+1\}$ and v_2 is adjacent to $t_2 = \{1, \ldots, s-2, 2s, 2s+2\}$, both t_1 and t_2 are distance 2 from u. However, each of these vertices have different intersection size with u, so by Lemma 4.14 there is no automorphism that can take t_1 to t_2, so $Kn(r,s)$ is not distance-transitive. □

4.3. **Hamming Graphs.**

Definition 4.17. Consider a graph whose vertices are all ordered $k-$tuples of Z_n, where two vertices are adjacent if the corresponding $k-$tuples differ in exactly one coordinate. The corresponding graph is known as the *Hamming Graph $H(n,k)$*.

Remark 4.18. It's easy to see that letting S_n act on each of the coordinates is an automorphism, as is permuting the coordinates themselves. Therefore, S_n Wr $S_k \leqslant Aut(H(n,k))$ where Wr denotes the wreath product $(S_n \times \cdots \times S_n) \rtimes S_k$, with k copies of S_n. We also notice that $H(n,k)$ is $k(n-1)-$regular.

Proposition 4.19. *The graph $H(n,k)$ is Distance-Transitive*

Proof. This is immediate from the previous remark and the observation that two vertices are at distance d if they differ in exactly d coordinates. □

Lemma 4.20. *Hamming Graph H(n,k) is primitive iff $k \neq 2$.*

Proof. Let k=2. Define blocks B_0 and B_1 to be tuples whose coordinates sum to 0 or 1 mod 2 respectively. The action of S_2 on any coordinate either maps the blocks to themselves or switches them. Furthermore, switching coordinates clearly preserves the sum mod 2. Therefore, B_0 and B_1 form a system of imprimitivity, and $H(n, 2)$ is not primitive.

Now suppose $k > 2$. Consider the block B containing $(0, \dots, 0)$. If B only contains $(0, \dots, 0)$, then the system of imprimitivity is trivial. Assume there is some non-zero tuple v_n in B. Let $v_n = (a_1, a_2, \dots, a_n)$. Since permuting the coordinates of an n-tuple sends $(0, \dots, 0)$ to itself, B contains all permutations of the coordinates of v_n, so we may assume there exists $j \geq 2$ such that $a_i \neq 0$for all $i < j$ and $a_i = 0$ for $i \geq j$.

Consider the tuple $(k, 0, \dots, 0)$ $(k \neq 0)$. If $k \neq a_i$ for all i, the action of (0 k) on the first coordinate of all elements of B sends $(0, \dots, 0)$ to $(k, 0, \dots, 0)$ and v_n to itself, so B must contain $(k, 0, \dots, 0)$. Now assume $k = a_m$ for some m. Consider the action of (0 a_1 k) on the first coordinate of elements of B along with the action of (a_j 0) on the jth coordinate of elements of B for $j \geq 2$. This sends $(0, \dots, 0)$ to v_n and v_n to $(k, 0, \dots, 0)$, so B must contain $(k, 0, \dots, 0)$. Since B contains all permutations of the coordinates of its elements, it must contain all n-tuples with exactly 1 non-zero coordinate.

We show by induction that B contains all n-tuples such that the first k coordinates are non-zero, for $1 \leq k \leq n$. The above paragraph shows the base case of k=1. Assume the statement is true for $1 \leq k \leq n-1$. Consider an n-tuple $(k_1, \dots, k_n)$ where all coordinates are non-zero. We know that B contains $(k_1, \dots, k_{n-1}, 0)$. Now, the action of (0 k_n) on the last coordinate of all elements of B sends $(k_1, \dots, k_{n-1}, 0)$ to $(k_1, \dots, k_{n-1}, k_n)$ and $(0, \dots, 0, 0)$ to $(0, \dots, 0, k_n)$, but by the previous paragraph we know B contains $(0, \dots, 0, k_n)$. Therefore, B contains $(k_1, \dots, k_n)$.

By permuting the coordinates, we conclude that B contains all non-zero n-tuples, so it contains all vertices of H(n,k). Therefore, H(n,k) is primitive. □

5. Cayley Digraphs

So far in this paper, we have been presented with graphs and proved results about their automorphism groups. This section operates in the reverse direction as we study Cayley digraphs, which allow us to construct graphs from a given group. Given a group G and some set $S \subset G$ of generators, we define a vertex set V to be G, and say that there is an edge from g_1 to g_2 if there exists $s \in G$ such that $g_2 = s \cdot g_1$. The resulting directed graph is called a *Cayley digraph* $\vec{\Gamma}(G, S)$, and the special case where $S = S^{-1}$ yields the *Cayley graph* $\Gamma(G, S)$.

5.1. Results on Cayley Digraphs.

Lemma 5.1. *A digraph X is Cayley if and only if $G_R \leqslant Aut(X)$.*

Proof. Let X=Cay(G,S) be a Cayley digraph. Consider $\sigma_g \in G_L$ so $\sigma_g : x \mapsto x \cdot g$. If there is an edge from x to y, then $\exists s \in S$ such that $y = s \cdot x$. Since $y \cdot g = s \cdot x \cdot g = s \cdot (x \cdot g)$, there is an edge from $\sigma_g(x)$ to $\sigma_g(y)$, and $G_R \leqslant Aut(X)$. Now let X be a digraph with vertex set G such that $G_R \leqslant Aut(X)$. Associate the elements of S with the vertices that have an edge from the vertex corresponding to 1. Suppose there's an edge from x to y. Since $\sigma_{x^{-1}}$ is an automorphism of X, there is an edge from 1 to $y \cdot x^{-1}$, so $y \cdot x^{-1} \in S$. Letting $s = y \cdot x^{-1}$, we have $y = s \cdot x$, so X is a Cayley digraph. □

Corollary 5.2. *Cayley digraphs are vertex-transitive.*

Proof. We conclude that G_R is regular by Lemma 2.41, and transitivity follows from the definition of regular permutation groups. □

Lemma 5.3. *A Cayley digraph $\Gamma(G, S)$ is weakly connected if and only if S generates G.*

Proof. Suppose S generates G, so any element of G can be written as a finite product of elements of S. Let x and y be two vertices. Since $y = x(x^{-1}y)$ and $x^{-1}y$ can be written as a finite product of elements of S, there is a path from x to y so $Cay(G, S)$ is connected.

Now suppose Cay(G,S) is connected. Since there is a path from 1 to g for any $g \in G$, g is a finite product of elements of S, so S generates G. □

Definition 5.4. A digraph is *Eulerian* if the indegree and outdegree are the same for each vertex.

Lemma 5.5. *If a finite Eulerian digraph G is weakly connected then it is strongly connected.*

Proof. Let A and B be two strongly connected components of G. Since G is weakly connected, there must be an edge extending from A to B. We will label this edge a_1b_1, for $a_1 \in A$ and $b_1 \in B$. Since G is finite, A has $m > 0$ internal edges. Each of these edges gets included in the sum of the total indegree across all vertices of A since each internal edge extends from one vertex of A to another. Conversely, every edge included in the sum of the total indegree of A must be an internal edge since there are no edges extending from B to A. Therefore, the total indegree of A is m. Each internal edge is also included in the sum of the total outdegree of A, but there is also at least one edge extending from A to B, so the total outdegree of A would be at least $m + 1$, which contradicts the Eulerian property of G. Therefore, there must be an edge extending from B to A, which we label b_2a_2 for $a_2 \in A$, $b_2 \in B$.

We may now take any $u \in A$ and $v \in B$. Since A is strongly connected, there is are paths $u \dots a_1$ and $a_2 \dots u$. Furthermore, B is strongly connected so there are paths $b_1 \dots v$ and $v \dots b_2$. Therefore, we obtain a path from u to v given by $u \dots a_1b_1 \dots v$ and a path from v to u given by $v \dots b_2a_2 \dots u$. This allows us to conclude that A and B are the same strongly connected component so G is strongly connected. □

Lemma 5.6. *If G is finite and S generates G then $\Gamma(G, S)$ is strongly connected.*

Proof. If S generates G, then $\Gamma(G, S)$ is weakly connected if we consider the underlying undirected graph. Now, by definition the indegree and outdegree of every vertex is $|S|$, so $\Gamma(G, S)$ is Eulerian and we may apply the previous lemma to conclude that it is strongly connected.

□

We now observe that the Payley Graph P_p is Cayley with vertex set $\mathbb{F}_p$ and connection set $(\mathbb{F}_p^\times)^2$, which allows us to compute the automorphism group of P_p

Proposition 5.7. *The automorphism group of P_p consists of all affine semilinear transformations $x \mapsto ax^\sigma + b$ where $a, b \in F_p$, a is a non-zero square, and σ is an automorphism of $\mathbb{F}_p$.*

Proof. If we let A $= \{ax^\sigma + b : a \in (\mathbb{F}_p^\times)^2, b \in \mathbb{F}_p, \sigma \in Aut(\mathbb{F}_p)\}$, we have shown that A is an index-2 subgroup of the affine semillinear group $\Gamma A(1, p)$, and $A \leqslant Aut(P_p)$. By Theorem 2.45, since P_p is not empty or complete, $Aut(P_p)$ is solvable. Let N be a minimal normal subgroup of $Aut(P_p)$. Since $Aut(P_p)$ is primitive, N is transitive, and since $Aut(P_p)$ is solvable, N is Abelian. Therefore, N is regular, and we can associate the elements of N with the vertices of P_p. If k is a quadratic non-residue and $\sigma : x \mapsto x^{-1}$ $(x \in N)$, σ is an anti automorphism of P_p. Therefore, H=$< Aut(P_p), \sigma >$ is solvable and doubly-transitive with $Aut(P_p)$ as an index-2 subgroup. Furthermore, H must be isomorphic to a subgroup of the affine semillinear group, and so must $Aut(P_p)$. This means that we must have $|Aut(P_p)| = |A|$ so $Aut(P_p) \cong A$. □

We now generalize our definition of Paley Graphs:

Definition 5.8. Given a prime power q and an integer $r \geq 2$, we define the *rth residue Paley Graph* $P(q, r)$ to have vertex set F_q and require that $x \sim y$ if $x - y$ is an rth power in $\mathbb{F}_q$.

We first notice that rth residue Paley Graphs are Cayley for certain values of r :

Proposition 5.9. *If r is an integer such that $r|\frac{p-1}{2}$, then $P(r, p)$ is an arc-transitive Cayley Graph over $\mathbb{Z}_p$. with degree $d = \frac{p-1}{r}$.*

Proof. This graph is arc-transitive due to analogous reasoning that showed P_p was arc-transitive. It is Cayley since its connection set is $(\mathbb{F}_p^\times)^r$, and its degree follows from the fact that there are $\frac{p-1}{r}$ rth powers in $\mathbb{Z}_p$. □

In fact, the rth residue Paley Graphs play an important role in the classification of arc-transitive Cayley Graphs over $\mathbb{Z}_p$:

Proposition 5.10. *If X is an arc-transitive Cayley Graph with odd prime order, then X is either complete, empty, or it is an rth residue Paley Graph for $r|\frac{p-1}{2}$.*

Proof. X must be vertex-transitive because otherwise it would be bipartite, but the order p is odd. Now, if we let $G = Aut(X)$, then by Theorem 2.45 G is either doubly-transitive or solvable. If G were doubly transitive, then X would be complete or empty. If G is solvable, then $G \leqslant A(1, p)$. To complete the proof, we now investigate the structure of $A(1, p)$:

Lemma 5.11. *Fix $k \in \mathbb{Z}_p$. The stabilizer of k under the action of $A(1, p)$ if isomorphic to $GL(1, p) \cong (\mathbb{Z}_p)^\times$.*

Proof. Consider the map ϕ from $(\mathbb{Z}_p)^\times$ to $A(1,p)_k$ where ϕ sends $a \in (\mathbb{Z}_p)^\times$ to the map $x \mapsto ax + (k - ak)$ in $A(1,p)_k$. This map is clearly a bijection because it has the two-sided inverse $\phi^{-1} : A(1,p)_k \to (\mathbb{Z}_p)^\times$ where ϕ^{-1} sends the map $x \mapsto ax + b$ to $a \in (\mathbb{Z}_p)^\times$. Now, ϕ sends $1 \in (\mathbb{Z}_p)^\times$ to the identity map, so it preserves the identity element.

If $a, c \in (\mathbb{Z}_p)^\times$ then $\phi(ab)$ is the map $x \to (ab)x + (k - (ab)k)$. Furthermore, the image of $x \in \mathbb{Z}_p$ under $phi(a)\phi(b)$ is the following:

$$a(bx+(k-bk))+(k-a(bk+(k-bk))) = (ab)x+a(k-bk)+k-(ab)k-a(k-bk) = (ab)x+(k-(ab)k)$$

This allows us to conclude that ϕ is an isomorphism. □

We now give a necessary condition for transitive subgroups of $A(1,p)$.

Lemma 5.12. *If H is a transitive subgroup of $A(1,p)$, then H contains all translations $x \mapsto x + b$.*

Proof. Let H be a transitive subgroup of $A(1,p)$. By the Orbit-Stabilizer Theorem, if we fix $x \in \mathbb{Z}_p$, then $|A(1,p)_x| = \frac{|H|}{p}$. By the previous lemma $A(1,p)_x$ is a subgroup of $GL(1,p)$ so $|A(1,p)_x| = \frac{(p-1)}{r}$ for some $r|p-1$. Therefore, $|H| = \frac{p(p-1)}{r}$.

By Sylow's Theorem, H has a Sylow p-subgroup. Now, we know that the group of translations is a Sylow p-subgroup of $A(1,p)$, and we will show now that this is the only Sylow p-subgroup of $A(1,p)$ as this would imply that the group of translations is contained in H:

If N is the number of Sylow p-subgroups in $A(1,p)$, then by Sylow's Theorem we know $N \equiv 1 \bmod p$ and N also divides the index of the subgroup in $A(1,p)$, which is $p-1$. Therefore, N must be 1, so the Sylow p-subgroup inside of H is the group of translations. □

We now return to the proof of Proposition 5.10. By the previous two lemmas, G contains all translations, and the stabilizer under the action of G is isomorphic to a subgroup of $(\mathbb{Z}_p)^\times$. Let A denote the possible values of a in the elements $x \mapsto ax+b$ in G. Since G contains all translations, there is a one-to-one correspondence between elements of A and elements of the stabilizer under the action of G, and the same isomorphism in Lemma 5.11 gives an isomorphism from A to $A(1,p)_k$. This implies that A is a subgroup of $(\mathbb{Z}_p)^\times$, so all elements of A are rth powers for some $r|p-1$. Since X is an undirected graph, $\frac{p-1}{r}$ must be even so $r|\frac{p-1}{2}$. □

5.2. **Circulant Digraphs.**

Definition 5.13. Given some orderd $n-$tuple $(a_0, \ldots, a_{n-1})$ of complex numbers, we say a matrix is *circulant* if it is of the form:

$$\begin{bmatrix} a_0 & a_1 & \ldots & a_{n-1} \\ a_{n-1} & a_0 & \ldots & a_{n-2} \\ \vdots & \vdots & \ldots & \vdots \\ a_1 & a_2 & \ldots & a_0 \end{bmatrix}$$

And a digraph whose adjacency matrix is circulant is called a *circulant digraph.*

Theorem 5.14. *Let M be an $n \times n$ circulant matrix and ω be the primitive nth root of unity. Then M has an eigenbasis given by $(1, \omega^j \dots, \omega^{(n-1)j})$ and the corresponding eigenvalues are $a_0 + a_1\omega^j + \dots + a_{n-1}\omega^{(n-1)j}$ for $0 \le j \le n-1$.*

Proof. We first verify that

$$\begin{bmatrix} a_0 & a_1 & \dots & a_{n-1} \\ a_{n-1} & a_0 & \dots & a_{n-2} \\ \vdots & \vdots & \dots & \vdots \\ a_1 & a_2 & \dots & a_0 \end{bmatrix} \begin{bmatrix} 1 \\ \omega^j \\ \vdots \\ \omega^{(n-1)j} \end{bmatrix} = \begin{bmatrix} a_0 + a_1\omega^j + \dots + a_{n-1}\omega^{(n-1)j} \\ a_{n-1} + a_0\omega^j + a_1\omega^{2j} + \dots + a_{n-2}\omega^{(n-1)j} \\ \vdots \\ a_1 + a_2\omega^j + \dots + a_0\omega^{(n-1)j} \end{bmatrix}$$

$$= (a_0 + a_1\omega^j + \dots + a_{n-1}\omega^{(n-1)j}) \begin{bmatrix} 1 \\ \omega^j \\ \vdots \\ \omega^{(n-1)j} \end{bmatrix}$$

for $0 \le j \le n-1$, and this gives us n eigenvalues. Since these eigenvalues are distinct, the corresponding eigenvectors are linearly independent, so they form a basis for $\mathbb{C}^n$. □

As we show below, circulant digraphs are a subclass of Cayley digraphs:

Lemma 5.15. *Let $\Gamma(G, S)$ be a Cayley digraph where $G = \mathbb{Z}/n\mathbb{Z}$. Then $\Gamma(G, S)$ is a circulant digraph.*

Proof. Given that the vertices of $\Gamma(G, S)$ correspond to $\{0, \dots, n-1\}$ and $i \sim j$ if and only if $j - i \in S$, the adjacency matrix for $\Gamma(G, S)$ has a 1 in row i and columns $x + i$ for all $x \in S$. Therefore, $\Gamma(G, S)$ has a circulant adjacency matrix. □

Lemma 5.16. *Let G be a circulant digraph with n vertices. Then there exists a subset $S \subset \mathbb{Z}/n\mathbb{Z}$ such that $G = \Gamma(\mathbb{Z}/n\mathbb{Z}, S)$.*

Proof. Given the adjacency matrix $A = (a_{ij})$ for G, let $S = \{j : a_{ij} = 1\}$. Then $\Gamma(\mathbb{Z}/n\mathbb{Z}, S)$ is isomorphic to G. □

We now give sufficient conditions for two Cayley Graphs to be isomorphic:

Proposition 5.17. *Let $\Gamma_1 = \Gamma(\mathbb{Z}/n\mathbb{Z}, S)$ and $\Gamma_2 = \Gamma(\mathbb{Z}/n\mathbb{Z}, bS)$ where $gcd(b, n) = 1$. Then Γ_1 and Γ_2 are isomorphic.*

Proof. Since $gcd(b, n) = 1$, $\phi : \mathbb{Z}/n\mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$ where $\phi(x) = bx$ is an automorphism of $\mathbb{Z}/n\mathbb{Z}$. This is a graph isomorphism since $x - y \in S \iff b(x - y) \in bS$. □

The following theorem of Elspas and Turner allows us to establish a converse to the previous proposition when n is a prime greater than 2.

Theorem 5.18 (Elspas and Turner [17])**.** *Let A and B be two circulant matrices with prime order $p > 2$ and rational entries. If A and B have the same eigenvalues then they are permutationally similar, so there exists a permutation matrix P such $P^{-1}AP = B$. Furthermore, P can be chosen to be the matrix $(\delta_{qi,j})$, where $\delta_{qi,j} = 1$ if $qi \equiv j$ mod n and 0 otherwise.*

Proof. Let $A = (a_{j-i})$, $B = (b_{j-i})$ be two circulant matrices. If $f_a(x) = \sum_i a_i x^i$ and $f_b(x) = \sum_i b_i x^i$, then the eigenvalues for A and B respectively are given by

$$\alpha_k = f_a(\omega^k)$$

$$\beta_k = f_b(\omega^k)$$

for $k = 0, \ldots, p-1$. Since A and B have the same eigenvalues, we know that $\alpha_1 = \beta_q$ for some $q = 0, \ldots, p-1$. We may assume $q > 0$ since we could replace ω with ω^k for any k such that $2 \leq k \leq p-1$ and this would not change the set of eigenvalues. If we set $F(x) = \sum_i a_i x^i - \sum_i b_i x^{qi \bmod p}$, then $\alpha_1 = \beta_q$ implies

$$F(\omega) = 0$$

so F is divisible by the minimum polynomial of ω over the rational numbers, which is cyclotomic. Since p is prime, this cyclotomic polynomial is given by

$$\phi_p = x^{p-1} + \cdots + x + 1$$

and this polynomial vanishes at ω^k for $k = 1, \ldots, p-1$. Therefore, we have $F(\omega^k) = 0$ for $k = 1, \ldots, p-1$. This implies

$$\alpha_k = \sum_i a_i \omega^{ki} = \sum_i b_i \omega^{kqi} = \beta_{kq}$$

for $k = 1, \ldots, p-1$. Since q is relatively prime to p, kq is a bijection from $Z_p^\times$ to itself. This means that we must have $\alpha_0 = \beta_0$, since β_k for non-zero k are already paired with α_j for non-zero j. To summarize our work so far, we have shown

$$\alpha_k = \beta_{kq}$$

for $k = 0, \ldots, p-1$. From theorem, we have

$$a_{qi} = \frac{1}{p} \sum_k \alpha_k \omega^{-kqi} = \frac{1}{p} \sum_k \beta_{qk} \omega^{-kqi} = \frac{1}{p} \sum_{s=0}^{p-1} \beta_s \omega^{-si} = b_i$$

This implies $B = P^{-1}AP$ where $P = (\delta_{qi,j})$. □

Corollary 5.19. *If Γ_1 and Γ_2 are isomorphic Cayley Graphs on $\mathbb{Z}/p\mathbb{Z}$ ($p > 2$) with generating sets S_1 and S_2, then there exists $b \in \mathbb{Z}/p\mathbb{Z}^\times$ such that $S_1 = bS_2$.*

Proof. Since Γ_1 and Γ_2 are isomorphic, their adjacency matrices are circulant, and they have the same eigenvalues. By the previous theorem, these adjacency matrices are permutationally equivalent according to $P = (\delta_{qi,j})$, which implies that $S_1 = qS_2$ where $q \in \mathbb{Z}/p\mathbb{Z}^\times$. □

6. Vertex-Transitive Graphs

In this section, we illustrate the relationship between vertex-transitivity and combinatorial parameters such as connectivity, independence number, chromatic number, and cycle length. The main result of the first subsection is roughly that vertex-transitive graphs have high connectivity. This motivates the main results of the following subsections, which are roughly that the product of independence and chromatic number in vertex-transitive graphs satisfy a nearly-tight linear bound, and connected vertex-transitive graphs contain long cycles.

6.1. **Vertex Connectivity.**

Definition 6.1. Let X be an undirected graph. The *vertex-connectivity* of X (denoted $\kappa(X)$) is the minimum number of vertices that must be removed to guarantee that X is disconnected or has one vertex. We say X is *k-connected* if its vertex-connectivity is at least k.

Definition 6.2. Let X be an undirected graph and A be a subset of its vertices. Define $N(A)$ to be all vertices in $V \backslash A$ that are adjacent to some vertex in A. Define $\overline{A} = (A \cup N(A))^C$, so $A, N(A)$, and $\overline{A}$ partition V.

Definition 6.3. A *fragment* is a subset $A \subset V$ such that $\overline{A} \neq \emptyset$ and $|N(A)| = \kappa(X)$.

Definition 6.4. An *atom* is a fragment with the minimum number of vertices.

The following theorem is a result of Mader and Watkins, and it will allow us to prove an auxiliary result that will allow us to lower-bound the vertex-connectivity of vertex-transitive graphs:

Theorem 6.5 (Mader and Watkins [22], [23], [28])**.** *Let X have connectivity κ. Suppose A and B are fragments and $A \cap B \neq \emptyset$. If $|A| \leq |\overline{B}|$, then $A \cap B$ is a fragment.*

We use this to prove our auxiliary result:

Lemma 6.6. *If A is an atom and B is a fragment, then either $A \subset B$, $A \subset N(B)$, or $A \subset \overline{B}$.*

Remark 6.7. The above lemma shows in particular that distinct atoms are pairwise disjoint. Therefore, atoms for a system of imprimitivity under the action of $Aut(X)$ when X is vertex-transitive.

Proof. Since A is an atom, we know $|A| \leq |B|$ and $|A| \leq |\overline{B}|$. By the previous theorem, if $A \cap B$ or $A \cap \overline{B}$ are nonempty, then $A \cap B$ and $A \cap \overline{B}$ respectively will be fragments. Since A has minimum size, we must have $A \cap B = A$ or $A \cap \overline{B} = A$ respectively, which would show $A \subset B$ or $A \subset \overline{B}$. Now, if $A \cap B = \emptyset = A \cap \overline{B}$, then we must have $A \subset N(B)$ since $B, N(B)$, and $\overline{B}$ partition V. □

We are now poised to prove the following:

Theorem 6.8. *If X is vertex-transitive, then $\kappa(X) \geq \frac{2(d+1)}{3}$.*

Proof. Since X is regular, let it have degree d. Suppose A is an atom. If $|A| = 1$, then $|N(A)| = d = \kappa$ so the result would hold. Assumed $|A| \geq 2$.

If $\sigma \in Aut(X)$ then the translate of A under σ is also an atom, so either $A = A^\sigma$ or $A \cap A^\sigma = \emptyset$. Therefore, the translates of A under $Aut(X)$ form a system of imprimitivity for X so these translates form a partition of $N(A)$. Thus, we have

$$|N(A)| = k|A|$$

for some positive integer k. If we fix $u \in A$ then the degree of u is at most

$$(|A| - 1) + |N(A)| = (k+1)|A| - 1$$

Therefore, we have

$$d + 1 \leq (k+1)|A| \implies d + 1 \leq (k+1)\frac{|N(A)|}{k}$$

which allows us to conclude $\kappa = |N(A)| \geq \frac{k}{k+1}d$.

To conclude the proof, we show that $k \geq 2$: If $k = 1$ then $N(A)$ is an atom, so A and $N(A)$ are blocks under the action of $Aut(X)$. Since X is vertex transitive, there exists $\sigma \in X$ such that $\sigma(A) = N(A)$, so $\sigma(N(A)) = N(N(A))$. This implies that $|A| = |N(N(A))|$. However, $A \cap N(N(A)) \neq \emptyset$ so $A = N(N(A))$, which contradicts the fact that $\overline{A} \neq \emptyset$. Therefore, we must have $k \geq 2$. □

Corollary 6.9. *Vertex-transitive graphs are 2-connected.*

Proof. Vertex-transitive graphs are regular with degree at least 2 so we may apply the previous theorem. □

Furthermore, the bounds in the previous theorem are tight. If we consider the lexicographic product of the cycle graph C_m ($m \geq 4$) with K_3, we will have constructed an infinite family of vertex-transitive graphs such that $\kappa(X) = \lceil \frac{2d+1}{3} \rceil$.

6.2. **Independence Number and Chromatic Number.** We start with a simple lemma that is true for any graph:

Lemma 6.10. *If X is a graph with n vertices, then $\alpha(X).\chi(X) \geq n$.*

Proof. Let $\chi(X) = k$ and $\alpha(X) = \alpha$. Suppose we fix a proper k-coloring of X. Then we can partition the vertex set into $P_1, \ldots, P_k$ where each set contains vertices with the same color, so $\sum_{i=1}^{k} |P_i| = n$. Since each P_i is an independent set, $|P_i| \leq \alpha$. Thus, $n = \sum_{i=1}^{k} |P_i| \leq k\alpha$. □

If we impose vertex-transitivity on X, this bound becomes nearly-tight in the following sense:

Proposition 6.11 (Szegedy [4])**.** *Let X be a vertex-transitive graph with n vertices. Then*

$$\alpha(X).\chi(X) \leq (1 + \ln n)n$$

Proof. Let X be a vertex transitive graph with n vertices. Define our probability space to be $Aut(X)$ where the permutations have a uniform distribution. Let $\alpha(X) = k$, and take an independent set M of size k. If we fix $v \in X$ and $\sigma \in Aut(X)$, $P(v \in \sigma(M))= \sum_{i=1}^{k} P(\sigma(e_i) = v)$ where $e_1, \ldots e_k$ are the elements of M. Let $K = stab(e_i)$, and τ be a permutation sending e_i to v (which we know exists by vertex-transitivity). Then elements of τK send e_i to v. Furthermore, if $\mu(e_i) = v$, $\tau^{-1}\mu \in K$ so $\mu \in \tau K$. Therefore, the permutations sending e_i to v are precisely the elements of coset τK, and the cardinatlity of this coset is the cardinality of K.

Since the action of $Aut(X)$ is transitive we have $|orb(e_i)| = n$, so $|K| = \frac{|Aut(X)|}{n}$. Therefore, $P(\sigma(e_i) = v) = \frac{\frac{|Aut(X)|}{n}}{|Aut(X)|} = \frac{1}{n}$. This means that P($v \in \sigma(M)$)= $\frac{k}{n}$.

Suppose we randomly choose m automorphisms $\sigma_1, \ldots, \sigma_m$. Let D denote the event that the images of M under these automorphisms don't cover X. If V is the vertex set of X, then $P(D) \leq \sum_{v \in V} P(v \notin \bigcup_{i=1}^{m} \sigma_i(M))$. $P(v \notin \bigcup_{i=1}^{m} \sigma_i(M)) = \prod_{i=1}^{m} P(v \notin \sigma_i(M))$ since these events are independent, and $P(v \notin \sigma_i(M) = 1 - \frac{k}{n}$. Therefore, $P(D) \leq n(1 - \frac{k}{n})^m < ne^{\frac{-km}{n}}$ since $\frac{k}{n} > 0$.

If we choose $m = \lceil\frac{nln(n)}{k}\rceil$ then $P(D) < 1$, which implies that some choice of m automorphisms will produce images of M that will cover X. Since the image of an independent set under an automorphism is independent, each image is 1-colorable. We have m images, so X is m-colorable. This means that $\chi(X) \leq m = \lceil\frac{nln(n)}{k}\rceil < \frac{nln(n)}{k} + 1 \leq \frac{nln(n)}{k} + \frac{n}{k}$ since $k \leq n \implies \frac{n}{k} \geq 1$. Then $k * \chi(X) = \alpha(X) * \chi(X) < n(ln(n) + 1)$. □

We note however that this bound cannot apply to all graphs in general, because if we consider the disjoint union of the empty graph with n vertices with the complete graph with n vertices, we will obtain an infinite family of graphs such that $\chi(X) \cdot \alpha(X) = \Omega(n^2)$.

6.3. **Longest Cycles.**

To present our next main result on the existence of long cycles in connected vertex-transitive graphs, we need to make use of the following lemma:

Lemma 6.12 (Regular Hypergraph Counting Lemma)**.** *Let G_1 be a r-uniform regular hypergraph and G_2 be a s-uniform regular hypergraph, both of which have the same set of n vertices. Let $A_1, \ldots, A_k$ be the edges of G_1 and $B_1, \ldots, B_\ell$ be the edges of G_2.*

(1) If $|A_i \cap B_j| \leq d$ for all i and j, then $rs \leq nd$.
(2) If $|A_i \cap B_j| \geq d$ for all i and j, then $rs \geq nd$.

Proof. We will just prove (1) since the proof of (2) is analogous:

Fix A_i. We will count the number of pairs (x, j) such that $x \in A_i \cap B_j$. Denote this number by M.

A fixed vertex in A_i appears in $deg(G_2)$ edges of G_2, so M$= r \times deg(G_2)$. In addition, for a fixed j, there are at most d vertices in $A_i \cap B_j$, and each vertex appears in $deg(G_2)$ edges of G_2. Therefore, $M = r \times deg(G_2) \leq d \times deg(G_2) \leq d\ell$. Since G_2 is a s-uniform, regular hypergraph, we have $n \times deg(G_2) = s\ell$, so $\ell = \frac{n \times deg(G_2)}{s}$. Therefore, $r \times deg(G_2) \leq \frac{nd \times deg(G_2)}{s}$ so $rs \leq nd$. □

We are now set to give a lower bound on the length of the cycles of connected vertex-transitive graphs:

Theorem 6.13 (Babai [1])**.** *If X is a vertex-transitive graph with $n \geq 5$ vertices then X has a cycle of length $\ell \geq \sqrt{n}$.*

Proof. We start with the following lemma:

Lemma 6.14. *If X is a 2-connected graph then any two longest cycles share at least 1 vertex.*

Proof. Let $C_1 = u_1, \ldots u_n, u_1$ and $C_2 = v_1, \ldots, v_n, v_1$ be two longest cycles, and assume C_1 and C_2 are disjoint. Since X is 2-connected, there must exist 2 pairs of vertices (u_i, v_j), (u_k, v_m) such that $i \neq k$, $j \neq m$, and X contains 2 paths P_1, P_2 that are disjoint from themselves and the cycles that connect u_i to v_j, and v_m to u_k respectively. Indeed, if this were not true, then one could delete the vertex where the two paths intersect (either at the endpoint or internal node), and this would cause X to become disconnected, which contradicts the assumption that X is 2-connected. Without loss of generality, assume $i-k \geq \frac{n}{2}$ and $j-m \geq \frac{n}{2}$ (otherwise one can change the labelling). In this case, the cycle $C' = u_k u_{k+1} \dots u_i P_1 v_j v_{j-1} \dots v_m P_2 u_k$ is longer than n, which is a contradiction. Therefore, C_1 and C_2 must share at least 1 vertex. □

Corollary 6.15. *If X is vertex-transitive then any two longest cycles share at least 1 vertex.*

Proof. This is immediate from the previous lemma along with Corollary 6.9. □

Turning back to the proof of the proposition, we note that since X is vertex-transitive, it must be connected. If ℓ denotes the length of the longest cycle, consider the $\ell-$regular hypergraphs induced by any two longest cycles in X. By the previous lemma, the edges of these two hypergraphs intersect in at least 1 vertex, so $\ell^2 \geq n$ and $\ell \geq \sqrt{n}$ □

7. Universality

In this section, we introduce the concept of universality for graphs and prove some extremal results related to the existence of k-universal graphs. We conclude the section by relating the concept of universality to the Paley and Kneser Graphs.

7.1. General Universality Results.

Definition 7.1. A graph X is *k-universal* if every graph with k vertices is an induced subgraph of X.

Remark 7.2. We notice that we can trivially construct a $k-$universal graph with $k2^{\binom{k}{2}}$ vertices by taking the disjoint union of all $2^{\binom{k}{2}}$ graphs with k vertices, so $k-$universal graphs do indeed exist. The following Proposition guarantees the existence of smaller $k-$universal graphs:

Proposition 7.3. *There exist $k-$universal graphs of size $O(k^2 2^k)$.*

Proof. Define a graph to be $(k-1)$-unconstrained as follows: Let $f(x,y) = 1$ if $x \sim y$ and 0 if $x \not\sim y$. For any $M = \{v_1, \dots, v_{k-1}\} \subset V$ and $p_1, \dots, p_{k-1} \in \{0,1\}$, then X is (k-1)-unconstrained if there exists some $x \in V - M$ such that $f(x, v_i) = p_i$ for all i. Then a graph is j-unconstrained if it is m-unconstrained for any $m \leq j$. Also, we claim a $(k-1)$-unconstrained graph is k-universal. Indeed, given a graph S on k vertices, one can inductively construct a graph isomorphic to S as an induced subgraph of X: Assume a subgraph of S with k-1 vertices is an induced subgraph of X. Using the unconstrained property, one can find a kth vertex in X that has the same adjacencies as the kth vertex in S.

Consider all random graphs with n vertices. Having established the above property, let C denote the event that X is k-unconstrained. We claim that for large n, the probability that X is not k-unconstrained is less than 1. For a fixed $x \in V - M$, the probability that $f(x, v_i) \neq p_i$ for some i is $(1 - \frac{1}{2^k})$, so the probability that all $x \in V - M$ have this property is $(1 - \frac{1}{2^k})^{n-k}$. Since there are at most 2^k choices for the p_i and less than n^k choices for the v_i, the probability that X is not k-unconstrained is less than $2^k n^k (1 - \frac{1}{2^k})^{n-k} < 2^k n^k e^{-\frac{n-k}{2^k}}$. Therefore, we must have $n = O(k^2 2^k)$ to ensure that the righthand side is strictly less than 1. □

We can also establish lower bounds on the size of a $k-$universal graph:

Proposition 7.4. *If X is $k-$universal, then X has size $\Omega(2^{\frac{k}{2}})$.*

Proof. Let X have n vertices. Since there are $k!$ labellings for a graph, there are at least $\frac{2^{\frac{k(k-1)}{2}}}{k!}$ non-isomorphic graphs. Since distinct graphs correspond to distinct k-subsets of the vertices of X, $\frac{2^{\frac{k(k-1)}{2}}}{k!} \leq \binom{n}{k} \leq \frac{n^k}{k!}$, so $n \geq 2^{\frac{k-1}{2}}$. □

7.2. **Universal Paley Graphs.** Our next goal is to prove that Paley Graphs with large enough size are $k-$universal. To accomplish this, we need to introduce the concept of multiplicative characters:

Definition 7.5. A *multiplicative character* over a finite field $\mathbb{F}$ is a function $\chi : \mathbb{F} \to \mathbb{C}$ such that $\chi(0) = 0$ and χ is a group-homomorphism from $\mathbb{F}^\times$ to the multiplicative group of complex numbers.

A classic example of a multiplicative character is the Legendre symbol, which is the function $\chi : \mathbb{F}_p \to \mathbb{C}$ where

$$\chi(x) = \begin{cases} 1 & x \not\equiv 0 \text{ mod p and x is a quadratic residue mod p} \\ -1 & x \not\equiv 0 \text{ mod p and x is not a quadratic residue mod p} \\ 0 & x \equiv 0 \text{ mod p} \end{cases}$$

To prove the existence of $k-$universal Paley Graphs, we need the following theorem of Andre Weil, whose proof can be found in [24]:

Theorem 7.6 (Weil's Character Sum Estimate)**.** *Let χ be a multiplicative character of the field F_q. Assume χ has order k, so k is the smallest positive integer such that $\chi(a)^k = 1$ for all $a \in \mathbb{F}_q^\times$. Let $f \in \mathbb{F}_q[x]$ have degree d and assume for any $c \in \mathbb{F}_q$ and any $g \in \mathbb{F}_q[x]$ we have $f \neq cg^k$. Then*

$$\mid \sum_{x \in \mathbb{F}_q} \chi(f(x)) \mid \leq (d-1)\sqrt{q}$$

With this Theorem, we may prove the following proposition:

Proposition 7.7. *Paley Graphs of size $O(k^2 4^k)$ are $k-$universal.*

Proof. Suppose our Paley graph has q vertices. Take a (k-1)-subset of the vertices, and fix some partition of the vertices into two sets A and B. Let N denote the number of vertices in P that are adjacent to all the vertices in A and non-adjacent to all the vertices in B. If We can show that $N > 0$ then P is k-universal. For any vertex x, define $\phi(x) = \prod_{a_i \in A}(\chi(x - a_i) + 1) \prod_{b_i \in B}(-\chi(x - b_i) + 1)$. Then

$$\chi(x) = \begin{cases} 2^{k-1} & x \notin A \cup B, x \sim v \ \forall v \in A, x \not\sim v \ \forall v \in B \\ 0 & x \notin A \cup B, \exists v \text{ s.t. } x \not\sim v \in A, \text{ or } x \sim v \in B \\ 0 \text{ or } 2^{k-2} & x \in A \cup B \end{cases}$$

In the last case, 2^{k-2} occurs if x is adjacent to all vertices in A and non-adjacent to all vertices in B. Define S = $\sum_{x\in\mathbb{F}_q}\phi(x) = N2^{k-1} + \epsilon 2^{k-2}$ where $\epsilon = 0$ or 1. Then

$$\sum_{x\in\mathbb{F}_q}\phi(x) = \sum_{x\in\mathbb{F}_q}\sum_{I\subset[|A|]}\sum_{J\subset[|B|]}\prod_{i\in I}(\chi(x-a_i))\prod_{j\in J}(-1)^{|J|}\chi(x-b_j)$$

Let $f_{IJ}(x) = (-1)^{|J|}\prod_{i\in I}(x-a_i)\prod_{j\in J}(x-b_j)$. Then the triple sum above becomes

$$\sum_{x\in\mathbb{F}_q}\sum_{I\subset[|A|]}\sum_{J\subset[|B|]}\chi(f_{IJ}(x)) = q + R$$

The last equality arises as follows: If I and J are both empty, $\chi(f_{IJ}(x)) = \chi(1) = 1$, so the sum over $\mathbb{F}_q$ of 1 is q. Then let R be the triple sum over all I and J such that $I \cup J \neq \emptyset$. Although this is a double sum, we will denote it by $\sum_{I\cup J\neq\emptyset}$ to avoid cluttered notation.

$$|R| \leq \sum_{I\cup J\neq\emptyset}|\sum_{x\in\mathbb{F}_q}\chi(f_{IJ}(x))| \leq \sum_{I\cup J\neq\emptyset}(|I|+|J|-1)\sqrt{q}$$

where the last inequality follows from Weil's Character Sum Estimate. We can apply this since f_{IJ} has no multiple roots so it is not of the form cg^k. Then we have $|R| < 2^{k-1}(k-2)\sqrt{q}$.

Finally, S= $2^{k-1}N + \epsilon 2^{k-2} = q + R$ so

$$N > \frac{q}{2^{k-1}} - (k-2)\sqrt{q} - \frac{1}{2} > \frac{q}{2^{k-1}} - 2k\sqrt{q} \leq 0$$

So $2k\sqrt{q} \leq 2\frac{q}{2^k}$ implies $q \geq k^2 4^k$. □

7.3. **Universal Kneser Graphs.** We conclude the section by proving the existence of $k-$universal Kneser Graphs.

Proposition 7.8. *There exist $k-$universal Kneser Graphs of size $O(k^2)$.*

Proof. A graph with k vertices has $\binom{k}{2}$ possible edges. Fix a labeling of the vertices $v_1, \dots, v_k$ and the possible edges $1, \dots m$ (so m=$\binom{k}{2}$). We claim that Kn(2k(k-1), k-1) is universal over Graphs(k). Let X be a graph with k vertices. If X is complete, we can label the vertices with k disjoint $(k-1)$-subsets. Therefore, we assume the minimum degree of X is less than $k-1$.

Create sets $S_1, \dots, S_k$ such that $n \in S_j$ if the edge n is adjacent to v_j in $\bar{X}$. This means S_m and S_l are disjoint iff v_m and v_l are adjacent in X. Now, add distinct elements to each S_j until they are of size k-1. We will have to add at most k(k-1) elements. We will have enough elements left over to do this since $\binom{k}{2} + k(k-1) < 2k(k-1)$ where $\binom{k}{2}$ corresponds to the fact that it takes at most this many elements to label the edges of X. Since we have added distinct elements to each S_j, we have preserved the adjacency property, so X can be represented as an induced subgraph of $Kn(2k(k-1), k-1)$. Furthermore, this mapping is injective since given a representation, we can remove the elements from each S_j that are not in $[m]$ and reconstruct a given graph with k vertices from the remaining elements in each S_j. Therefore, $Kn(2k(k-1), k-1)$ is k-universal. □

8. Independence Number of Paley Graphs

In this section, we study the independence number of Paley Graphs. In particular, we show that $\alpha(P_q) = O(\sqrt{q})$ and $\alpha(P_q) = \Omega(logq)$. We end the section with a brief review of what is known about finding tighter estimates on $\alpha(P_p)$ when p is prime.

Lemma 8.1. *Paley Graphs are self-complementary. As a result $\alpha(P_q) = \omega(P_q)$.*

Proof. Let G=P_q. Let $\phi : \bar{P_q} \mapsto P_q$ such that $phi(x) = kx$ where k is a quadratic nonresidue in F_q^x. Then ϕ is a bijection since k has a multiplicative inverse. x and y are adjacent in $\bar{P_q}$ if and only if x-y is a quadratic nonresidue iff kx-ky=k(x-y) is a quadratic residue iff $\phi(x)$ and $\phi(y)$ are adjacent. Therefore, P_q is isomorphic to its complement. Now, α is the largest independent set in P_q iff ω is the largest clique in $\bar{P_q}$. The same holds if we switch P_q and $\bar{P_q}$. Then since P_q is isomorphic to its complement, $\alpha(P_q) = \omega(P_q)$. □

The next proposition gives an upper bound on the independence number of any vertex-transitive graph, and this allows us to give an upper bound on the indpendence number of the Paley Graph.

Proposition 8.2. *If X is vertex transitive, then $\alpha(X)\omega(X) \leq n$.*

Proof. Let $\alpha(X) = r$ and $\omega(X) = s$. Define hypergraphs X_1 and X_2 to have the same vertex set as X; Let the edges of X_1 be the maximal independent sets of X and the edges of X_2 be the maximal cliques of X. Since X is vertex-transitive, both hypergraphs are regular. Furthermore, X_1 is r-uniform and X_2 is s-uniform. From Lemma 6.12, we have $\alpha(X)\omega(X) = rs \leq n$ since the edges of both hypergraphs can share at most one vertex. □

Corollary 8.3. *For the Paley Graph P_q, we have $\alpha(P_q) \leq \sqrt{q}$.*

Proof. This follows from the previous two propositions. □

Proposition 8.4. *There exists an infinite family of Paley Graphs such that such that $\alpha = \chi = \sqrt{q}$.*

Proof. We claim P_q works when $q = p^{2r}$ with p an odd prime. If q satisfies these conditions, then there exists a finite field G of size p^{2r}, which has a subfield $\mathbb{F}$ of size p^r . Also, $\frac{p^{2r}-1}{p^r-1} = p^r + 1$ is even since p is odd. Since G is a finite field, $G^\times$ is a cyclic group under multiplication, and so is $\mathbb{F}^\times$. Every element of $\mathbb{F}^\times$ can be written as $e^{\frac{2\pi ij}{k}}$ where $k = p^r - 1$, which is $e^{\frac{2\pi ij(p^r+1)}{k(p^r+1)}} = (e^{\frac{2\pi ij}{p^{2r}-1}})^{(p^r+1)}$. Therefore, every element of $\mathbb{F}^\times$ can be written in the form g^{p^r+1} for some $g \in G^\times$. However, $p^r + 1$ is even, so every $f \in \mathbb{F}^\times$ is a quadratic residue. In other words, if S denotes the set of quadratic residues, then $\mathbb{F}^\times \subset S$. Since $\mathbb{F}$ is closed under addition, $\mathbb{F}$ is a clique. Therefore, $\alpha = \omega \geq \sqrt{q}$, so $\alpha = \sqrt{q}$ by Corollary 8.3.

Now, since $\mathbb{F}$ is a clique in P_q, its elements form an independent set in $\bar{P_q}$, as do its cosets. Therefore, each coset can be 1-colored so $\chi \leq \frac{p^{2r}}{p^r} = \sqrt{q}$. Since any valid coloring requires at least ω colors, we also have $\chi \geq \omega = \sqrt{q}$ so $\chi = \sqrt{q}$. □

We now give a lower bound on $\alpha(P_q)$:

Proposition 8.5. *Given a Paley Graph P_q, we have $\alpha(P_q) \geq \frac{1}{2}log(q)$.*

Proof. In light of Lemma 8.1, it suffices to show that $\max\{\alpha, \omega\} \geq \frac{1}{2}\log_2(n)$ for any graph with n vertices.

Let R(r,s) be the Ramsey number j where any two-coloring of the edges of K_j has a red K_r or a blue K_s. We claim R(r,s) is also the minimum n such that a simple graph with n vertices has an independent set of size r or a clique of size s. Indeed, if we take any two-coloring of K_n, the subgraph induced by the blue edges either has an independent set of size r or a clique of size s. If the subgraph has a clique of size s, this gives us a blue K_s. Otherwise, the graph's complement (made of red edges) contains a clique of size r, which is the red K_r. Therefore, R(r,s) $\leq n$. Now, if we have any simple graph with n vertices, we can color the graphs edges blue and its complement's edges red. This is a two-coloring of K_n and $j \leq n$ so K_n either contains a red K_r or a blue K_s. The blue K_s is a clique and the red K_r is an independent set, so R(r,s)=n.

If we could show $R(r,s) \leq \binom{r+s-2}{r-1}$, then we would have $R(r,r) \leq \binom{2r-2}{r-1} \leq 4^r$ which would give us the statement we want if we set r=n. If s or r equals 2, the statement is immediate since if at least 1 edge of K_r is blue (or red) then we automatically have a blue K_2, and if all edges are red we would have a red K_r.Thus, we may assume $s, r \geq 3$, and we will prove the inequality by induction on s+t.

Base case (s+r=6): We must show K(3,3) $\leq$ 6. If we take some vertex v in K_6, it has degree 5 so without loss of generality at least 3 edges must be blue. Call 3 vertices incident to v by a blue edge a,b, and c. If ab, bc, or ac were blue then we would have a blue K_3. If not, these edges would form a red K_3. Therefore, the base case holds.

Assume the statement is true for $s+r-1$. Suppose we have a complete graph with R(s, r-1)+R(s-1,r) vertices. Fix some vertex v and partition the remaining vertices into R and S based on whether they are incident to v by a red or blue edge. Since R(s, r-1)+R(s-1,r) = $|R|+|S|+1$, we must have $|R| \geq R(s, r-1)$ or $|S| \geq R(s-1, r)$, otherwise we would have $|R| + |S| + 1 \leq R(s, r-1) + R(s-1, r) - 1$. If R contains a blue K_s, we would be done. Otherwise, add v to R, and this would yield a red K_r. Analogous reasoning holds for S. Therefore, R(r,s) $\leq R(s, r-1) + R(s-1, r) \leq 2\binom{r+s-2}{r-1} \leq (s+r-2)(r-2)\binom{r+s-2}{r-1} = \binom{r+s-2}{r-1}$ where the last inequality holds because $s + t \geq 6$. □

Open Question: A large open question is how to approximate $\alpha(P_p)$ when p is a prime. In light of the previous proposition, it was believed that $\alpha(P_p) = O(logp)$. However, this conjecture was disproved in the next two theorems. We note that these results are phrased in terms of proving lower bounds on the smallest quadratic non-residue mod p, denoted $q(p)$. Such lower bounds are equivalent to lower bounds on $\alpha(P_p)$ since $\{0, 1, \ldots, q(p) - 1\}$ forms a clique as all of these numbers must be quadratic residues. We now mention the results:

Theorem 8.6 (Montgomery [24])**.** *Assuming the Generalized Riemann Hypothesis, there are infinitely primes $p \equiv 1$ mod 4 such that $q(p) = \Omega(logp \cdot loglogp)$.*

Theorem 8.7 (Graham and Ringrose [18])**.** *Without the Generalized Riemann Hypothesis, there are infinitely primes* $p \equiv 1 \mod 4$ *such that* $q(p) = \Omega(logp \cdot logloglogp)$.

The current conjecture is now that $\alpha(P_p)$ is polylogarithmically bounded, but the authors do not know of a tighter upper bound than $\sqrt{p}$.

9. Kneser Graphs

In this section, we investigate the combinatorial properties of the Kneser Graph, particularly its girth and chromatic number.

9.1. **Girth.**

Definition 9.1. The *girth* of a graph is the length of its shortest cycle. The *odd girth* is the length of the shortest cycle with odd length > 1.

Proposition 9.2. *The girth of the Kneser Graph* $Kn(r, s)$ *is at most* 6.

Proof. Case A: If $r \geq 3s$, the graph has a 3-cycle so the girth is 3.

Case B: Suppose $2s + 2 \leq r \leq 3s - 1$. Then we have a 4-cycle consisting of :

(1) $v_1 = \{1, \ldots, s\}$
(2) $v_2 = \{s + 1, \ldots, 2s\}$
(3) $v_1 = \{1, \ldots, s - 1, 2s + 1\}$
(4) $v_1 = \{s + 1, \ldots, 2s - 1, 2s + 2\}$

Now if the graph has a 3-cycle, the corresponding sets must have distinct elements since they are pairwise disjoint, so we'd need $3s \leq r$, which is not possible. Therefore, the girth is 4.

Case C: Suppose r=2s+1. If s=2, this is the Petersen graph, which has girth 5. Assume $s > 2$. Then we have a 6-cycle consisting of:

(1) $v_1 = \{1, \ldots, s\}$
(2) $v_2 = \{s + 1, \ldots, 2s\}$
(3) $v_3 = \{2, \ldots, s, 2s + 1\}$
(4) $v_4 = \{1, s + 1 \ldots, 2s - 1\}$
(5) $v_5 = \{2, \ldots, s, 2s\}$
(6) $v_6 = \{s + 1, \ldots, 2s - 1, 2s + 1\}$

Now, suppose we have a 5-cycle and we fix v_1. v_2 and v_5 must contain distinct elements from v_1, but there are only 2s+1-s=s+1 elements remaining to put in these sets, so we must have $v_2 \cup v_5 = s + 1$ (ie. s-1 of the elements in each are the same). In other words, $v_5 \cup v_1 \cup v_2 = [r]$. Now, v_3 is adjacent to v_2 but not v_5 so it must contain the single element in $v_5 - v_2$, and the remaining s-1 elements must come from v_1. Now, v_4 is adjacent to v_5 but not v_2 so it must contain the single element in $v_2 - v_5$. However, it must be disjoint from v_3, which contains s-1 of the elements from v_1. This means that we only have 1 element from v_1 left to add to v_4, so it will not have enough elements. Therefore, there is no 5-cycle, so the girth is 6.

□

Informally speaking, the next proposition shows that if $r-2s$ is small compared to r then the Kneser Graph $Kn(r,s)$ has large odd girth.

Proposition 9.3. *The Kneser Graph $Kn(r,s)$ has no odd-cycles shorter than $\frac{r}{r-2s}$ where $r<3s$.*

Remark 9.4. Note that we impose the upper bound on r because as r goes to infinity, $\frac{r}{r-2s} \to 1$ but the graph will always have a 3-cycle if $r \geq 3s$.

Proof. Case 1: If $r \leq 2s$, there are no edges and therefore no cycles anyways.

Case 2: Suppose r= 2s+t for $0<t<s$. Let the shortest odd-cycle have length 2m+1. Fixing v_1, v_2 is disjoint from v_1. Since v_3 has at most t elements distinct from v_1 and v_2, it contains at least s-t elements from v_1. Using the same reasoning for the rest of the vertices on the cycle, we find that v_{2k+1} contains at least s-kt elements from v_1. Then since v_{2m+1} is disjoint from v_1, we must have s-mt ≤ 0. Thus, $m \geq \frac{s}{t} = \frac{s}{r-2s} = \frac{1}{2}\frac{2s}{r-2s} = \frac{1}{2}(\frac{r}{r-2s}-1)$. Therefore, $2m+1 \geq \frac{r}{r-2s}$.
Independence Number If $s > \frac{r}{2}$, any two s-subsets must have a non-empty intersection so $\alpha = \binom{r}{s}$. It is easy to construct an independent set of size $\binom{r-1}{s-1}$. Fix some element $x \in [r]$. We count how many s-subsets contain x by noticing that we can choose the remaining s-1 elements from $[r-1]$. Therefore, the number of s-subsets containing x is $\binom{r-1}{s-1}$. This shows that $\alpha \geq \binom{r-1}{s-1}$, and we conjecture that this $\alpha = \binom{r-1}{s-1}$.An easy case is when $s=\frac{r}{2}$; suppose A and B are two s-subsets of $[r]$. Then A is an s-subset $\iff$ $\bar{A}$ is an s-subset. Furthermore, $A \cap B = \emptyset \iff A \cap \bar{B} \neq \emptyset$. This means that the largest independent set is half the number of s-subsets, or $\frac{1}{2}\binom{2s}{s}$. But $\binom{2s}{s} = \binom{2s-1}{s} + \binom{2s-1}{s} = 2\binom{2s-1}{s-1} = 2\binom{r-1}{s-1}$. Therefore, $\alpha = \binom{r-1}{s-1}$. For $s < \frac{r}{2}$, we have $\alpha = \binom{r-1}{s-1}$ by the Erdos-Ko-Rado Theorem since a collection of vertices is independent iff their corresponding s-subsets intersect pairwise. □

9.2. **Chromatic Number.** We now give an upper bound on the chromatic number of the Kneser Graph:

Proposition 9.5. $\chi(Kn(r,s)) \leq r-2s+2$

Proof. If $s > \frac{r}{2}$, any two s-subsets will have a non-empty intersection, so the degree of every vertex is 0. Therefore, $\chi = 1$. If $s = \frac{r}{2}$ the degree of every vertex will be 1, so the chromatic number will be 2. Suppose $s < \frac{r}{2}$. We claim that $\chi \leq r-2s+2$. Partition the vertices into $V_1, \ldots, V_{r-2s+1}, V_{r-2s+2} \cup \cdots \cup V_{r-s+1}$ where V_j is the collection of all s-subsets with j as their smallest element. We first notice that each of $V_1, \ldots, V_{r-2s+1}$ form an independent set since any two s-subsets in V_j intersect at j. Now, we also claim that any two s-subsets in $V_{r-2s+2} \cup \cdots \cup V_{r-s+1}$ intersect. This is true since $(r-s+1)-(r-2s+2) = s-1$ so two s-subsets must intersect by Pidgeonhole Principle. Thus, we can 1-color each of the $r-2s+2$ collections V_i, yielding $\chi \leq r-2s+2$. □

10. VPAT Graphs

In this section, we prove the two main results of this paper:

Theorem 10.1. *There exist infinitely many VPAT graphs of degree $d \geq \frac{n-1}{2}$ such that $\alpha > \sqrt{n}$.*

Proof. Consider the Kneser Graphs Kn(r,s). We have shown that these are VPAT. Now, we claim that there exists a function s(r) such that $\frac{d}{n} \geq \frac{2}{3}$ for large r and $\frac{d}{n}$ is bounded away from 1.

We have

$$\frac{d}{n} = \frac{\binom{r-s}{s}}{\binom{r}{s}} = \frac{(r-s)\ldots(r-s-(s-1))}{r(r-1)\ldots(r-(s-1))}$$

since (r-s) $\leq$ r, we have

$$(\frac{r-2s+1}{r-s+1})^s \leq \frac{d}{n} \leq (\frac{r-s}{r})^s$$

and thus

$$e^{-\frac{s^2}{r-s+1}} \leq \frac{d}{n} \leq e^{-\frac{s^2}{r}}$$

If we set $s = \sqrt{\frac{r}{3}}$, the rightmost term above becomes $e^{-\frac{1}{3}}$ and the leftmost term converges to $e^{-\frac{1}{3}}$. This means that $\frac{d}{n}$ converges to $e^{-\frac{1}{3}}$ and is bounded away from 1. Furthermore, $e^{-\frac{1}{3}} > \frac{2}{3}$, so $\frac{d}{n} \geq \frac{2}{3}$ for large r.

Now, we notice that

$$\frac{\alpha}{n} = \frac{\binom{r-1}{s-1}}{\binom{r}{s}} = \frac{s}{r} = \frac{1}{\sqrt{3r}} > \frac{1}{\sqrt{n}}$$

for large r. Therefore, we have $\alpha > \sqrt{n}$. Since $d \geq \frac{2}{3}n > \frac{n-1}{2}$, our family of Kneser Graphs satisfies the conditions of the problem. □

Theorem 10.2. *There exists an infinite family of VPAT graphs such that the degree $d \to \infty$ yet χ remains bounded.*

Proof. We claim that the Hamming Graphs H(n, 3) ($n > 2$) satisfy these conditions. Indeed, these graphs are distance-transitive and therefore arc-transitive. Furthermore, $d = 3(n-1)$ which goes to infinity as $n \to \infty$. However, $\chi = 3$ since we can let our colors correspond to the elements of $\mathbb{F}_3$, and color a vertex based on the sum of its coordinates. This shows $\chi \leq 3$, but H(n, 3) has no 2-coloring since $\{(0,0,0),(1,0,0),(2,0,0)\}$ is a clique. Finally, vertex-primitivity follows from Lemma 4.20. □

Acknowledgements

First and foremost, I thank Professor László Babai for giving me so many delightful problems to think about, and for putting in constant effort and support into advising me and helping me edit this paper. Next, I thank Professor Peter May for organizing this REU. I also thank my brilliant peers and professors at Columbia for inspiring me every day with their infectious enthusiasm for math.

References

[1] L. Babai. Longest Cycles in Vertex-Transitive Graphs. Journal of Graph Theory, Vol. 3, pages 301-304, 1979.

[2] L. Babai. On the Order of Uniprimitive Permutation Groups. Annals of Mathematics, Second Series, Vol. 113, No. 3, pages 553-568, 1981.

[3] L. Babai and P. Frankl. Linear Algebra Methods in Combinatorics (Preliminary Version 2). The University of Chicago Dept. of Computer Science, 1992.

[4] L. Babai. Automorphism Groups, Isomorphism, Reconstruction. The Handbook of Combinatorics (Chapter 27), 1995.

[5] L. Babai and J. Wilmes. Quasipolynomial-time Canonical Form for Steiner Designs. Proceedings of the fourty-fifth annual ACM symposium on Theory of Computing, 2013.

[6] L. Babai. Graph Isomorphism in Quasipolynomial Time. arXiv:1512.03547 [cs.DS], 2016. Updated version (http://people.cs.uchicago.edu/ laci/17groups/version2.1.pdf).

[7] S. Bang, A. Dubickas, J. Koolen, V. Moulton. There are only finitely many distance-regular graphs of fixed valency greater than two. Advances in Mathematics, Vol. 269, pages 1-55, 2015.

[8] I. Bárány. A short proof of Kneser's Conjecture. Journal of Combinatorial Theory, Vol. 25, pages 325-326, 1978.

[9] N. Biggs. Three Remarkable Graphs. Canadian Journal of Mathematics, Vol. 25, Issue 2, pages 397-411, 1973.

[10] N. Biggs. Algebraic Graph Theory (2nd ed., Cambridge Mathematical Library). Cambridge: Cambridge University Press. doi:10.1017/CBO9780511608704, 1974.

[11] J. Bon. Finite Primitive Distance-Transitive Graphs. European Journal of Combinatorics, Vol. 28, Issue 2, pages 517-532, 2007.

[12] R. Bose. Strongly regular graphs, partial geometries, and partially balanced designs. Pacific Journal of Mathematic, Vol. 13, No. 2, pages 389-419, 1963.

[13] A.E. Brouwer, A.M. Cohen, A. Neumaier. Distance-regular graphs. Ergebnisse der Mathematik und ihrerGrenzgebiete (3) (Results in Mathematics and Related Areas (3)), Vol. 18, Springer, Berlin, 1989.

[14] P. J. Cameron. Automorphism groups of graphs. In R. J. Wilson L. W. Beineke, editor, Selected Topics in Graph Theory, 2, pages 89–127. Acad. Press, 1983. MR 86i:05079.

[15] J. Dixon and B. Mortimer. Permutation Groups. Graduate Texts in Mathematics, Springer-Verlag New York, 1996.

[16] D.S. Dummit and R.M. Foote. Abstract Algebra. Wiley, Hoboken, 2004.

[17] B. Elspas and J. Turner. Graphs with circulant adjacency matrices. Journal of Combinatorial Theory, Vol. 9, pages 297-307, 1970.

[18] S. W. Graham, C. J. Ringrose, Lower bounds for least quadratic nonresidues, Analytic number theory (Allerton Park, IL, 1989), Progr. Math., 85, Birkhauser (1990), 269-309

[19] C. Godsil. Algebraic Combinatorics. Chapman and Hall Mathematics, 1993.

[20] C. Godsil and G. Royle. Algebraic Graph Theory. New York: Springer-Verlag, 2001.

[21] L. Lovász. Combinatorial Problems and Exercises. Akadémiai Kiadó, Budapest and North-Holland, Amsterdam, 1979. 2nd ed., 1993.

[22] W. Mader. n-fach kantenzusammenhängende Graphen. Math. Ann., Vol. 191, pages 21-28, 1971.

[23] W. Mader. Über den Zusammenhang symmetrischer Graphen. Arch. Math., Vol. 22, pages 333-336, 1971.

[24] H. L. Montgomery, Topics in multiplicative number theory, Lecture Notes in Math. 227, Springer, 1971.

[25] P. Müller. Permutation groups of prime degree, a quick proof of Burnside's theorem. Archiv der Mathematik, Vol. 85, pages 15-17, 2005.

[26] J. Rotman. An Introduction to the Theory of Groups. Graduate Texts in Mathematics, Vol. 148, 4th Edition, Springer, 1995.

[27] D.H. Smith. Primitive and Imprimitive Graphs. The Quarterly Journal of Mathematics, Vol. 22, Issue 4, pages 551-557, 1971.

[28] M.E. Watkins. Connectivity of transitive graphs. Journal of Combinatorial Theory, Vol. 8, pages 23-29, 1970.

[29] H. Whitney. Congruent Graphs and the Connectivity of Graphs. Amer. J. Math, Vol. 54, pages 150-168, 1932.